NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

April 12, 2011

VIA ELECTRONIC FILING

Ms. Kimberly D. Bose
Secretary
Federal Energy Regulatory Commission
888 First Street, NE
Washington, D.C. 20426

Re: Errata to Petition of the North American Electric Reliability Corporation for Approval of Critical Infrastructure Protection (CIP) Reliability Standards Version 4
FERC Docket No. RM06-22-000

Dear Ms. Bose:

On February 10, 2011, the North American Electric Reliability Corporation ("NERC") submitted a Petition for Approval of Critical Infrastructure Protection (CIP) Reliability Standards Version 4 in the above-referenced docket ("February 10 Petition").[1] NERC is filing these errata to correct several deficiencies in the February 10 Petition. NERC is including with this errata filing a revised set of exhibits to replace those included in the February 10 Petition. NERC is including all of the original exhibits submitted with the February 10 Petition as well as the corrected exhibits included in this errata filing, with the exception of original Exhibit E (Development History) due to the size of the file. Only those items noted below have been corrected in the revised set of exhibits. All other exhibits included in this filing remain unchanged from the version filed in the February 10 Petition.

[1] *Petition of the North American Electric Reliability Corporation for Approval of Critical Infrastructure Protection (CIP) Reliability Standards Version 4*, Docket No. RM06-22-000 (February 10, 2011)

116-390 Village Blvd.
Princeton, NJ 08540
609.452.8060 | www.nerc.com

ERRATA

1) It has come to NERC's attention that there is a typo on page six of the February 10 Petition. The last sentence of the first full paragraph on page six should be corrected as follows: "While the standard drafting team is still working to determine what form the next version of the CIP Reliability Standards will take, with the revisions in Version 4, an established baseline of cyber protection will be extended to all Bulk Electric System ~~Cyber~~ Critical Assets."

2) The redline included for the proposed CIP-002-4 Reliability Standard was not made with the previous version, CIP-002-3, as its base. **Corrected Exhibit A** to the filing includes the correct redline and clean version of the proposed CIP-002-4 standard.

3) On page 70 and 75 of the February 10 Petition, NERC has identified typographical errors in the proposed CIP-003-4 Reliability Standard, Applicability Section, Part 4.2.4. This section should read "Responsible Entities that, in compliance with Standard CIP-002-4, identify that they have no Critical Cyber Assets shall only be required to comply with CIP- 003-4 Requirement R2." **Corrected Exhibit A** to this filing includes the redline and clean versions of the proposed CIP-003-4 Reliability Standard with the corrections to the Applicability Section, Part 4.2.4.

4) NERC has identified a correction to the proposed CIP-005-4 Reliability Standard. The Effective date and the Compliance section have been modified for consistency with the rest of the Version 4 CIP standards. The effective date language was filed incorrectly because, at the time of the ballot of the CIP Version 4 standards, the ballot for the Urgent Action Standards Authorization Request for CIP-005 (Project 2010-15) was taking place

concurrently. In both the initial ballot and the successive ballot for the CIP Version 4 standards, NERC stated the following:

> Each of the CIP standards (CIP-003-3 through CIP-009-3) contains at least one reference to CIP-002-3. To maintain clarity, CIP-003-3 through CIP-009-3 have had conforming changes made, so that all cross references within the set of standards are to "CIP Version 4" standards. *(CIP-005-4 – Cyber Security – Electronic Security Perimeter is posted separately, with a set of proposed revisions for expedited processing under Project 2010-15. If CIP-005-4 is not approved under Project 2010-15, it will be returned to this set of CIP standards.)*

Accordingly, because the proposed CIP-005-4 standard balloted as part of Project 2010-15 did not pass the ballot process, the effective date language in the proposed CIP-005-4 standard included in the February 10 Petition should have included the conforming changes consistent with the conforming changes included in the other proposed CIP Version 4 standards included in the February 10 Petition. A clean and redline of the corrections to the effective date language in the CIP-005-4 standard is included in **Corrected Exhibit A** to this filing.

5) In the proposed CIP-005-4 standard, the letter "a" has been added to indicate the FERC approved interpretation included as CIP-005-3a should be carried over to the proposed CIP-005-4 standard and be designated as CIP-005-4a. **Corrected Exhibit A** to this filing includes the corrected redline and clean versions of the proposed CIP-005-4a standard.

6) NERC has added a "c" to CIP-006-4 to correctly indicate that the previously FERC approved interpretation to CIP-006-3c has been carried forward to CIP-006-4, thereby designating the Reliability Standard as CIP-006-4c. **Corrected Exhibit A** to this filing includes the redline and clean versions of CIP-006-4c.

7) In reviewing the development record included as Exhibit E to the February 10 Petition, NERC determined that the meeting notes from the Standard Drafting Team meetings were mistakenly left out of the final version of the exhibit. NERC is hereby including the meeting minutes from the Standard Drafting Team meetings in a new **Exhibit G** to this filing.

8) For completeness, NERC is including in this errata filing the revised, complete set of proposed VRFs and VSLs for the CIP Version 4 standards that was filed by NERC in its March 21, 2011 Compliance filing of CIP VRFs and VSLs.[2] A clean and redline of the VRFs and the VSLs for the CIP Version 4 Reliability Standards carried over from the CIP Versions 2 and 3 VRFs and VSLs that was proposed in the March 31 filing in compliance with the Commission's January 6, 2011 Order,[3] should replace the CIP VRFs and VSLs included in the February 10 Petition to take into account the Commission's January 20 directed changes. A **Corrected Exhibit F** is included with this filing.

NERC respectfully requests that the Commission take note of this errata filing, and issue an order consistent with NERC's filings submitted in this proceeding.

Respectfully submitted,

/s/ Holly A. Hawkins
Holly A. Hawkins
Attorney for North American Electric Reliability Corporation

cc: Official service lists in Docket No. RM06-22-000

[2] *See, Compliance Filing of the North American Electric Reliability Corporation in Response to January 20, 2011 Order on Violation Risk Factors and Violation Severity Levels for Critical Infrastructure Protection Reliability Standards,* Docket Nos. RD10-6-000 and RD09-7-002 (March 21, 2011).
[3] *Order on Version 2 and Version 3 Violation Risk Factors and Violation Severity Levels for Critical Infrastructure Protection Reliability Standards,* 134 FERC ¶ 61,045 (January 20, 2011).

CORRECTED Exhibit A

Proposed CIP-002-4 through CIP-009-4 Reliability Standards submitted for approval

Corrected CIP-002-4 Clean and Redline

A. Introduction

1. Title: Cyber Security — Critical Cyber Asset Identification

2. Number: CIP-002-4

3. Purpose: NERC Standards CIP-002-4 through CIP-009-4 provide a cyber security framework for the identification and protection of Critical Cyber Assets to support reliable operation of the Bulk Electric System.

These standards recognize the differing roles of each entity in the operation of the Bulk Electric System, the criticality and vulnerability of the assets needed to manage Bulk Electric System reliability, and the risks to which they are exposed.

Business and operational demands for managing and maintaining a reliable Bulk Electric System increasingly rely on Cyber Assets supporting critical reliability functions and processes to communicate with each other, across functions and organizations, for services and data. This results in increased risks to these Cyber Assets.

Standard CIP-002-4 requires the identification and documentation of the Critical Cyber Assets associated with the Critical Assets that support the reliable operation of the Bulk Electric System. These Critical Assets are to be identified through the application of the criteria in Attachment 1.

4. Applicability:

4.1. Within the text of Standard CIP-002-4, "Responsible Entity" shall mean:

4.1.1 Reliability Coordinator.

4.1.2 Balancing Authority.

4.1.3 Interchange Authority.

4.1.4 Transmission Service Provider.

4.1.5 Transmission Owner.

4.1.6 Transmission Operator.

4.1.7 Generator Owner.

4.1.8 Generator Operator.

4.1.9 Load Serving Entity.

4.1.10 NERC.

4.1.11 Regional Entity.

4.2. The following are exempt from Standard CIP-002-4:

4.2.1 Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.3 In nuclear plants, the systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F. R. Section 73.54.

5. Effective Date: The first day of the eighth calendar quarter after applicable regulatory approvals have been received (or the Reliability Standard otherwise becomes effective the first day of the ninth calendar quarter after BOT adoption in those jurisdictions where regulatory approval is not required)

B. Requirements

R1. Critical Asset Identification — The Responsible Entity shall develop a list of its identified Critical Assets determined through an annual application of the criteria contained in *CIP-002-4 Attachment 1 – Critical Asset Criteria*. The Responsible Entity shall update this list as necessary, and review it at least annually.

R2. Critical Cyber Asset Identification — Using the list of Critical Assets developed pursuant to Requirement R1, the Responsible Entity shall develop a list of associated Critical Cyber Assets essential to the operation of the Critical Asset. The Responsible Entity shall update this list as necessary, and review it at least annually.

For each group of generating units (including nuclear generation) at a single plant location identified in Attachment 1, criterion 1.1, the only Cyber Assets that must be considered are those shared Cyber Assets that could, within 15 minutes, adversely impact the reliable operation of any combination of units that in aggregate equal or exceed Attachment 1, criterion 1.1.

For the purpose of Standard CIP-002-4, Critical Cyber Assets are further qualified to be those having at least one of the following characteristics:

- The Cyber Asset uses a routable protocol to communicate outside the Electronic Security Perimeter; or,
- The Cyber Asset uses a routable protocol within a control center; or,
- The Cyber Asset is dial-up accessible.

R3. Annual Approval — The senior manager or delegate(s) shall approve annually the list of Critical Assets and the list of Critical Cyber Assets. Based on Requirements R1 and R2 the Responsible Entity may determine that it has no Critical Assets or Critical Cyber Assets. The Responsible Entity shall keep a signed and dated record of the senior manager or delegate(s)'s approval of the list of Critical Assets and the list of Critical Cyber Assets (even if such lists are null.)

C. Measures

M1. The Responsible Entity shall make available its list of Critical Assets as specified in Requirement R1.

M2. The Responsible Entity shall make available its list of Critical Cyber Assets as specified in Requirement R2.

M3. The Responsible Entity shall make available its records of approvals as specified in Requirement R3.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

1.1.1 The Regional Entity shall serve as the Compliance Enforcement Authority with the following exceptions:

- For entities that do not work for the Regional Entity, the Regional Entity shall serve as the Compliance Enforcement Authority.
- For Reliability Coordinators and other functional entities that work for their Regional Entity, the ERO shall serve as the Compliance Enforcement Authority.

- For Responsible Entities that are also Regional Entities, the ERO or a Regional Entity approved by the ERO and FERC or other applicable governmental authorities shall serve as the Compliance Enforcement Authority.
- For the ERO, a third-party monitor without vested interest in the outcome for the ERO shall serve as the Compliance Enforcement Authority.

1.2. Compliance Monitoring and Enforcement Processes

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints

1.3. Data Retention

1.3.1 The Responsible Entity shall keep documentation required by Standard CIP-002-4 from the previous full calendar year unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

1.3.2 The Compliance Enforcement Authority in conjunction with the Registered Entity shall keep the last audit records and all requested and submitted subsequent audit records.

1.4. Additional Compliance Information

1.4.1 None.

2. Violation Severity Levels (To be developed later.)

E. Regional Variances

None identified.

Version History

Version	Date	Action	Change Tracking
1	January 16, 2006	R3.2 — Change “Control Center” to “control center”	03/24/06
2		Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	

3		Updated version number from -2 to -3	
3	12/16/09	Approved by the NERC Board of Trustees	Update
4	12/30/10	Modified to add specific criteria for Critical Asset identification	Update
4	1/24/11	Approved by the NERC Board of Trustees	

CIP-002-4 - Attachment 1

Critical Asset Criteria

The following are considered Critical Assets:

1.1. Each group of generating units (including nuclear generation) at a single plant location with an aggregate highest rated net Real Power capability of the preceding 12 months equal to or exceeding 1500 MW in a single Interconnection.

1.2. Each reactive resource or group of resources at a single location (excluding generation Facilities) having aggregate net Reactive Power nameplate rating of 1000 MVAR or greater.

1.3. Each generation Facility that the Planning Coordinator or Transmission Planner designates and informs the Generator Owner or Generator Operator as necessary to avoid BES Adverse Reliability Impacts in the long-term planning horizon.

1.4. Each Blackstart Resource identified in the Transmission Operator's restoration plan.

1.5. The Facilities comprising the Cranking Paths and meeting the initial switching requirements from the Blackstart Resource to the first interconnection point of the generation unit(s) to be started, or up to the point on the Cranking Path where two or more path options exist, as identified in the Transmission Operator's restoration plan.

1.6. Transmission Facilities operated at 500 kV or higher.

1.7. Transmission Facilities operated at 300 kV or higher at stations or substations interconnected at 300 kV or higher with three or more other transmission stations or substations.

1.8. Transmission Facilities at a single station or substation location that are identified by the Reliability Coordinator, Planning Authority or Transmission Planner as critical to the derivation of Interconnection Reliability Operating Limits (IROLs) and their associated contingencies.

1.9. Flexible AC Transmission Systems (FACTS), at a single station or substation location, that are identified by the Reliability Coordinator, Planning Authority or Transmission Planner as critical to the derivation of Interconnection Reliability Operating Limits (IROLs) and their associated contingencies.

1.10. Transmission Facilities providing the generation interconnection required to connect generator output to the transmission system that, if destroyed, degraded, misused, or otherwise rendered unavailable, would result in the loss of the assets identified by any Generator Owner as a result of its application of Attachment 1, criterion 1.1 or 1.3.

1.11. Transmission Facilities identified as essential to meeting Nuclear Plant Interface Requirements.

1.12. Each Special Protection System (SPS), Remedial Action Scheme (RAS) or automated switching system that operates BES Elements that, if destroyed, degraded, misused or otherwise rendered unavailable, would cause one or more Interconnection Reliability Operating Limits (IROLs) violations for failure to operate as designed.

1.13. Each system or Facility that performs automatic load shedding, without human operator initiation, of 300 MW or more implementing Under Voltage Load Shedding (UVLS) or Under Frequency Load Shedding (UFLS) as required by the regional load shedding program.

1.14. Each control center or backup control center used to perform the functional obligations of the Reliability Coordinator.

1.15. Each control center or backup control center used to control generation at multiple plant locations, for any generation Facility or group of generation Facilities identified in criteria 1.1, 1.3, or 1.4. Each control center or backup control center used to control generation equal to or exceeding 1500 MW in a single Interconnection.

1.16. Each control center or backup control center used to perform the functional obligations of the Transmission Operator that includes control of at least one asset identified in criteria 1.2, 1.5, 1.6, 1.7, 1.8, 1.9, 1.10, 1.11 or 1.12.

1.17. Each control center or backup control center used to perform the functional obligations of the Balancing Authority that includes at least one asset identified in criteria 1.1, 1.3, 1.4, or 1.13. Each control center or backup control center used to perform the functional obligations of the Balancing Authority for generation equal to or greater than an aggregate of 1500 MW in a single Interconnection.

A. Introduction

1. Title: Cyber Security — Critical Cyber Asset Identification

2. Number: CIP-002-~~3~~4

3. Purpose: NERC Standards CIP-002-~~3~~4 through CIP-009-~~3~~4 provide a cyber security framework for the identification and protection of Critical Cyber Assets to support reliable operation of the Bulk Electric System.

These standards recognize the differing roles of each entity in the operation of the Bulk Electric System, the criticality and vulnerability of the assets needed to manage Bulk Electric System reliability, and the risks to which they are exposed.

Business and operational demands for managing and maintaining a reliable Bulk Electric System increasingly rely on Cyber Assets supporting critical reliability functions and processes to communicate with each other, across functions and organizations, for services and data. This results in increased risks to these Cyber Assets.

Standard CIP-002-~~3~~4 requires the identification and documentation of the Critical Cyber Assets associated with the Critical Assets that support the reliable operation of the Bulk Electric System. These Critical Assets are to be identified through the application of ~~a risk based assessment~~the criteria in Attachment 1.

4. Applicability:

4.1. Within the text of Standard CIP-002-~~3~~4, "Responsible Entity" shall mean:

4.1.1 Reliability Coordinator.

4.1.2 Balancing Authority.

4.1.3 Interchange Authority.

4.1.4 Transmission Service Provider.

4.1.5 Transmission Owner.

4.1.6 Transmission Operator.

4.1.7 Generator Owner.

4.1.8 Generator Operator.

4.1.9 Load Serving Entity.

4.1.10 NERC.

4.1.11 Regional Entity.

4.2. The following are exempt from Standard CIP-002-~~3~~4:

4.2.1 Facilities regulated by ~~the U.S. Nuclear Regulatory Commission or~~ the Canadian Nuclear Safety Commission.

4.2.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.3 In nuclear plants, the systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F. R. Section 73.54.

5. Effective Date: The first day of the ~~third~~eighth calendar quarter after applicable regulatory approvals have been received (or the Reliability Standard otherwise becomes effective the first

day of the ~~third~~ninth calendar quarter after BOT adoption in those jurisdictions where regulatory approval is not required)

B. Requirements

~~**R1.** Critical Asset Identification Method — The Responsible Entity shall identify and document a risk-based assessment methodology to use to identify its Critical Assets.~~

~~**R1.1.** The Responsible Entity shall maintain documentation describing its risk-based assessment methodology that includes procedures and evaluation criteria.~~

~~**R1.2.** The risk-based assessment shall consider the following assets:~~

~~**R1.2.1.** Control centers and backup control centers performing the functions of the entities listed in the Applicability section of this standard.~~

~~**R1.2.2.** Transmission substations that support the reliable operation of the Bulk Electric System.~~

~~**R1.2.3.** Generation resources that support the reliable operation of the Bulk Electric System.~~

~~**R1.2.4.** Systems and facilities critical to system restoration, including blackstart generators and substations in the electrical path of transmission lines used for initial system restoration.~~

~~**R1.2.5.** Systems and facilities critical to automatic load shedding under a common control system capable of shedding 300 MW or more.~~

~~**R1.2.6.** Special Protection Systems that support the reliable operation of the Bulk Electric System.~~

~~**R1.2.7.** Any additional assets that support the reliable operation of the Bulk Electric System that the Responsible Entity deems appropriate to include in its assessment.~~

~~**R2.**~~**R1.** Critical Asset Identification — The Responsible Entity shall develop a list of its identified Critical Assets determined through an annual application of the ~~risk-based assessment methodology required~~criteria contained in ~~R1.~~*CIP-002-4 Attachment 1 – Critical Asset Criteria*. The Responsible Entity shall ~~review~~update this list as necessary, and review it at least annually~~, and update it as necessary~~.

R2. Critical Cyber Asset Identification — Using the list of Critical Assets developed pursuant to Requirement ~~R2~~R1, the Responsible Entity shall develop a list of associated Critical Cyber Assets essential to the operation of the Critical Asset. ~~Examples at control centers and backup control centers include systems and facilities at master and remote sites that provide monitoring and control, automatic generation control, real-time power system modeling, and real-time inter-utility data exchange.~~ The Responsible Entity shall ~~review~~update this list as necessary, and review it at least annually~~, and update it as necessary.~~ .

For each group of generating units (including nuclear generation) at a single plant location identified in Attachment 1, criterion 1.1, the only Cyber Assets that must be considered are those shared Cyber Assets that could, within 15 minutes, adversely impact the reliable operation of any combination of units that in aggregate equal or exceed Attachment 1, criterion 1.1.

~~**R3.**~~ For the purpose of Standard CIP-002-~~3~~4, Critical Cyber Assets are further qualified to be those having at least one of the following characteristics:

~~**R3.1.**~~• The Cyber Asset uses a routable protocol to communicate outside the Electronic Security Perimeter; or,

~~**R3.2.**~~• The Cyber Asset uses a routable protocol within a control center; or,

~~**R3.3.**~~• The Cyber Asset is dial-up accessible.

~~R4.~~R3. Annual Approval — The senior manager or delegate(s) shall approve annually the ~~risk-based assessment methodology, the~~ list of Critical Assets and the list of Critical Cyber Assets. Based on Requirements R1~~, R2,~~ and ~~R3~~R2 the Responsible Entity may determine that it has no Critical Assets or Critical Cyber Assets. The Responsible Entity shall keep a signed and dated record of the senior manager or delegate(s)'s approval of the ~~risk-based assessment methodology, the~~ list of Critical Assets and the list of Critical Cyber Assets (even if such lists are null.)

C. Measures

~~**M1.** The Responsible Entity shall make available its current risk-based assessment methodology documentation as specified in Requirement R1.~~

~~M2.~~M1. The Responsible Entity shall make available its list of Critical Assets as specified in Requirement ~~R2~~R1.

~~M3.~~M2. The Responsible Entity shall make available its list of Critical Cyber Assets as specified in Requirement ~~R3~~R2.

~~M4.~~M3. The Responsible Entity shall make available its ~~approval~~ records of ~~annual~~ approvals as specified in Requirement ~~R4~~R3.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

1.1.1 The Regional Entity ~~for Responsible Entities~~shall serve as the Compliance Enforcement Authority with the following exceptions:

- For entities that do not ~~perform delegated tasks~~work for the Regional Entity, the Regional Entity shall serve as the Compliance Enforcement Authority.

~~**1.1.1**~~ For Reliability Coordinators and other functional entities that work for their Regional Entity, the ERO shall serve as the Compliance Enforcement Authority.

~~**1.1.2 ERO for Regional Entity.**~~

- ~~Third~~For Responsible Entities that are also Regional Entities, the ERO or a Regional Entity approved by the ERO and FERC or other applicable governmental authorities shall serve as the Compliance Enforcement Authority.

~~**1.1.3**~~ For the ERO, a third-party monitor without vested interest in the outcome for ~~NERC.~~

~~**1.2.**~~ the ERO shall serve as the Compliance ~~**Monitoring Period and Reset Time Frame**~~

- ~~Not applicable~~Enforcement Authority.

~~1.3.~~1.2. **Compliance Monitoring and Enforcement Processes**

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints

~~1.4.~~1.3. **Data Retention**

~~1.4.1~~1.3.1 The Responsible Entity shall keep documentation required by Standard CIP-002-~~3~~4 from the previous full calendar year unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

~~1.4.2~~1.3.2 The Compliance Enforcement Authority in conjunction with the Registered Entity shall keep the last audit records and all requested and submitted subsequent audit records.

~~1.5.~~1.4. **Additional Compliance Information**

~~1.5.1~~1.4.1 None.

2. Violation Severity Levels (To be developed later.)

E. Regional Variances

None identified.

Version History

Version	Date	Action	Change Tracking
1	January 16, 2006	R3.2 — Change "Control Center" to "control center"	~~Errata~~03/24/06
2		Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3		Updated version number from -2 to -3	
3	~~December~~ 12/16~~,~~ ~~2009~~/09	Approved by the NERC Board of Trustees	Update
4	12/30/10	Modified to add specific criteria for Critical Asset identification	Update
4	1/24/11	Approved by the NERC Board of Trustees	

CIP-002-4 - Attachment 1

Critical Asset Criteria

The following are considered Critical Assets:

1.1. Each group of generating units (including nuclear generation) at a single plant location with an aggregate highest rated net Real Power capability of the preceding 12 months equal to or exceeding 1500 MW in a single Interconnection.

1.2. Each reactive resource or group of resources at a single location (excluding generation Facilities) having aggregate net Reactive Power nameplate rating of 1000 MVAR or greater.

1.3. Each generation Facility that the Planning Coordinator or Transmission Planner designates and informs the Generator Owner or Generator Operator as necessary to avoid BES Adverse Reliability Impacts in the long-term planning horizon.

1.4. Each Blackstart Resource identified in the Transmission Operator's restoration plan.

1.5. The Facilities comprising the Cranking Paths and meeting the initial switching requirements from the Blackstart Resource to the first interconnection point of the generation unit(s) to be started, or up to the point on the Cranking Path where two or more path options exist, as identified in the Transmission Operator's restoration plan.

1.6. Transmission Facilities operated at 500 kV or higher.

1.7. Transmission Facilities operated at 300 kV or higher at stations or substations interconnected at 300 kV or higher with three or more other transmission stations or substations.

1.8. Transmission Facilities at a single station or substation location that are identified by the Reliability Coordinator, Planning Authority or Transmission Planner as critical to the derivation of Interconnection Reliability Operating Limits (IROLs) and their associated contingencies.

1.9. Flexible AC Transmission Systems (FACTS), at a single station or substation location, that are identified by the Reliability Coordinator, Planning Authority or Transmission Planner as critical to the derivation of Interconnection Reliability Operating Limits (IROLs) and their associated contingencies.

1.10. Transmission Facilities providing the generation interconnection required to connect generator output to the transmission system that, if destroyed, degraded, misused, or otherwise rendered unavailable, would result in the loss of the assets identified by any Generator Owner as a result of its application of Attachment 1, criterion 1.1 or 1.3.

1.11. Transmission Facilities identified as essential to meeting Nuclear Plant Interface Requirements.

1.12. Each Special Protection System (SPS), Remedial Action Scheme (RAS) or automated switching system that operates BES Elements that, if destroyed, degraded, misused or otherwise rendered unavailable, would cause one or more Interconnection Reliability Operating Limits (IROLs) violations for failure to operate as designed.

1.13. Each system or Facility that performs automatic load shedding, without human operator initiation, of 300 MW or more implementing Under Voltage Load Shedding (UVLS) or Under Frequency Load Shedding (UFLS) as required by the regional load shedding program.

1.14. Each control center or backup control center used to perform the functional obligations of the Reliability Coordinator.

1.15. Each control center or backup control center used to control generation at multiple plant locations, for any generation Facility or group of generation Facilities identified in criteria 1.1, 1.3, or 1.4. Each control center or backup control center used to control generation equal to or exceeding 1500 MW in a single Interconnection.

1.16. Each control center or backup control center used to perform the functional obligations of the Transmission Operator that includes control of at least one asset identified in criteria 1.2, 1.5, 1.6, 1.7, 1.8, 1.9, 1.10, 1.11 or 1.12.

1.17. Each control center or backup control center used to perform the functional obligations of the Balancing Authority that includes at least one asset identified in criteria 1.1, 1.3, 1.4, or 1.13. Each control center or backup control center used to perform the functional obligations of the Balancing Authority for generation equal to or greater than an aggregate of 1500 MW in a single Interconnection.

Corrected CIP-003-4 Clean and Redline

A. Introduction

1. Title: Cyber Security — Security Management Controls

2. Number: CIP-003-4

3. Purpose: Standard CIP-003-4 requires that Responsible Entities have minimum security management controls in place to protect Critical Cyber Assets. Standard CIP-003-4 should be read as part of a group of standards numbered Standards CIP-002-4 through CIP-009-4.

4. Applicability:

4.1. Within the text of Standard CIP-003-4, "Responsible Entity" shall mean:

4.1.1 Reliability Coordinator.

4.1.2 Balancing Authority.

4.1.3 Interchange Authority.

4.1.4 Transmission Service Provider.

4.1.5 Transmission Owner.

4.1.6 Transmission Operator.

4.1.7 Generator Owner.

4.1.8 Generator Operator.

4.1.9 Load Serving Entity.

4.1.10 NERC.

4.1.11 Regional Entity.

4.2. The following are exempt from Standard CIP-003-4:

4.2.1 Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.3 In nuclear plants, the systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F. R. Section 73.54

4.2.4 Responsible Entities that, in compliance with Standard CIP-002-4, identify that they have no Critical Cyber Assets shall only be required to comply with CIP-003-4 Requirement R2.

5. Effective Date: The first day of the eighth calendar quarter after applicable regulatory approvals have been received (or the Reliability Standard otherwise becomes effective the first day of the ninth calendar quarter after BOT adoption in those jurisdictions where regulatory approval is not required).

B. Requirements

R1. Cyber Security Policy — The Responsible Entity shall document and implement a cyber security policy that represents management's commitment and ability to secure its Critical Cyber Assets. The Responsible Entity shall, at minimum, ensure the following:

R1.1. The cyber security policy addresses the requirements in Standards CIP-002-4 through CIP-009-4, including provision for emergency situations.

R1.2. The cyber security policy is readily available to all personnel who have access to, or are responsible for, Critical Cyber Assets.

R1.3. Annual review and approval of the cyber security policy by the senior manager assigned pursuant to R2.

R2. Leadership — The Responsible Entity shall assign a single senior manager with overall responsibility and authority for leading and managing the entity's implementation of, and adherence to, Standards CIP-002-4 through CIP-009-4.

R2.1. The senior manager shall be identified by name, title, and date of designation.

R2.2. Changes to the senior manager must be documented within thirty calendar days of the effective date.

R2.3. Where allowed by Standards CIP-002-4 through CIP-009-4, the senior manager may delegate authority for specific actions to a named delegate or delegates. These delegations shall be documented in the same manner as R2.1 and R2.2, and approved by the senior manager.

R2.4. The senior manager or delegate(s), shall authorize and document any exception from the requirements of the cyber security policy.

R3. Exceptions — Instances where the Responsible Entity cannot conform to its cyber security policy must be documented as exceptions and authorized by the senior manager or delegate(s).

R3.1. Exceptions to the Responsible Entity's cyber security policy must be documented within thirty days of being approved by the senior manager or delegate(s).

R3.2. Documented exceptions to the cyber security policy must include an explanation as to why the exception is necessary and any compensating measures.

R3.3. Authorized exceptions to the cyber security policy must be reviewed and approved annually by the senior manager or delegate(s) to ensure the exceptions are still required and valid. Such review and approval shall be documented.

R4. Information Protection — The Responsible Entity shall implement and document a program to identify, classify, and protect information associated with Critical Cyber Assets.

R4.1. The Critical Cyber Asset information to be protected shall include, at a minimum and regardless of media type, operational procedures, lists as required in Standard CIP-002-4, network topology or similar diagrams, floor plans of computing centers that contain Critical Cyber Assets, equipment layouts of Critical Cyber Assets, disaster recovery plans, incident response plans, and security configuration information.

R4.2. The Responsible Entity shall classify information to be protected under this program based on the sensitivity of the Critical Cyber Asset information.

R4.3. The Responsible Entity shall, at least annually, assess adherence to its Critical Cyber Asset information protection program, document the assessment results, and implement an action plan to remediate deficiencies identified during the assessment.

R5. Access Control — The Responsible Entity shall document and implement a program for managing access to protected Critical Cyber Asset information.

R5.1. The Responsible Entity shall maintain a list of designated personnel who are responsible for authorizing logical or physical access to protected information.

R5.1.1. Personnel shall be identified by name, title, and the information for which they are responsible for authorizing access.

R5.1.2. The list of personnel responsible for authorizing access to protected information shall be verified at least annually.

R5.2. The Responsible Entity shall review at least annually the access privileges to protected information to confirm that access privileges are correct and that they correspond with the Responsible Entity's needs and appropriate personnel roles and responsibilities.

R5.3. The Responsible Entity shall assess and document at least annually the processes for controlling access privileges to protected information.

R6. Change Control and Configuration Management — The Responsible Entity shall establish and document a process of change control and configuration management for adding, modifying, replacing, or removing Critical Cyber Asset hardware or software, and implement supporting configuration management activities to identify, control and document all entity or vendor-related changes to hardware and software components of Critical Cyber Assets pursuant to the change control process.

C. Measures

M1. The Responsible Entity shall make available documentation of its cyber security policy as specified in Requirement R1. Additionally, the Responsible Entity shall demonstrate that the cyber security policy is available as specified in Requirement R1.2.

M2. The Responsible Entity shall make available documentation of the assignment of, and changes to, its leadership as specified in Requirement R2.

M3. The Responsible Entity shall make available documentation of the exceptions, as specified in Requirement R3.

M4. The Responsible Entity shall make available documentation of its information protection program as specified in Requirement R4.

M5. The Responsible Entity shall make available its access control documentation as specified in Requirement R5.

M6. The Responsible Entity shall make available its change control and configuration management documentation as specified in Requirement R6.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

1.2. The RE shall serve as the CEA with the following exceptions:

1.2.1 For entities that do not work for the Regional Entity, the Regional Entity shall serve as the Compliance Enforcement Authority.

1.2.2 For Reliability Coordinators and other functional entities that work for their Regional Entity, the ERO shall serve as the Compliance Enforcement Authority.

1.2.3 For Responsible Entities that are also Regional Entities, the ERO or a Regional Entity approved by the ERO and FERC or other applicable governmental authorities shall serve as the Compliance Enforcement Authority.

1.2.4 For the ERO, a third-party monitor without vested interest in the outcome for the ERO shall serve as the Compliance Enforcement Authority.

1.3. Compliance Monitoring and Enforcement Processes

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints

1.4. Data Retention

1.4.1 The Responsible Entity shall keep all documentation and records from the previous full calendar year unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

1.4.2 The Compliance Enforcement Authority in conjunction with the Registered Entity shall keep the last audit records and all requested and submitted subsequent audit records.

1.5. Additional Compliance Information

1.5.1 None

2. Violation Severity Levels (To be developed later.)

E. Regional Variances

None identified.

Version History

Version	Date	Action	Change Tracking
2		Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Requirement R2 applies to all Responsible Entities, including Responsible Entities which have no Critical Cyber Assets. Modified the personnel identification information requirements in R5.1.1 to include name, title, and the information for which they are responsible for authorizing access (removed the business phone information). Changed compliance monitor to Compliance	

		Enforcement Authority.	
3		Update version number from -2 to -3	
3	12/16/09	Approved by the NERC Board of Trustees	Update
4	01/24/2011	Board approved Update version number from “3” to “4”	Update to conform to changes to CIP-002-4 (Project 2008-06)

A. Introduction

1. Title: Cyber Security — Security Management Controls

2. Number: CIP-003-~~3~~4

3. Purpose: Standard CIP-003-~~3~~4 requires that Responsible Entities have minimum security management controls in place to protect Critical Cyber Assets. Standard CIP-003-~~3~~4 should be read as part of a group of standards numbered Standards CIP-002-~~3~~4 through CIP-009-~~3~~4.

4. Applicability:

4.1. Within the text of Standard CIP-003-~~3~~4, "Responsible Entity" shall mean:

4.1.1 Reliability Coordinator.

4.1.2 Balancing Authority.

4.1.3 Interchange Authority.

4.1.4 Transmission Service Provider.

4.1.5 Transmission Owner.

4.1.6 Transmission Operator.

4.1.7 Generator Owner.

4.1.8 Generator Operator.

4.1.9 Load Serving Entity.

4.1.10 NERC.

4.1.11 Regional Entity.

4.2. The following are exempt from Standard CIP-003-~~3~~4:

4.2.1 Facilities regulated by ~~the U.S. Nuclear Regulatory Commission or~~ the Canadian Nuclear Safety Commission.

4.2.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.3 In nuclear plants, the systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F. R. Section 73.54

~~4.2.3~~4.2.4 Responsible Entities that, in compliance with Standard CIP-002-~~3~~4, identify that they have no Critical Cyber Assets shall only be required to comply with CIP-003-~~3~~4 Requirement R2.

5. Effective Date: The first day of the ~~third~~eighth calendar quarter after applicable regulatory approvals have been received (or the Reliability Standard otherwise becomes effective the first day of the ~~third~~ninth calendar quarter after BOT adoption in those jurisdictions where regulatory approval is not required).

B. Requirements

R1. Cyber Security Policy — The Responsible Entity shall document and implement a cyber security policy that represents management's commitment and ability to secure its Critical Cyber Assets. The Responsible Entity shall, at minimum, ensure the following:

R1.1. The cyber security policy addresses the requirements in Standards CIP-002-~~3~~4 through CIP-009-~~3~~4, including provision for emergency situations.

R1.2. The cyber security policy is readily available to all personnel who have access to, or are responsible for, Critical Cyber Assets.

R1.3. Annual review and approval of the cyber security policy by the senior manager assigned pursuant to R2.

R2. Leadership — The Responsible Entity shall assign a single senior manager with overall responsibility and authority for leading and managing the entity's implementation of, and adherence to, Standards CIP-002-~~3~~4 through CIP-009-~~3~~4.

R2.1. The senior manager shall be identified by name, title, and date of designation.

R2.2. Changes to the senior manager must be documented within thirty calendar days of the effective date.

R2.3. Where allowed by Standards CIP-002-~~3~~4 through CIP-009-~~3~~4, the senior manager may delegate authority for specific actions to a named delegate or delegates. These delegations shall be documented in the same manner as R2.1 and R2.2, and approved by the senior manager.

R2.4. The senior manager or delegate(s), shall authorize and document any exception from the requirements of the cyber security policy.

R3. Exceptions — Instances where the Responsible Entity cannot conform to its cyber security policy must be documented as exceptions and authorized by the senior manager or delegate(s).

R3.1. Exceptions to the Responsible Entity's cyber security policy must be documented within thirty days of being approved by the senior manager or delegate(s).

R3.2. Documented exceptions to the cyber security policy must include an explanation as to why the exception is necessary and any compensating measures.

R3.3. Authorized exceptions to the cyber security policy must be reviewed and approved annually by the senior manager or delegate(s) to ensure the exceptions are still required and valid. Such review and approval shall be documented.

R4. Information Protection — The Responsible Entity shall implement and document a program to identify, classify, and protect information associated with Critical Cyber Assets.

R4.1. The Critical Cyber Asset information to be protected shall include, at a minimum and regardless of media type, operational procedures, lists as required in Standard CIP-002-~~3~~4, network topology or similar diagrams, floor plans of computing centers that contain Critical Cyber Assets, equipment layouts of Critical Cyber Assets, disaster recovery plans, incident response plans, and security configuration information.

R4.2. The Responsible Entity shall classify information to be protected under this program based on the sensitivity of the Critical Cyber Asset information.

R4.3. The Responsible Entity shall, at least annually, assess adherence to its Critical Cyber Asset information protection program, document the assessment results, and implement an action plan to remediate deficiencies identified during the assessment.

R5. Access Control — The Responsible Entity shall document and implement a program for managing access to protected Critical Cyber Asset information.

R5.1. The Responsible Entity shall maintain a list of designated personnel who are responsible for authorizing logical or physical access to protected information.

R5.1.1. Personnel shall be identified by name, title, and the information for which they are responsible for authorizing access.

R5.1.2. The list of personnel responsible for authorizing access to protected information shall be verified at least annually.

R5.2. The Responsible Entity shall review at least annually the access privileges to protected information to confirm that access privileges are correct and that they correspond with the Responsible Entity's needs and appropriate personnel roles and responsibilities.

R5.3. The Responsible Entity shall assess and document at least annually the processes for controlling access privileges to protected information.

R6. Change Control and Configuration Management — The Responsible Entity shall establish and document a process of change control and configuration management for adding, modifying, replacing, or removing Critical Cyber Asset hardware or software, and implement supporting configuration management activities to identify, control and document all entity or vendor-related changes to hardware and software components of Critical Cyber Assets pursuant to the change control process.

C. Measures

M1. The Responsible Entity shall make available documentation of its cyber security policy as specified in Requirement R1. Additionally, the Responsible Entity shall demonstrate that the cyber security policy is available as specified in Requirement R1.2.

M2. The Responsible Entity shall make available documentation of the assignment of, and changes to, its leadership as specified in Requirement R2.

M3. The Responsible Entity shall make available documentation of the exceptions, as specified in Requirement R3.

M4. The Responsible Entity shall make available documentation of its information protection program as specified in Requirement R4.

M5. The Responsible Entity shall make available its access control documentation as specified in Requirement R5.

M6. The Responsible Entity shall make available its change control and configuration management documentation as specified in Requirement R6.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

1.2. The RE shall serve as the CEA with the following exceptions:

1.2.1 For entities that do not work for the Regional Entity ~~for Responsible Entities that do not perform delegated tasks~~, the Regional Entity shall serve as the Compliance Enforcement Authority.

~~1.1.1~~1.2.2 For Reliability Coordinators and other functional entities that work for their Regional Entity, the ERO shall serve as the Compliance Enforcement Authority.

~~**1.1.2** ERO for Regional Entity.~~

1.2.3 ~~Third~~For Responsible Entities that are also Regional Entities, the ERO or a Regional Entity approved by the ERO and FERC or other applicable governmental authorities shall serve as the Compliance Enforcement Authority.

1.1.3 For the ERO, a third-party monitor without vested interest in the outcome for ~~NERC.~~

1.2. the ERO shall serve as the Compliance **~~Monitoring Period and Reset Time Frame~~**

1.2.4 ~~Not applicable~~Enforcement Authority.

1.3. Compliance Monitoring and Enforcement Processes

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints

1.4. Data Retention

1.4.1 The Responsible Entity shall keep all documentation and records from the previous full calendar year unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

1.4.2 The Compliance Enforcement Authority in conjunction with the Registered Entity shall keep the last audit records and all requested and submitted subsequent audit records.

1.5. Additional Compliance Information

1.5.1 None

2. Violation Severity Levels (To be developed later.)

E. Regional Variances

None identified.

Version History

Version	Date	Action	Change Tracking
2		Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Requirement R2 applies to all Responsible Entities, including Responsible Entities which have no Critical Cyber Assets.	

		Modified the personnel identification information requirements in R5.1.1 to include name, title, and the information for which they are responsible for authorizing access (removed the business phone information). Changed compliance monitor to Compliance Enforcement Authority.	
3		Update version number from -2 to -3	
3	12/16/09	Approved by the NERC Board of Trustees	Update
4	01/24/2011	Board approved Update version number from "3" to "4"	Update to conform to changes to CIP-002-4 (Project 2008-06)

CIP-004-4 Clean and Redline

A. Introduction

1. Title: Cyber Security — Personnel & Training

2. Number: CIP-004-4

3. Purpose: Standard CIP-004-4 requires that personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets, including contractors and service vendors, have an appropriate level of personnel risk assessment, training, and security awareness. Standard CIP-004-4 should be read as part of a group of standards numbered Standards CIP-002-4 through CIP-009-4.

4. Applicability:

4.1. Within the text of Standard CIP-004-4, "Responsible Entity" shall mean:

4.1.1 Reliability Coordinator.

4.1.2 Balancing Authority.

4.1.3 Interchange Authority.

4.1.4 Transmission Service Provider.

4.1.5 Transmission Owner.

4.1.6 Transmission Operator.

4.1.7 Generator Owner.

4.1.8 Generator Operator.

4.1.9 Load Serving Entity.

4.1.10 NERC.

4.1.11 Regional Entity.

4.2. The following are exempt from Standard CIP-004-4:

4.2.1 Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.3 In nuclear plants, the systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F. R. Section 73.54

4.2.4 Responsible Entities that, in compliance with Standard CIP-002-4, identify that they have no Critical Cyber Assets.

5. Effective Date: The first day of the eighth calendar quarter after applicable regulatory approvals have been received (or the Reliability Standard otherwise becomes effective the first day of the ninth calendar quarter after BOT adoption in those jurisdictions where regulatory approval is not required).

B. Requirements

R1. Awareness — The Responsible Entity shall establish, document, implement, and maintain a security awareness program to ensure personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets receive on-going reinforcement in sound security practices. The program shall include security awareness reinforcement on at least a quarterly basis using mechanisms such as:

- Direct communications (e.g., emails, memos, computer based training, etc.);

- Indirect communications (e.g., posters, intranet, brochures, etc.);
- Management support and reinforcement (e.g., presentations, meetings, etc.).

R2. Training — The Responsible Entity shall establish, document, implement, and maintain an annual cyber security training program for personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets. The cyber security training program shall be reviewed annually, at a minimum, and shall be updated whenever necessary.

R2.1. This program will ensure that all personnel having such access to Critical Cyber Assets, including contractors and service vendors, are trained prior to their being granted such access except in specified circumstances such as an emergency.

R2.2. Training shall cover the policies, access controls, and procedures as developed for the Critical Cyber Assets covered by CIP-004-4, and include, at a minimum, the following required items appropriate to personnel roles and responsibilities:

R2.2.1. The proper use of Critical Cyber Assets;

R2.2.2. Physical and electronic access controls to Critical Cyber Assets;

R2.2.3. The proper handling of Critical Cyber Asset information; and,

R2.2.4. Action plans and procedures to recover or re-establish Critical Cyber Assets and access thereto following a Cyber Security Incident.

R2.3. The Responsible Entity shall maintain documentation that training is conducted at least annually, including the date the training was completed and attendance records.

R3. Personnel Risk Assessment —The Responsible Entity shall have a documented personnel risk assessment program, in accordance with federal, state, provincial, and local laws, and subject to existing collective bargaining unit agreements, for personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets. A personnel risk assessment shall be conducted pursuant to that program prior to such personnel being granted such access except in specified circumstances such as an emergency.

The personnel risk assessment program shall at a minimum include:

R3.1. The Responsible Entity shall ensure that each assessment conducted include, at least, identity verification (e.g., Social Security Number verification in the U.S.) and seven-year criminal check. The Responsible Entity may conduct more detailed reviews, as permitted by law and subject to existing collective bargaining unit agreements, depending upon the criticality of the position.

R3.2. The Responsible Entity shall update each personnel risk assessment at least every seven years after the initial personnel risk assessment or for cause.

R3.3. The Responsible Entity shall document the results of personnel risk assessments of its personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets, and that personnel risk assessments of contractor and service vendor personnel with such access are conducted pursuant to Standard CIP-004-4.

R4. Access — The Responsible Entity shall maintain list(s) of personnel with authorized cyber or authorized unescorted physical access to Critical Cyber Assets, including their specific electronic and physical access rights to Critical Cyber Assets.

R4.1. The Responsible Entity shall review the list(s) of its personnel who have such access to Critical Cyber Assets quarterly, and update the list(s) within seven calendar days of any change of personnel with such access to Critical Cyber Assets, or any change in the access rights of such personnel. The Responsible Entity shall ensure access list(s) for contractors and service vendors are properly maintained.

R4.2. The Responsible Entity shall revoke such access to Critical Cyber Assets within 24 hours for personnel terminated for cause and within seven calendar days for personnel who no longer require such access to Critical Cyber Assets.

C. Measures

M1. The Responsible Entity shall make available documentation of its security awareness and reinforcement program as specified in Requirement R1.

M2. The Responsible Entity shall make available documentation of its cyber security training program, review, and records as specified in Requirement R2.

M3. The Responsible Entity shall make available documentation of the personnel risk assessment program and that personnel risk assessments have been applied to all personnel who have authorized cyber or authorized unescorted physical access to Critical Cyber Assets, as specified in Requirement R3.

M4. The Responsible Entity shall make available documentation of the list(s), list review and update, and access revocation as needed as specified in Requirement R4.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

1.2. The RE shall serve as the CEA with the following exceptions:

1.2.1 For entities that do not work for the Regional Entity, the Regional Entity shall serve as the Compliance Enforcement Authority.

1.2.2 For Reliability Coordinators and other functional entities that work for their Regional Entity, the ERO shall serve as the Compliance Enforcement Authority.

1.2.3 For Responsible Entities that are also Regional Entities, the ERO or a Regional Entity approved by the ERO and FERC or other applicable governmental authorities shall serve as the Compliance Enforcement Authority.

1.2.4 For the ERO, a third-party monitor without vested interest in the outcome for the ERO shall serve as the Compliance Enforcement Authority.

1.3. Compliance Monitoring and Enforcement Processes

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints

1.4. Data Retention

1.4.1 The Responsible Entity shall keep personnel risk assessment documents in accordance with federal, state, provincial, and local laws.

1.4.2 The Responsible Entity shall keep all other documentation required by Standard CIP-004-4 from the previous full calendar year unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

1.4.3 The Compliance Enforcement Authority in conjunction with the Registered Entity shall keep the last audit records and all requested and submitted subsequent audit records.

1.5. Additional Compliance Information

2. Violation Severity Levels (To be developed later.)

E. Regional Variances

None identified.

Version History

Version	Date	Action	Change Tracking
1	01/16/06	D.2.2.4 — Insert the phrase "for cause" as intended. "One instance of personnel termination for cause…"	03/24/06
1	06/01/06	D.2.1.4 — Change "access control rights" to "access rights."	06/05/06
2		Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Reference to emergency situations. Modification to R1 for the Responsible Entity to establish, document, implement, and maintain the awareness program. Modification to R2 for the Responsible Entity to establish, document, implement, and maintain the training program; also stating the requirements for the cyber security training program. Modification to R3 Personnel Risk Assessment to clarify that it pertains to personnel having authorized cyber or authorized unescorted physical access to "Critical Cyber Assets". Removal of 90 day window to complete training and 30 day window to complete personnel risk assessments. Changed compliance monitor to Compliance Enforcement Authority.	
3		Update version number from -2 to -3	
3	12/16/09	Approved by NERC Board of Trustees	Update
4	Board approved 01/24/2011	Update version number from "3" to "4"	Update to conform to changes to CIP-002-4 (Project 2008-06)

A. Introduction

1. Title: Cyber Security — Personnel & Training

2. Number: CIP-004-~~3~~4

3. Purpose: Standard CIP-004-~~3~~4 requires that personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets, including contractors and service vendors, have an appropriate level of personnel risk assessment, training, and security awareness. Standard CIP-004-~~3~~4 should be read as part of a group of standards numbered Standards CIP-002-~~3~~4 through CIP-009-~~3~~4.

4. Applicability:

4.1. Within the text of Standard CIP-004-~~3~~4, "Responsible Entity" shall mean:

4.1.1 Reliability Coordinator.

4.1.2 Balancing Authority.

4.1.3 Interchange Authority.

4.1.4 Transmission Service Provider.

4.1.5 Transmission Owner.

4.1.6 Transmission Operator.

4.1.7 Generator Owner.

4.1.8 Generator Operator.

4.1.9 Load Serving Entity.

4.1.10 NERC.

4.1.11 Regional Entity.

4.2. The following are exempt from Standard CIP-004-~~3~~4:

4.2.1 Facilities regulated by ~~the U.S. Nuclear Regulatory Commission or~~ the Canadian Nuclear Safety Commission.

4.2.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.3 In nuclear plants, the systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F. R. Section 73.54

~~Cyber Assets associated with Cyber Security Plans submitted to and verified by the U. S. Nuclear Regulatory Commission pursuant to 10 C.F.R. Section 73.54.~~

~~4.2.3~~4.2.4 Responsible Entities that, in compliance with Standard CIP-002-~~3~~4, identify that they have no Critical Cyber Assets.

5. Effective Date: The first day of the ~~third~~eighth calendar quarter after applicable regulatory approvals have been received (or the Reliability Standard otherwise becomes effective the first day of the ~~third~~ninth calendar quarter after BOT adoption in those jurisdictions where regulatory approval is not required).

B. Requirements

R1. Awareness — The Responsible Entity shall establish, document, implement, and maintain a security awareness program to ensure personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets receive on-going reinforcement in sound

Formatted: Font color: Black

Formatted: Font color: Black

security practices. The program shall include security awareness reinforcement on at least a quarterly basis using mechanisms such as:

- Direct communications (e.g., emails, memos, computer based training, etc.);
- Indirect communications (e.g., posters, intranet, brochures, etc.);
- Management support and reinforcement (e.g., presentations, meetings, etc.).

R2. Training — The Responsible Entity shall establish, document, implement, and maintain an annual cyber security training program for personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets. The cyber security training program shall be reviewed annually, at a minimum, and shall be updated whenever necessary.

R2.1. This program will ensure that all personnel having such access to Critical Cyber Assets, including contractors and service vendors, are trained prior to their being granted such access except in specified circumstances such as an emergency.

R2.2. Training shall cover the policies, access controls, and procedures as developed for the Critical Cyber Assets covered by CIP-004-~~3~~4, and include, at a minimum, the following required items appropriate to personnel roles and responsibilities:

R2.2.1. The proper use of Critical Cyber Assets;

R2.2.2. Physical and electronic access controls to Critical Cyber Assets;

R2.2.3. The proper handling of Critical Cyber Asset information; and,

R2.2.4. Action plans and procedures to recover or re-establish Critical Cyber Assets and access thereto following a Cyber Security Incident.

R2.3. The Responsible Entity shall maintain documentation that training is conducted at least annually, including the date the training was completed and attendance records.

R3. Personnel Risk Assessment —The Responsible Entity shall have a documented personnel risk assessment program, in accordance with federal, state, provincial, and local laws, and subject to existing collective bargaining unit agreements, for personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets. A personnel risk assessment shall be conducted pursuant to that program prior to such personnel being granted such access except in specified circumstances such as an emergency.

The personnel risk assessment program shall at a minimum include:

R3.1. The Responsible Entity shall ensure that each assessment conducted include, at least, identity verification (e.g., Social Security Number verification in the U.S.) and seven-year criminal check. The Responsible Entity may conduct more detailed reviews, as permitted by law and subject to existing collective bargaining unit agreements, depending upon the criticality of the position.

R3.2. The Responsible Entity shall update each personnel risk assessment at least every seven years after the initial personnel risk assessment or for cause.

R3.3. The Responsible Entity shall document the results of personnel risk assessments of its personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets, and that personnel risk assessments of contractor and service vendor personnel with such access are conducted pursuant to Standard CIP-004-~~3~~4.

R4. Access — The Responsible Entity shall maintain list(s) of personnel with authorized cyber or authorized unescorted physical access to Critical Cyber Assets, including their specific electronic and physical access rights to Critical Cyber Assets.

R4.1. The Responsible Entity shall review the list(s) of its personnel who have such access to Critical Cyber Assets quarterly, and update the list(s) within seven calendar days of any change of personnel with such access to Critical Cyber Assets, or any change in the access rights of such personnel. The Responsible Entity shall ensure access list(s) for contractors and service vendors are properly maintained.

R4.2. The Responsible Entity shall revoke such access to Critical Cyber Assets within 24 hours for personnel terminated for cause and within seven calendar days for personnel who no longer require such access to Critical Cyber Assets.

C. Measures

M1. The Responsible Entity shall make available documentation of its security awareness and reinforcement program as specified in Requirement R1.

M2. The Responsible Entity shall make available documentation of its cyber security training program, review, and records as specified in Requirement R2.

M3. The Responsible Entity shall make available documentation of the personnel risk assessment program and that personnel risk assessments have been applied to all personnel who have authorized cyber or authorized unescorted physical access to Critical Cyber Assets, as specified in Requirement R3.

M4. The Responsible Entity shall make available documentation of the list(s), list review and update, and access revocation as needed as specified in Requirement R4.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

1.2. The RE shall serve as the CEA with the following exceptions:

1.2.1 For entities that do not work for the Regional Entity ~~for Responsible Entities that do not perform delegated tasks~~, the Regional Entity shall serve as the Compliance Enforcement Authority.

~~1.1.1~~1.2.2 For Reliability Coordinators and other functional entities that work for their Regional Entity, the ERO shall serve as the Compliance Enforcement Authority.

~~**1.1.2 ERO for Regional Entity.**~~

1.2.3 ~~Third~~For Responsible Entities that are also Regional Entities, the ERO or a Regional Entity approved by the ERO and FERC or other applicable governmental authorities shall serve as the Compliance Enforcement Authority.

~~**1.1.3**~~ For the ERO, a third-party monitor without vested interest in the outcome for ~~NERC.~~

~~**1.2.**~~ the ERO shall serve as the Compliance ~~**Monitoring Period and Reset Time Frame**~~

1.2.4 ~~Not Applicable~~Enforcement Authority.

1.3. Compliance Monitoring and Enforcement Processes

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Formatted: Font: Not Bold

Formatted: List Number, Outline numbered + Level: 3 + Numbering Style: 1, 2, 3, … + Start at: 1 + Alignment: Left + Aligned at: 1" + Tab after: 1.5" + Indent at: 1.5"

Self-Reporting

Complaints

1.4. Data Retention

1.4.1 The Responsible Entity shall keep personnel risk assessment documents in accordance with federal, state, provincial, and local laws.

1.4.2 The Responsible Entity shall keep all other documentation required by Standard CIP-004-~~3~~4 from the previous full calendar year unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

1.4.3 The Compliance Enforcement Authority in conjunction with the Registered Entity shall keep the last audit records and all requested and submitted subsequent audit records.

1.5. Additional Compliance Information

2. Violation Severity Levels (To be developed later.)

E. Regional Variances

None identified.

Version History

Version	Date	Action	Change Tracking
1	01/16/06	D.2.2.4 — Insert the phrase "for cause" as intended. "One instance of personnel termination for cause…"	03/24/06
1	06/01/06	D.2.1.4 — Change "access control rights" to "access rights."	06/05/06
2		Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Reference to emergency situations. Modification to R1 for the Responsible Entity to establish, document, implement, and maintain the awareness program. Modification to R2 for the Responsible Entity to establish, document, implement, and maintain the training program; also stating the requirements for the cyber security training program. Modification to R3 Personnel Risk Assessment to clarify that it pertains to personnel having authorized cyber or authorized unescorted physical access to "Critical Cyber Assets".	

		Removal of 90 day window to complete training and 30 day window to complete personnel risk assessments. Changed compliance monitor to Compliance Enforcement Authority.	
3		Update version number from -2 to -3	
3	12/16/09	Approved by NERC Board of Trustees	Update
4	Board approved 01/24/2011	Update version number from "3" to "4"	Update to conform to changes to CIP-002-4 (Project 2008-06)

Corrected CIP-005-4a Clean and Redline

A. Introduction

1. Title: Cyber Security — Electronic Security Perimeter(s)

2. Number: CIP-005-4a

3. Purpose: Standard CIP-005-4a requires the identification and protection of the Electronic Security Perimeter(s) inside which all Critical Cyber Assets reside, as well as all access points on the perimeter. Standard CIP-005-4a should be read as part of a group of standards numbered Standards CIP-002-4 through CIP-009-4.

4. Applicability

4.1. Within the text of Standard CIP-005-4a, "Responsible Entity" shall mean:

4.1.1 Reliability Coordinator.

4.1.2 Balancing Authority.

4.1.3 Interchange Authority.

4.1.4 Transmission Service Provider.

4.1.5 Transmission Owner.

4.1.6 Transmission Operator.

4.1.7 Generator Owner.

4.1.8 Generator Operator.

4.1.9 Load Serving Entity.

4.1.10 NERC.

4.1.11 Regional Entity

4.2. The following are exempt from Standard CIP-005-4a:

4.2.1 Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.3 Responsible Entities that, in compliance with Standard CIP-002-4, identify that they have no Critical Cyber Assets.

4.2.4 In nuclear plants, the systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F. R. Section 73.54.

5. Effective Date: The first day of the eighth calendar quarter after applicable regulatory approvals have been received (or the Reliability Standard otherwise becomes effective the first day of the ninth calendar quarter after BOT adoption in those jurisdictions where regulatory approval is not required).

B. Requirements

R1. Electronic Security Perimeter — The Responsible Entity shall ensure that every Critical Cyber Asset resides within an Electronic Security Perimeter. The Responsible Entity shall identify and document the Electronic Security Perimeter(s) and all access points to the perimeter(s).

R1.1. Access points to the Electronic Security Perimeter(s) shall include any externally connected communication end point (for example, dial-up modems) terminating at any device within the Electronic Security Perimeter(s).

R1.2. For a dial-up accessible Critical Cyber Asset that uses a non-routable protocol, the Responsible Entity shall define an Electronic Security Perimeter for that single access point at the dial-up device.

R1.3. Communication links connecting discrete Electronic Security Perimeters shall not be considered part of the Electronic Security Perimeter. However, end points of these communication links within the Electronic Security Perimeter(s) shall be considered access points to the Electronic Security Perimeter(s).

R1.4. Any non-critical Cyber Asset within a defined Electronic Security Perimeter shall be identified and protected pursuant to the requirements of Standard CIP-005-4a.

R1.5. Cyber Assets used in the access control and/or monitoring of the Electronic Security Perimeter(s) shall be afforded the protective measures as a specified in Standard CIP-003-4; Standard CIP-004-4 Requirement R3; Standard CIP-005-4a Requirements R2 and R3; Standard CIP-006-4c Requirement R3; Standard CIP-007-4 Requirements R1 and R3 through R9; Standard CIP-008-4; and Standard CIP-009-4.

R1.6. The Responsible Entity shall maintain documentation of Electronic Security Perimeter(s), all interconnected Critical and non-critical Cyber Assets within the Electronic Security Perimeter(s), all electronic access points to the Electronic Security Perimeter(s) and the Cyber Assets deployed for the access control and monitoring of these access points.

R2. Electronic Access Controls — The Responsible Entity shall implement and document the organizational processes and technical and procedural mechanisms for control of electronic access at all electronic access points to the Electronic Security Perimeter(s).

R2.1. These processes and mechanisms shall use an access control model that denies access by default, such that explicit access permissions must be specified.

R2.2. At all access points to the Electronic Security Perimeter(s), the Responsible Entity shall enable only ports and services required for operations and for monitoring Cyber Assets within the Electronic Security Perimeter, and shall document, individually or by specified grouping, the configuration of those ports and services.

R2.3. The Responsible Entity shall implement and maintain a procedure for securing dial-up access to the Electronic Security Perimeter(s).

R2.4. Where external interactive access into the Electronic Security Perimeter has been enabled, the Responsible Entity shall implement strong procedural or technical controls at the access points to ensure authenticity of the accessing party, where technically feasible.

R2.5. The required documentation shall, at least, identify and describe:

R2.5.1. The processes for access request and authorization.

R2.5.2. The authentication methods.

R2.5.3. The review process for authorization rights, in accordance with Standard CIP-004-4 Requirement R4.

R2.5.4. The controls used to secure dial-up accessible connections.

R2.6. Appropriate Use Banner — Where technically feasible, electronic access control devices shall display an appropriate use banner on the user screen upon all interactive access attempts. The Responsible Entity shall maintain a document identifying the content of the banner.

R3. Monitoring Electronic Access — The Responsible Entity shall implement and document an electronic or manual process(es) for monitoring and logging access at access points to the Electronic Security Perimeter(s) twenty-four hours a day, seven days a week.

R3.1. For dial-up accessible Critical Cyber Assets that use non-routable protocols, the Responsible Entity shall implement and document monitoring process(es) at each access point to the dial-up device, where technically feasible.

R3.2. Where technically feasible, the security monitoring process(es) shall detect and alert for attempts at or actual unauthorized accesses. These alerts shall provide for appropriate notification to designated response personnel. Where alerting is not technically feasible, the Responsible Entity shall review or otherwise assess access logs for attempts at or actual unauthorized accesses at least every ninety calendar days.

R4. Cyber Vulnerability Assessment — The Responsible Entity shall perform a cyber vulnerability assessment of the electronic access points to the Electronic Security Perimeter(s) at least annually. The vulnerability assessment shall include, at a minimum, the following:

R4.1. A document identifying the vulnerability assessment process;

R4.2. A review to verify that only ports and services required for operations at these access points are enabled;

R4.3. The discovery of all access points to the Electronic Security Perimeter;

R4.4. A review of controls for default accounts, passwords, and network management community strings;

R4.5. Documentation of the results of the assessment, the action plan to remediate or mitigate vulnerabilities identified in the assessment, and the execution status of that action plan.

R5. Documentation Review and Maintenance — The Responsible Entity shall review, update, and maintain all documentation to support compliance with the requirements of Standard CIP-005-4a.

R5.1. The Responsible Entity shall ensure that all documentation required by Standard CIP-005-4a reflect current configurations and processes and shall review the documents and procedures referenced in Standard CIP-005-4a at least annually.

R5.2. The Responsible Entity shall update the documentation to reflect the modification of the network or controls within ninety calendar days of the change.

R5.3. The Responsible Entity shall retain electronic access logs for at least ninety calendar days. Logs related to reportable incidents shall be kept in accordance with the requirements of Standard CIP-008-4.

C. Measures

M1. The Responsible Entity shall make available documentation about the Electronic Security Perimeter as specified in Requirement R1.

M2. The Responsible Entity shall make available documentation of the electronic access controls to the Electronic Security Perimeter(s), as specified in Requirement R2.

M3. The Responsible Entity shall make available documentation of controls implemented to log and monitor access to the Electronic Security Perimeter(s) as specified in Requirement R3.

M4. The Responsible Entity shall make available documentation of its annual vulnerability assessment as specified in Requirement R4.

M5. The Responsible Entity shall make available access logs and documentation of review, changes, and log retention as specified in Requirement R5.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

1.2. The RE shall serve as the CEA with the following exceptions:

1.2.1 For entities that do not work for the Regional Entity, the Regional Entity shall serve as the Compliance Enforcement Authority.

1.2.2 For Reliability Coordinators and other functional entities that work for their Regional Entity, the ERO shall serve as the Compliance Enforcement Authority.

1.2.3 For Responsible Entities that are also Regional Entities, the ERO or a Regional Entity approved by the ERO and FERC or other applicable governmental authorities shall serve as the Compliance Enforcement Authority.

1.2.4 For the ERO, a third-party monitor without vested interest in the outcome for the ERO shall serve as the Compliance Enforcement Authority.

1.3. Compliance Monitoring and Enforcement Processes

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints

1.4. Data Retention

1.4.1 The Responsible Entity shall keep logs for a minimum of ninety calendar days, unless: a) longer retention is required pursuant to Standard CIP-008-4, Requirement R2; b) directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

1.4.2 The Responsible Entity shall keep other documents and records required by Standard CIP-005-4a from the previous full calendar year.

1.4.3 The Compliance Enforcement Authority in conjunction with the Registered Entity shall keep the last audit records and all requested and submitted subsequent audit records.

1.5. Additional Compliance Information

2. Violation Severity Levels (Developed separately.)

E. Regional Variances

None identified.

Version History

Version	Date	Action	Change Tracking
1	01/16/06	D.2.3.1 — Change “Critical Assets,” to “Critical Cyber Assets” as intended.	03/24/06
2	Approved by NERC Board of	Modifications to clarify the requirements and to bring the compliance elements into	Revised.

	Trustees 5/6/09	conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Revised the wording of the Electronic Access Controls requirement stated in R2.3 to clarify that the Responsible Entity shall "implement and maintain" a procedure for securing dial-up access to the Electronic Security Perimeter(s). Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Approved by the NERC Board of Trustees Changed CIP-005-2 to CIP-005-3. Changed all references to CIP Version "2" standards to CIP Version "3" standards. For Violation Severity Levels, changed, "To be developed later" to "Developed separately."	Conforming revisions for FERC Order on CIP V2 Standards (9/30/2009)
2a	02/16/10	Added Appendix 1 — Interpretation of R1.3 approved by BOT on February 16, 2010.	Addition
4a	01/24/2011	Approved by the NERC Board of Trustees	Update to conform to changes to CIP-002-4 (Project 2008-06) Update version number from "3" to "4a"

Appendix 1

Requirement Number and Text of Requirement
Section 4.2.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters. **Requirement R1.3** Communication links connecting discrete Electronic Security Perimeters shall not be considered part of the Electronic Security Perimeter. However, end points of these communication links within the Electronic Security Perimeter(s) shall be considered access points to the Electronic Security Perimeter(s).
Question 1 (Section 4.2.2)
What kind of cyber assets are referenced in 4.2.2 as "associated"? What else could be meant except the devices forming the communication link?
Response to Question 1
In the context of applicability, associated Cyber Assets refer to any communications devices external to the Electronic Security Perimeter, i.e., beyond the point at which access to the Electronic Security Perimeter is controlled. Devices controlling access into the Electronic Security Perimeter are not exempt.
Question 2 (Section 4.2.2)
Is the communication link physical or logical? Where does it begin and terminate?
Response to Question 2
The drafting team interprets the data communication link to be physical or logical, and its termination points depend upon the design and architecture of the communication link.
Question 3 (Requirement R1.3)
Please clarify what is meant by an “endpoint”? Is it physical termination? Logical termination of OSI layer 2, layer 3, or above?
Response to Question 3
The drafting team interprets the endpoint to mean the device at which a physical or logical communication link terminates. The endpoint is the Electronic Security Perimeter access point if access into the Electronic Security Perimeter is controlled at the endpoint, irrespective of which Open Systems Interconnection (OSI) layer is managing the communication.
Question 4 (Requirement R1.3)
If “endpoint” is defined as logical and refers to layer 3 and above, please clarify if the termination points of an encrypted tunnel (layer 3) must be treated as an “access point? If two control centers are

owned and managed by the same entity, connected via an encrypted link by properly applied Federal Information Processing Standards, with tunnel termination points that are within the control center ESPs and PSPs and do not terminate on the firewall but on a separate internal device, and the encrypted traffic already passes through a firewall access point at each ESP boundary where port/protocol restrictions are applied, must these encrypted communication tunnel termination points be treated as "access points" in addition to the firewalls through which the encrypted traffic has already passed?
Response to Question 4
In the case where the “endpoint” is defined as logical and is >= layer 3, the termination points of an encrypted tunnel must be treated as an “access point.” The encrypted communication tunnel termination points referred to above are “access points.”

A. Introduction

1. Title: Cyber Security — Electronic Security Perimeter(s)

2. Number: CIP-005-~~3~~4a

3. Purpose: Standard CIP-005-~~3~~4a requires the identification and protection of the Electronic Security Perimeter(s) inside which all Critical Cyber Assets reside, as well as all access points on the perimeter. Standard CIP-005-~~3~~4a should be read as part of a group of standards numbered Standards CIP-002-~~3~~4 through CIP-009-~~3~~4.

4. Applicability

4.1. Within the text of Standard CIP-005-~~3~~4a, "Responsible Entity" shall mean:

4.1.1 Reliability Coordinator.

4.1.2 Balancing Authority.

4.1.3 Interchange Authority.

4.1.4 Transmission Service Provider.

4.1.5 Transmission Owner.

4.1.6 Transmission Operator.

4.1.7 Generator Owner.

4.1.8 Generator Operator.

4.1.9 Load Serving Entity.

4.1.10 NERC.

4.1.11 Regional Entity

4.2. The following are exempt from Standard CIP-005-~~3~~4a:

4.2.1 Facilities regulated by ~~the U.S. Nuclear Regulatory Commission or~~ the Canadian Nuclear Safety Commission.

4.2.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.3 Responsible Entities that, in compliance with Standard CIP-002-~~3~~4, identify that they have no Critical Cyber Assets.

4.2.4 In nuclear plants, the systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F. R. Section 73.54.

5. Effective Date: The first day of the ~~third~~eighth calendar quarter after applicable regulatory approvals have been received (or the Reliability Standard otherwise becomes effective the first day of the ninth calendar quarter after BOT adoption in those jurisdictions where regulatory approval is not required).

B. Requirements

R1. Electronic Security Perimeter — The Responsible Entity shall ensure that every Critical Cyber Asset resides within an Electronic Security Perimeter. The Responsible Entity shall identify and document the Electronic Security Perimeter(s) and all access points to the perimeter(s).

R1.1. Access points to the Electronic Security Perimeter(s) shall include any externally connected communication end point (for example, dial-up modems) terminating at any device within the Electronic Security Perimeter(s).

R1.2. For a dial-up accessible Critical Cyber Asset that uses a non-routable protocol, the Responsible Entity shall define an Electronic Security Perimeter for that single access point at the dial-up device.

R1.3. Communication links connecting discrete Electronic Security Perimeters shall not be considered part of the Electronic Security Perimeter. However, end points of these communication links within the Electronic Security Perimeter(s) shall be considered access points to the Electronic Security Perimeter(s).

R1.4. Any non-critical Cyber Asset within a defined Electronic Security Perimeter shall be identified and protected pursuant to the requirements of Standard CIP-005-~~3~~4a.

R1.5. Cyber Assets used in the access control and/or monitoring of the Electronic Security Perimeter(s) shall be afforded the protective measures as a specified in Standard CIP-003-~~3~~4; Standard CIP-004-~~3~~4 Requirement R3; Standard CIP-005-~~3~~4a Requirements R2 and R3; Standard CIP-006-~~3~~4c Requirement R3; Standard CIP-007-~~3~~4 Requirements R1 and R3 through R9; Standard CIP-008-~~3~~4; and Standard CIP-009-~~3~~4.

R1.6. The Responsible Entity shall maintain documentation of Electronic Security Perimeter(s), all interconnected Critical and non-critical Cyber Assets within the Electronic Security Perimeter(s), all electronic access points to the Electronic Security Perimeter(s) and the Cyber Assets deployed for the access control and monitoring of these access points.

R2. Electronic Access Controls — The Responsible Entity shall implement and document the organizational processes and technical and procedural mechanisms for control of electronic access at all electronic access points to the Electronic Security Perimeter(s).

R2.1. These processes and mechanisms shall use an access control model that denies access by default, such that explicit access permissions must be specified.

R2.2. At all access points to the Electronic Security Perimeter(s), the Responsible Entity shall enable only ports and services required for operations and for monitoring Cyber Assets within the Electronic Security Perimeter, and shall document, individually or by specified grouping, the configuration of those ports and services.

R2.3. The Responsible Entity shall implement and maintain a procedure for securing dial-up access to the Electronic Security Perimeter(s).

R2.4. Where external interactive access into the Electronic Security Perimeter has been enabled, the Responsible Entity shall implement strong procedural or technical controls at the access points to ensure authenticity of the accessing party, where technically feasible.

R2.5. The required documentation shall, at least, identify and describe:

R2.5.1. The processes for access request and authorization.

R2.5.2. The authentication methods.

R2.5.3. The review process for authorization rights, in accordance with Standard CIP-004-~~3~~4 Requirement R4.

R2.5.4. The controls used to secure dial-up accessible connections.

R2.6. Appropriate Use Banner — Where technically feasible, electronic access control devices shall display an appropriate use banner on the user screen upon all interactive access attempts. The Responsible Entity shall maintain a document identifying the content of the banner.

R3. Monitoring Electronic Access — The Responsible Entity shall implement and document an electronic or manual process(es) for monitoring and logging access at access points to the Electronic Security Perimeter(s) twenty-four hours a day, seven days a week.

R3.1. For dial-up accessible Critical Cyber Assets that use non-routable protocols, the Responsible Entity shall implement and document monitoring process(es) at each access point to the dial-up device, where technically feasible.

R3.2. Where technically feasible, the security monitoring process(es) shall detect and alert for attempts at or actual unauthorized accesses. These alerts shall provide for appropriate notification to designated response personnel. Where alerting is not technically feasible, the Responsible Entity shall review or otherwise assess access logs for attempts at or actual unauthorized accesses at least every ninety calendar days.

R4. Cyber Vulnerability Assessment — The Responsible Entity shall perform a cyber vulnerability assessment of the electronic access points to the Electronic Security Perimeter(s) at least annually. The vulnerability assessment shall include, at a minimum, the following:

R4.1. A document identifying the vulnerability assessment process;

R4.2. A review to verify that only ports and services required for operations at these access points are enabled;

R4.3. The discovery of all access points to the Electronic Security Perimeter;

R4.4. A review of controls for default accounts, passwords, and network management community strings;

R4.5. Documentation of the results of the assessment, the action plan to remediate or mitigate vulnerabilities identified in the assessment, and the execution status of that action plan.

R5. Documentation Review and Maintenance — The Responsible Entity shall review, update, and maintain all documentation to support compliance with the requirements of Standard CIP-005-~~3~~4a.

R5.1. The Responsible Entity shall ensure that all documentation required by Standard CIP-005-~~3~~4a reflect current configurations and processes and shall review the documents and procedures referenced in Standard CIP-005-~~3~~4a at least annually.

R5.2. The Responsible Entity shall update the documentation to reflect the modification of the network or controls within ninety calendar days of the change.

R5.3. The Responsible Entity shall retain electronic access logs for at least ninety calendar days. Logs related to reportable incidents shall be kept in accordance with the requirements of Standard CIP-008-~~3~~4.

C. Measures

M1. The Responsible Entity shall make available documentation about the Electronic Security Perimeter as specified in Requirement R1.

M2. The Responsible Entity shall make available documentation of the electronic access controls to the Electronic Security Perimeter(s), as specified in Requirement R2.

M3. The Responsible Entity shall make available documentation of controls implemented to log and monitor access to the Electronic Security Perimeter(s) as specified in Requirement R3.

M4. The Responsible Entity shall make available documentation of its annual vulnerability assessment as specified in Requirement R4.

M5. The Responsible Entity shall make available access logs and documentation of review, changes, and log retention as specified in Requirement R5.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

1.2. The RE shall serve as the CEA with the following exceptions:

1.2.1 For entities that do not work for the Regional Entity for Responsible Entities that do not perform delegated tasks, the Regional Entity shall serve as the Compliance Enforcement Authority.

1.1.11.2.2 For Reliability Coordinators and other functional entities that work for their Regional Entity, the ERO shall serve as the Compliance Enforcement Authority.

1.1.2 ERO for Regional Entity.

1.2.3 ThirdFor Responsible Entities that are also Regional Entities, the ERO or a Regional Entity approved by the ERO and FERC or other applicable governmental authorities shall serve as the Compliance Enforcement Authority.

1.1.3 For the ERO, a third-party monitor without vested interest in the outcome for NERC.

1.2. the ERO shall serve as the Compliance **Monitoring Period and Reset Time Frame**

1.2.4 Not applicableEnforcement Authority.

1.3. Compliance Monitoring and Enforcement Processes

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints

1.4. Data Retention

1.4.1 The Responsible Entity shall keep logs for a minimum of ninety calendar days, unless: a) longer retention is required pursuant to Standard CIP-008-34, Requirement R2; b) directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

1.4.2 The Responsible Entity shall keep other documents and records required by Standard CIP-005-34a from the previous full calendar year.

1.4.3 The Compliance Enforcement Authority in conjunction with the Registered Entity shall keep the last audit records and all requested and submitted subsequent audit records.

1.5. Additional Compliance Information

2. Violation Severity Levels (To be developed laterDeveloped separately.)

E. Regional Variances

None identified.

Version History

Version	Date	Action	Change Tracking
1	01/16/06	D.2.3.1 — Change "Critical Assets," to "Critical Cyber Assets" as intended.	03/24/06
2	Approved by NERC Board of Trustees 5/6/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Revised the wording of the Electronic Access Controls requirement stated in R2.3 to clarify that the Responsible Entity shall "implement and maintain" a procedure for securing dial-up access to the Electronic Security Perimeter(s). Changed compliance monitor to Compliance Enforcement Authority.	Revised.
3	12/16/09	~~Update version from~~ Approved by the NERC Board of Trustees Changed CIP-005-2 to CIP-005-3. Changed all references to CIP Version "2" standards to CIP Version "3" standards. For Violation Severity Levels, changed, "To be developed later" to "Developed separately."	Conforming revisions for FERC Order on CIP V2 Standards (9/30/2009)
2a	02/16/10	Added Appendix 1 — Interpretation of R1.3 approved by BOT on February 16, 2010.	Addition
~~3~~4a	01/24/2011~~12/16/09~~	Approved by the NERC Board of Trustees	~~Update~~Update to conform to changes to CIP-002-4 (Project 2008-06) Update version number from "3" to "4a"

Appendix 1

Requirement Number and Text of Requirement
Section 4.2.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters. **Requirement R1.3** Communication links connecting discrete Electronic Security Perimeters shall not be considered part of the Electronic Security Perimeter. However, end points of these communication links within the Electronic Security Perimeter(s) shall be considered access points to the Electronic Security Perimeter(s).
Question 1 (Section 4.2.2)
What kind of cyber assets are referenced in 4.2.2 as "associated"? What else could be meant except the devices forming the communication link?
Response to Question 1
In the context of applicability, associated Cyber Assets refer to any communications devices external to the Electronic Security Perimeter, i.e., beyond the point at which access to the Electronic Security Perimeter is controlled. Devices controlling access into the Electronic Security Perimeter are not exempt.
Question 2 (Section 4.2.2)
Is the communication link physical or logical? Where does it begin and terminate?
Response to Question 2
The drafting team interprets the data communication link to be physical or logical, and its termination points depend upon the design and architecture of the communication link.
Question 3 (Requirement R1.3)
Please clarify what is meant by an “endpoint”? Is it physical termination? Logical termination of OSI layer 2, layer 3, or above?
Response to Question 3
The drafting team interprets the endpoint to mean the device at which a physical or logical communication link terminates. The endpoint is the Electronic Security Perimeter access point if access into the Electronic Security Perimeter is controlled at the endpoint, irrespective of which Open Systems Interconnection (OSI) layer is managing the communication.
Question 4 (Requirement R1.3)
If “endpoint” is defined as logical and refers to layer 3 and above, please clarify if the termination points of an encrypted tunnel (layer 3) must be treated as an “access point? If two control centers are

owned and managed by the same entity, connected via an encrypted link by properly applied Federal Information Processing Standards, with tunnel termination points that are within the control center ESPs and PSPs and do not terminate on the firewall but on a separate internal device, and the encrypted traffic already passes through a firewall access point at each ESP boundary where port/protocol restrictions are applied, must these encrypted communication tunnel termination points be treated as "access points" in addition to the firewalls through which the encrypted traffic has already passed?
Response to Question 4
In the case where the “endpoint” is defined as logical and is >= layer 3, the termination points of an encrypted tunnel must be treated as an “access point.” The encrypted communication tunnel termination points referred to above are “access points.”

Corrected CIP-006-4c Clean and Redline

A. Introduction

1. Title: Cyber Security — Physical Security of Critical Cyber Assets

2. Number: CIP-006-4c

3. Purpose: Standard CIP-006-4c is intended to ensure the implementation of a physical security program for the protection of Critical Cyber Assets. Standard CIP-006-4c should be read as part of a group of standards numbered Standards CIP-002-4 through CIP-009-4.

4. Applicability:

4.1. Within the text of Standard CIP-006-4c, "Responsible Entity" shall mean:

4.1.1 Reliability Coordinator

4.1.2 Balancing Authority

4.1.3 Interchange Authority

4.1.4 Transmission Service Provider

4.1.5 Transmission Owner

4.1.6 Transmission Operator

4.1.7 Generator Owner

4.1.8 Generator Operator

4.1.9 Load Serving Entity

4.1.10 NERC

4.1.11 Regional Entity

4.2. The following are exempt from Standard CIP-006-4c:

4.2.1 Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.3 In nuclear plants, the systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F. R. Section 73.54

4.2.4 Responsible Entities that, in compliance with Standard CIP-002-4, identify that they have no Critical Cyber Assets

5. Effective Date: The first day of the eighth calendar quarter after applicable regulatory approvals have been received (or the Reliability Standard otherwise becomes effective the first day of the ninth calendar quarter after BOT adoption in those jurisdictions where regulatory approval is not required).

B. Requirements

R1. Physical Security Plan — The Responsible Entity shall document, implement, and maintain a physical security plan, approved by the senior manager or delegate(s) that shall address, at a minimum, the following:

R1.1. All Cyber Assets within an Electronic Security Perimeter shall reside within an identified Physical Security Perimeter. Where a completely enclosed ("six-wall") border cannot be established, the Responsible Entity shall deploy and document alternative measures to control physical access to such Cyber Assets.

R1.2. Identification of all physical access points through each Physical Security Perimeter and measures to control entry at those access points.

R1.3. Processes, tools, and procedures to monitor physical access to the perimeter(s).

R1.4. Appropriate use of physical access controls as described in Requirement R4 including visitor pass management, response to loss, and prohibition of inappropriate use of physical access controls.

R1.5. Review of access authorization requests and revocation of access authorization, in accordance with CIP-004-4 Requirement R4.

R1.6. A visitor control program for visitors (personnel without authorized unescorted access to a Physical Security Perimeter), containing at a minimum the following:

R1.6.1. Logs (manual or automated) to document the entry and exit of visitors, including the date and time, to and from Physical Security Perimeters.

R1.6.2. Continuous escorted access of visitors within the Physical Security Perimeter.

R1.7. Update of the physical security plan within thirty calendar days of the completion of any physical security system redesign or reconfiguration, including, but not limited to, addition or removal of access points through the Physical Security Perimeter, physical access controls, monitoring controls, or logging controls.

R1.8. Annual review of the physical security plan.

R2. Protection of Physical Access Control Systems — Cyber Assets that authorize and/or log access to the Physical Security Perimeter(s), exclusive of hardware at the Physical Security Perimeter access point such as electronic lock control mechanisms and badge readers, shall:

R2.1. Be protected from unauthorized physical access.

R2.2. Be afforded the protective measures specified in Standard CIP-003-4; Standard CIP-004-4 Requirement R3; Standard CIP-005-4a Requirements R2 and R3; Standard CIP-006-4c Requirements R4 and R5; Standard CIP-007-4; Standard CIP-008-4; and Standard CIP-009-4.

R3. Protection of Electronic Access Control Systems — Cyber Assets used in the access control and/or monitoring of the Electronic Security Perimeter(s) shall reside within an identified Physical Security Perimeter.

R4. Physical Access Controls — The Responsible Entity shall document and implement the operational and procedural controls to manage physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week. The Responsible Entity shall implement one or more of the following physical access methods:

- Card Key: A means of electronic access where the access rights of the card holder are predefined in a computer database. Access rights may differ from one perimeter to another.
- Special Locks: These include, but are not limited to, locks with "restricted key" systems, magnetic locks that can be operated remotely, and "man-trap" systems.
- Security Personnel: Personnel responsible for controlling physical access who may reside on-site or at a monitoring station.
- Other Authentication Devices: Biometric, keypad, token, or other equivalent devices that control physical access to the Critical Cyber Assets.

R5. Monitoring Physical Access — The Responsible Entity shall document and implement the technical and procedural controls for monitoring physical access at all access points to the

Physical Security Perimeter(s) twenty-four hours a day, seven days a week. Unauthorized access attempts shall be reviewed immediately and handled in accordance with the procedures specified in Requirement CIP-008-4. One or more of the following monitoring methods shall be used:

- Alarm Systems: Systems that alarm to indicate a door, gate or window has been opened without authorization. These alarms must provide for immediate notification to personnel responsible for response.
- Human Observation of Access Points: Monitoring of physical access points by authorized personnel as specified in Requirement R4.

R6. Logging Physical Access — Logging shall record sufficient information to uniquely identify individuals and the time of access twenty-four hours a day, seven days a week. The Responsible Entity shall implement and document the technical and procedural mechanisms for logging physical entry at all access points to the Physical Security Perimeter(s) using one or more of the following logging methods or their equivalent:

- Computerized Logging: Electronic logs produced by the Responsible Entity's selected access control and monitoring method.
- Video Recording: Electronic capture of video images of sufficient quality to determine identity.
- Manual Logging: A log book or sign-in sheet, or other record of physical access maintained by security or other personnel authorized to control and monitor physical access as specified in Requirement R4.

R7. Access Log Retention — The Responsible Entity shall retain physical access logs for at least ninety calendar days. Logs related to reportable incidents shall be kept in accordance with the requirements of Standard CIP-008-4.

R8. Maintenance and Testing — The Responsible Entity shall implement a maintenance and testing program to ensure that all physical security systems under Requirements R4, R5, and R6 function properly. The program must include, at a minimum, the following:

R8.1. Testing and maintenance of all physical security mechanisms on a cycle no longer than three years.

R8.2. Retention of testing and maintenance records for the cycle determined by the Responsible Entity in Requirement R8.1.

R8.3. Retention of outage records regarding access controls, logging, and monitoring for a minimum of one calendar year.

C. Measures

M1. The Responsible Entity shall make available the physical security plan as specified in Requirement R1 and documentation of the implementation, review and updating of the plan.

M2. The Responsible Entity shall make available documentation that the physical access control systems are protected as specified in Requirement R2.

M3. The Responsible Entity shall make available documentation that the electronic access control systems are located within an identified Physical Security Perimeter as specified in Requirement R3.

M4. The Responsible Entity shall make available documentation identifying the methods for controlling physical access to each access point of a Physical Security Perimeter as specified in Requirement R4.

M5. The Responsible Entity shall make available documentation identifying the methods for monitoring physical access as specified in Requirement R5.

M6. The Responsible Entity shall make available documentation identifying the methods for logging physical access as specified in Requirement R6.

M7. The Responsible Entity shall make available documentation to show retention of access logs as specified in Requirement R7.

M8. The Responsible Entity shall make available documentation to show its implementation of a physical security system maintenance and testing program as specified in Requirement R8.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

1.2. The RE shall serve as the CEA with the following exceptions:

1.2.1 For entities that do not work for the Regional Entity, the Regional Entity shall serve as the Compliance Enforcement Authority.

1.2.2 For Reliability Coordinators and other functional entities that work for their Regional Entity, the ERO shall serve as the Compliance Enforcement Authority.

1.2.3 For Responsible Entities that are also Regional Entities, the ERO or a Regional Entity approved by the ERO and FERC or other applicable governmental authorities shall serve as the Compliance Enforcement Authority.

1.2.4 For the ERO, a third-party monitor without vested interest in the outcome for the ERO shall serve as the Compliance Enforcement Authority.

1.3. Compliance Monitoring and Enforcement Processes

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints

1.4. Data Retention

1.4.1 The Responsible Entity shall keep documents other than those specified in Requirements R7 and R8.2 from the previous full calendar year unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

1.4.2 The Compliance Enforcement Authority in conjunction with the Registered Entity shall keep the last audit records and all requested and submitted subsequent audit records.

1.5. Additional Compliance Information

1.5.1 The Responsible Entity may not make exceptions in its cyber security policy to the creation, documentation, or maintenance of a physical security plan.

1.5.2 For dial-up accessible Critical Cyber Assets that use non-routable protocols, the Responsible Entity shall not be required to comply with Standard CIP-006-4c for that single access point at the dial-up device.

2. Violation Severity Levels (Under development by the CIP VSL Drafting Team)

E. Regional Variances

None identified.

Version History

Version	Date	Action	Change Tracking
2		Modifications to remove extraneous information from the requirements, improve readability, and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Replaced the RRO with RE as a responsible entity. Modified CIP-006-1 Requirement R1 to clarify that a physical security plan to protect Critical Cyber Assets must be documented, maintained, implemented, and approved by the senior manager. Revised the wording in R1.2 to identify all "physical" access points. Added Requirement R2 to CIP-006-2 to clarify the requirement to safeguard the Physical Access Control Systems and exclude hardware at the Physical Security Perimeter access point, such as electronic lock control mechanisms and badge readers from the requirement. Requirement R2.1 requires the Responsible Entity to protect the Physical Access Control Systems from unauthorized access. CIP-006-1 Requirement R1.8 was moved to become CIP-006-2 Requirement R2.2. Added Requirement R3 to CIP-006-2, clarifying the requirement for Electronic Access Control Systems to be safeguarded within an identified Physical Security Perimeter. The sub requirements of CIP-006-2 Requirements R4, R5, and R6 were changed from formal requirements to bulleted lists of options consistent with the intent of the requirements. Changed the Compliance Monitor to Compliance Enforcement Authority.	
3		Updated version numbers from -2 to -3 Revised Requirement 1.6 to add a Visitor Control program component to the Physical Security Plan, in response to FERC order issued September 30, 2009. In Requirement R7, the term "Responsible Entity" was capitalized.	
	11/18/2009	Updated Requirements R1.6.1 and R1.6.2 to be responsive to FERC Order RD09-7	
3	12/16/09	Approved by NERC Board of Trustees	Update
1a	2/12/2008	Approved by NERC Board of Trustees Interpretation of R1 and Additional Compliance	Interpretation (Project 2007-27)

		Information Section 1.4.4 (Appendix 1)	
1b/2b	08/05/2009	Approved by NERC Board of Trustees Interpretation of R4 (Appendix 2)	Interpretation (Project 2008-15)
3c	02/16/2010	Approved by the NERC Board of Trustees Interpretation of R1 and R1.1 (Appendix 3)	Interpretation (Project 2009-13)
4c	01/24/2011	Approved by the NERC Board of Trustees Update version number from “3” to “4c”	Update to conform to changes to CIP-002-4 (Project 2008-06)

Appendix 1

Interpretation of Requirement R1.1.

Request: *Are dial-up RTUs that use non-routable protocols and have dial-up access required to have a six-wall perimeters or are they exempted from CIP-006-1 and required to have only electronic security perimeters? This has a direct impact on how any identified RTUs will be physically secured.*

Interpretation:

Dial-up assets are Critical Cyber Assets, assuming they meet the criteria in CIP-002-1, and they must reside within an Electronic Security Perimeter. However, physical security control over a critical cyber asset is not required if that asset does not have a routable protocol. Since there is minimal risk of compromising other critical cyber assets dial-up devices such as Remote Terminals Units that do not use routable protocols are not required to be enclosed within a "six-wall" border.

CIP-006-1 — Requirement 1.1 requires a Responsible Entity to have a physical security plan that stipulate cyber assets that are within the Electronic Security Perimeter also be within a Physical Security Perimeter.

R1. Physical Security Plan — The Responsible Entity shall create and maintain a physical security plan, approved by a senior manager or delegate(s) that shall address, at a minimum, the following:

R1.1. Processes to ensure and document that all Cyber Assets within an Electronic Security Perimeter also reside within an identified Physical Security Perimeter. Where a completely enclosed ("six-wall") border cannot be established, the Responsible Entity shall deploy and document alternative measures to control physical access to the Critical Cyber Assets.

CIP-006-1 — Additional Compliance Information 1.4.4 identifies dial-up accessible assets that use non-routable protocols as a special class of cyber assets that are not subject to the Physical Security Perimeter requirement of this standard.

1.4. Additional Compliance Information

1.4.4 For dial-up accessible Critical Cyber Assets that use non-routable protocols, the Responsible Entity shall not be required to comply with Standard CIP-006 for that single access point at the dial-up device.

Appendix 2

The following interpretation of CIP-006-1a — Cyber Security — Physical Security of Critical Cyber Assets, Requirement R4 was developed by the standard drafting team assigned to Project 2008-14 (Cyber Security Violation Severity Levels) on October 23, 2008.

Request:

1. *For physical access control to cyber assets, does this include monitoring when an individual leaves the controlled access cyber area?*
2. *Does the term, "time of access" mean logging when the person entered the facility or does it mean logging the entry/exit time and "length" of time the person had access to the critical asset?*

Interpretation:

No, monitoring and logging of access are only required for ingress at this time. The term "time of access" refers to the time an authorized individual enters the physical security perimeter.

Requirement Number and Text of Requirement

R4. Logging Physical Access — Logging shall record sufficient information to uniquely identify individuals and the time of access twenty-four hours a day, seven days a week. The Responsible Entity shall implement and document the technical and procedural mechanisms for logging physical entry at all access points to the Physical Security Perimeter(s) using one or more of the following logging methods or their equivalent:

R4.1. Computerized Logging: Electronic logs produced by the Responsible Entity's selected access control and monitoring method.

R4.2. Video Recording: Electronic capture of video images of sufficient quality to determine identity.

R4.3. Manual Logging: A log book or sign-in sheet, or other record of physical access maintained by security or other personnel authorized to control and monitor physical access as specified in Requirement R2.3.

Appendix 3

Requirement Number and Text of Requirement
R1. Physical Security Plan — The Responsible Entity shall create and maintain a physical security plan, approved by a senior manager or delegate(s) that shall address, at a minimum, the following: R1.1. Processes to ensure and document that all Cyber Assets within an Electronic Security Perimeter also reside within an identified Physical Security Perimeter. Where a completely enclosed ("six-wall") border cannot be established, the Responsible Entity shall deploy and document alternative measures to control physical access to the Critical Cyber Assets.
Question
If a completely enclosed border cannot be created, what does the phrase, "to control physical access" require? Must the alternative measure be physical in nature? If so, must the physical barrier literally prevent physical access e.g. using concrete encased fiber, or can the alternative measure effectively mitigate the risks associated with physical access through cameras, motions sensors, or encryption? Does this requirement preclude the application of logical controls as an alternative measure in mitigating the risks of physical access to Critical Cyber Assets?
Response
For Electronic Security Perimeter wiring external to a Physical Security Perimeter, the drafting team interprets the Requirement R1.1 as not limited to measures that are "physical in nature." The alternative measures may be physical or logical, on the condition that they provide security equivalent or better to a completely enclosed ("six-wall") border. Alternative physical control measures may include, but are not limited to, multiple physical access control layers within a non-public, controlled space. Alternative logical control measures may include, but are not limited to, data encryption and/or circuit monitoring to detect unauthorized access or physical tampering.

A. Introduction

1. Title: Cyber Security — Physical Security of Critical Cyber Assets

2. Number: CIP-006-~~3c~~4c

3. Purpose: Standard CIP-006-~~3~~4c is intended to ensure the implementation of a physical security program for the protection of Critical Cyber Assets. Standard CIP-006-~~3~~4c should be read as part of a group of standards numbered Standards CIP-002-~~3~~4 through CIP-009-~~3~~4.

4. Applicability:

4.1. Within the text of Standard CIP-006-~~3~~4c, "Responsible Entity" shall mean:

4.1.1 Reliability Coordinator

4.1.2 Balancing Authority

4.1.3 Interchange Authority

4.1.4 Transmission Service Provider

4.1.5 Transmission Owner

4.1.6 Transmission Operator

4.1.7 Generator Owner

4.1.8 Generator Operator

4.1.9 Load Serving Entity

4.1.10 NERC

4.1.11 Regional Entity

4.2. The following are exempt from Standard CIP-006-~~3~~4c:

4.2.1 Facilities regulated by ~~the U.S. Nuclear Regulatory Commission or~~ the Canadian Nuclear Safety Commission.

4.2.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.3 In nuclear plants, the systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F. R. Section 73.54

~~4.2.3~~4.2.4 Responsible Entities that, in compliance with Standard CIP-002-~~3~~4, identify that they have no Critical Cyber Assets

5. Effective Date: The first day of the ~~third~~eighth calendar quarter after applicable regulatory approvals have been received (or the Reliability Standard otherwise becomes effective the first day of the ~~third~~ninth calendar quarter after BOT adoption in those jurisdictions where regulatory approval is not required).

B. Requirements

R1. Physical Security Plan — The Responsible Entity shall document, implement, and maintain a physical security plan, approved by the senior manager or delegate(s) that shall address, at a minimum, the following:

R1.1. All Cyber Assets within an Electronic Security Perimeter shall reside within an identified Physical Security Perimeter. Where a completely enclosed ("six-wall") border cannot be established, the Responsible Entity shall deploy and document alternative measures to control physical access to such Cyber Assets.

R1.2. Identification of all physical access points through each Physical Security Perimeter and measures to control entry at those access points.

R1.3. Processes, tools, and procedures to monitor physical access to the perimeter(s).

R1.4. Appropriate use of physical access controls as described in Requirement R4 including visitor pass management, response to loss, and prohibition of inappropriate use of physical access controls.

R1.5. Review of access authorization requests and revocation of access authorization, in accordance with CIP-004-~~3~~4 Requirement R4.

R1.6. A visitor control program for visitors (personnel without authorized unescorted access to a Physical Security Perimeter), containing at a minimum the following:

R1.6.1. Logs (manual or automated) to document the entry and exit of visitors, including the date and time, to and from Physical Security Perimeters.

R1.6.2. Continuous escorted access of visitors within the Physical Security Perimeter.

R1.7. Update of the physical security plan within thirty calendar days of the completion of any physical security system redesign or reconfiguration, including, but not limited to, addition or removal of access points through the Physical Security Perimeter, physical access controls, monitoring controls, or logging controls.

R1.8. Annual review of the physical security plan.

R2. Protection of Physical Access Control Systems — Cyber Assets that authorize and/or log access to the Physical Security Perimeter(s), exclusive of hardware at the Physical Security Perimeter access point such as electronic lock control mechanisms and badge readers, shall:

R2.1. Be protected from unauthorized physical access.

R2.2. Be afforded the protective measures specified in Standard CIP-003-~~3~~4; Standard CIP-004-~~3~~4 Requirement R3; Standard CIP-005-~~3~~4a Requirements R2 and R3; Standard CIP-006-~~3~~4c Requirements R4 and R5; Standard CIP-007-~~3~~4; Standard CIP-008-~~3~~4; and Standard CIP-009-~~3~~4.

R3. Protection of Electronic Access Control Systems — Cyber Assets used in the access control and/or monitoring of the Electronic Security Perimeter(s) shall reside within an identified Physical Security Perimeter.

R4. Physical Access Controls — The Responsible Entity shall document and implement the operational and procedural controls to manage physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week. The Responsible Entity shall implement one or more of the following physical access methods:

- Card Key: A means of electronic access where the access rights of the card holder are predefined in a computer database. Access rights may differ from one perimeter to another.
- Special Locks: These include, but are not limited to, locks with "restricted key" systems, magnetic locks that can be operated remotely, and "man-trap" systems.
- Security Personnel: Personnel responsible for controlling physical access who may reside on-site or at a monitoring station.
- Other Authentication Devices: Biometric, keypad, token, or other equivalent devices that control physical access to the Critical Cyber Assets.

R5. Monitoring Physical Access — The Responsible Entity shall document and implement the technical and procedural controls for monitoring physical access at all access points to the

Physical Security Perimeter(s) twenty-four hours a day, seven days a week. Unauthorized access attempts shall be reviewed immediately and handled in accordance with the procedures specified in Requirement CIP-008-~~3~~4. One or more of the following monitoring methods shall be used:

- Alarm Systems: Systems that alarm to indicate a door, gate or window has been opened without authorization. These alarms must provide for immediate notification to personnel responsible for response.
- Human Observation of Access Points: Monitoring of physical access points by authorized personnel as specified in Requirement R4.

R6. Logging Physical Access — Logging shall record sufficient information to uniquely identify individuals and the time of access twenty-four hours a day, seven days a week. The Responsible Entity shall implement and document the technical and procedural mechanisms for logging physical entry at all access points to the Physical Security Perimeter(s) using one or more of the following logging methods or their equivalent:

- Computerized Logging: Electronic logs produced by the Responsible Entity's selected access control and monitoring method.
- Video Recording: Electronic capture of video images of sufficient quality to determine identity.
- Manual Logging: A log book or sign-in sheet, or other record of physical access maintained by security or other personnel authorized to control and monitor physical access as specified in Requirement R4.

R7. Access Log Retention — The Responsible Entity shall retain physical access logs for at least ninety calendar days. Logs related to reportable incidents shall be kept in accordance with the requirements of Standard CIP-008-~~3~~4.

R8. Maintenance and Testing — The Responsible Entity shall implement a maintenance and testing program to ensure that all physical security systems under Requirements R4, R5, and R6 function properly. The program must include, at a minimum, the following:

R8.1. Testing and maintenance of all physical security mechanisms on a cycle no longer than three years.

R8.2. Retention of testing and maintenance records for the cycle determined by the Responsible Entity in Requirement R8.1.

R8.3. Retention of outage records regarding access controls, logging, and monitoring for a minimum of one calendar year.

C. Measures

M1. The Responsible Entity shall make available the physical security plan as specified in Requirement R1 and documentation of the implementation, review and updating of the plan.

M2. The Responsible Entity shall make available documentation that the physical access control systems are protected as specified in Requirement R2.

M3. The Responsible Entity shall make available documentation that the electronic access control systems are located within an identified Physical Security Perimeter as specified in Requirement R3.

M4. The Responsible Entity shall make available documentation identifying the methods for controlling physical access to each access point of a Physical Security Perimeter as specified in Requirement R4.

M5. The Responsible Entity shall make available documentation identifying the methods for monitoring physical access as specified in Requirement R5.

M6. The Responsible Entity shall make available documentation identifying the methods for logging physical access as specified in Requirement R6.

M7. The Responsible Entity shall make available documentation to show retention of access logs as specified in Requirement R7.

M8. The Responsible Entity shall make available documentation to show its implementation of a physical security system maintenance and testing program as specified in Requirement R8.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

1.2. The RE shall serve as the CEA with the following exceptions:

1.2.1 For entities that do not work for the Regional Entity ~~for Responsible Entities that do not perform delegated tasks~~, the Regional Entity shall serve as the Compliance Enforcement Authority.

~~1.1.1~~1.2.2 For Reliability Coordinators and other functional entities that work for their Regional Entity, the ERO shall serve as the Compliance Enforcement Authority.

~~**1.1.2 ERO for Regional Entities.**~~

1.2.3 ~~Third~~For Responsible Entities that are also Regional Entities, the ERO or a Regional Entity approved by the ERO and FERC or other applicable governmental authorities shall serve as the Compliance Enforcement Authority.

~~**1.1.3**~~ For the ERO, a third-party monitor without vested interest in the outcome for ~~NERC.~~

~~**1.2.**~~ the ERO shall serve as the Compliance ~~**Monitoring Period and Reset Time Frame**~~

1.2.4 ~~Not applicable~~Enforcement Authority.

1.3. Compliance Monitoring and Enforcement Processes

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints

1.4. Data Retention

1.4.1 The Responsible Entity shall keep documents other than those specified in Requirements R7 and R8.2 from the previous full calendar year unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

1.4.2 The Compliance Enforcement Authority in conjunction with the Registered Entity shall keep the last audit records and all requested and submitted subsequent audit records.

1.5. Additional Compliance Information

1.5.1 The Responsible Entity may not make exceptions in its cyber security policy to the creation, documentation, or maintenance of a physical security plan.

1.5.2 For dial-up accessible Critical Cyber Assets that use non-routable protocols, the Responsible Entity shall not be required to comply with Standard CIP-006-~~3~~4c for that single access point at the dial-up device.

2. Violation Severity Levels (Under development by the CIP VSL Drafting Team)

E. Regional Variances

None identified.

Version History

Version	Date	Action	Change Tracking
2		Modifications to remove extraneous information from the requirements, improve readability, and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Replaced the RRO with RE as a responsible entity. Modified CIP-006-1 Requirement R1 to clarify that a physical security plan to protect Critical Cyber Assets must be documented, maintained, implemented, and approved by the senior manager. Revised the wording in R1.2 to identify all "physical" access points. Added Requirement R2 to CIP-006-2 to clarify the requirement to safeguard the Physical Access Control Systems and exclude hardware at the Physical Security Perimeter access point, such as electronic lock control mechanisms and badge readers from the requirement. Requirement R2.1 requires the Responsible Entity to protect the Physical Access Control Systems from unauthorized access. CIP-006-1 Requirement R1.8 was moved to become CIP-006-2 Requirement R2.2. Added Requirement R3 to CIP-006-2, clarifying the requirement for Electronic Access Control Systems to be safeguarded within an identified Physical Security Perimeter. The sub requirements of CIP-006-2 Requirements R4, R5, and R6 were changed from formal requirements to bulleted lists of options consistent with the intent of the requirements. Changed the Compliance Monitor to Compliance Enforcement Authority.	
3		Updated version numbers from -2 to -3 Revised Requirement 1.6 to add a Visitor Control program component to the Physical Security Plan, in response to FERC order issued September 30, 2009. In Requirement R7, the term "Responsible Entity" was	

		capitalized.	
	11/18/2009	Updated Requirements R1.6.1 and R1.6.2 to be responsive to FERC Order RD09-7	
3	12/16/09	Approved by NERC Board of Trustees	Update
1a	~~Board approved~~ ~~02~~2/12/2008	Approved by NERC Board of Trustees Interpretation of R1 and Additional Compliance Information Section 1.4.4 (Appendix 1)	Interpretation (Project 2007-27)
1b/2b	~~Board approved~~ 08/05/2009	Approved by NERC Board of Trustees Interpretation of R4 (Appendix 2)	Interpretation (Project 2008-15)
3c	~~**Board approved**~~ 02/16/2010	Approved by the NERC Board of Trustees Interpretation of R1 and R1.1 (Appendix 3)	Interpretation (Project 2009-13)
4c	01/24/2011	Approved by the NERC Board of Trustees Update version number from "3" to "4c"	Update to conform to changes to CIP-002-4 (Project 2008-06)

Appendix 1

Interpretation of Requirement R1.1.

Request: *Are dial-up RTUs that use non-routable protocols and have dial-up access required to have a six-wall perimeters or are they exempted from CIP-006-1 and required to have only electronic security perimeters? This has a direct impact on how any identified RTUs will be physically secured.*

Interpretation:

Dial-up assets are Critical Cyber Assets, assuming they meet the criteria in CIP-002-1, and they must reside within an Electronic Security Perimeter. However, physical security control over a critical cyber asset is not required if that asset does not have a routable protocol. Since there is minimal risk of compromising other critical cyber assets dial-up devices such as Remote Terminals Units that do not use routable protocols are not required to be enclosed within a "six-wall" border.

CIP-006-1 — Requirement 1.1 requires a Responsible Entity to have a physical security plan that stipulate cyber assets that are within the Electronic Security Perimeter also be within a Physical Security Perimeter.

R1. Physical Security Plan — The Responsible Entity shall create and maintain a physical security plan, approved by a senior manager or delegate(s) that shall address, at a minimum, the following:

R1.1. Processes to ensure and document that all Cyber Assets within an Electronic Security Perimeter also reside within an identified Physical Security Perimeter. Where a completely enclosed ("six-wall") border cannot be established, the Responsible Entity shall deploy and document alternative measures to control physical access to the Critical Cyber Assets.

CIP-006-1 — Additional Compliance Information 1.4.4 identifies dial-up accessible assets that use non-routable protocols as a special class of cyber assets that are not subject to the Physical Security Perimeter requirement of this standard.

1.4. Additional Compliance Information

1.4.4 For dial-up accessible Critical Cyber Assets that use non-routable protocols, the Responsible Entity shall not be required to comply with Standard CIP-006 for that single access point at the dial-up device.

Appendix 2

The following interpretation of CIP-006-1a — Cyber Security — Physical Security of Critical Cyber Assets, Requirement R4 was developed by the standard drafting team assigned to Project 2008-14 (Cyber Security Violation Severity Levels) on October 23, 2008.

Request:

1. *For physical access control to cyber assets, does this include monitoring when an individual leaves the controlled access cyber area?*
2. *Does the term, "time of access" mean logging when the person entered the facility or does it mean logging the entry/exit time and "length" of time the person had access to the critical asset?*

Interpretation:

No, monitoring and logging of access are only required for ingress at this time. The term "time of access" refers to the time an authorized individual enters the physical security perimeter.

Requirement Number and Text of Requirement

R4. Logging Physical Access — Logging shall record sufficient information to uniquely identify individuals and the time of access twenty-four hours a day, seven days a week. The Responsible Entity shall implement and document the technical and procedural mechanisms for logging physical entry at all access points to the Physical Security Perimeter(s) using one or more of the following logging methods or their equivalent:

R4.1. Computerized Logging: Electronic logs produced by the Responsible Entity's selected access control and monitoring method.

R4.2. Video Recording: Electronic capture of video images of sufficient quality to determine identity.

R4.3. Manual Logging: A log book or sign-in sheet, or other record of physical access maintained by security or other personnel authorized to control and monitor physical access as specified in Requirement R2.3.

Appendix 3

Requirement Number and Text of Requirement
R1. Physical Security Plan — The Responsible Entity shall create and maintain a physical security plan, approved by a senior manager or delegate(s) that shall address, at a minimum, the following: R1.1. Processes to ensure and document that all Cyber Assets within an Electronic Security Perimeter also reside within an identified Physical Security Perimeter. Where a completely enclosed ("six-wall") border cannot be established, the Responsible Entity shall deploy and document alternative measures to control physical access to the Critical Cyber Assets.
Question
If a completely enclosed border cannot be created, what does the phrase, "to control physical access" require? Must the alternative measure be physical in nature? If so, must the physical barrier literally prevent physical access e.g. using concrete encased fiber, or can the alternative measure effectively mitigate the risks associated with physical access through cameras, motions sensors, or encryption? Does this requirement preclude the application of logical controls as an alternative measure in mitigating the risks of physical access to Critical Cyber Assets?
Response
For Electronic Security Perimeter wiring external to a Physical Security Perimeter, the drafting team interprets the Requirement R1.1 as not limited to measures that are "physical in nature." The alternative measures may be physical or logical, on the condition that they provide security equivalent or better to a completely enclosed ("six-wall") border. Alternative physical control measures may include, but are not limited to, multiple physical access control layers within a non-public, controlled space. Alternative logical control measures may include, but are not limited to, data encryption and/or circuit monitoring to detect unauthorized access or physical tampering.

CIP-007-4 Clean and Redline

A. Introduction

1. Title: Cyber Security — Systems Security Management

2. Number: CIP-007-4

3. Purpose: Standard CIP-007-4 requires Responsible Entities to define methods, processes, and procedures for securing those systems determined to be Critical Cyber Assets, as well as the other (non-critical) Cyber Assets within the Electronic Security Perimeter(s). Standard CIP-007-4 should be read as part of a group of standards numbered Standards CIP-002-4 through CIP-009-4.

4. Applicability:

4.1. Within the text of Standard CIP-007-4, "Responsible Entity" shall mean:

4.1.1 Reliability Coordinator.

4.1.2 Balancing Authority.

4.1.3 Interchange Authority.

4.1.4 Transmission Service Provider.

4.1.5 Transmission Owner.

4.1.6 Transmission Operator.

4.1.7 Generator Owner.

4.1.8 Generator Operator.

4.1.9 Load Serving Entity.

4.1.10 NERC.

4.1.11 Regional Entity.

4.2. The following are exempt from Standard CIP-007-4:

4.2.1 Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.3 In nuclear plants, the systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F. R. Section 73.54

4.2.4 Responsible Entities that, in compliance with Standard CIP-002-4, identify that they have no Critical Cyber Assets.

5. Effective Date: The first day of the eighth calendar quarter after applicable regulatory approvals have been received (or the Reliability Standard otherwise becomes effective the first day of the ninth calendar quarter after BOT adoption in those jurisdictions where regulatory approval is not required).

B. Requirements

R1. Test Procedures — The Responsible Entity shall ensure that new Cyber Assets and significant changes to existing Cyber Assets within the Electronic Security Perimeter do not adversely affect existing cyber security controls. For purposes of Standard CIP-007-4, a significant change shall, at a minimum, include implementation of security patches, cumulative service packs, vendor releases, and version upgrades of operating systems, applications, database platforms, or other third-party software or firmware.

R1.1. The Responsible Entity shall create, implement, and maintain cyber security test procedures in a manner that minimizes adverse effects on the production system or its operation.

R1.2. The Responsible Entity shall document that testing is performed in a manner that reflects the production environment.

R1.3. The Responsible Entity shall document test results.

R2. Ports and Services — The Responsible Entity shall establish, document and implement a process to ensure that only those ports and services required for normal and emergency operations are enabled.

R2.1. The Responsible Entity shall enable only those ports and services required for normal and emergency operations.

R2.2. The Responsible Entity shall disable other ports and services, including those used for testing purposes, prior to production use of all Cyber Assets inside the Electronic Security Perimeter(s).

R2.3. In the case where unused ports and services cannot be disabled due to technical limitations, the Responsible Entity shall document compensating measure(s) applied to mitigate risk exposure.

R3. Security Patch Management — The Responsible Entity, either separately or as a component of the documented configuration management process specified in CIP-003-4 Requirement R6, shall establish, document and implement a security patch management program for tracking, evaluating, testing, and installing applicable cyber security software patches for all Cyber Assets within the Electronic Security Perimeter(s).

R3.1. The Responsible Entity shall document the assessment of security patches and security upgrades for applicability within thirty calendar days of availability of the patches or upgrades.

R3.2. The Responsible Entity shall document the implementation of security patches. In any case where the patch is not installed, the Responsible Entity shall document compensating measure(s) applied to mitigate risk exposure.

R4. Malicious Software Prevention — The Responsible Entity shall use anti-virus software and other malicious software ("malware") prevention tools, where technically feasible, to detect, prevent, deter, and mitigate the introduction, exposure, and propagation of malware on all Cyber Assets within the Electronic Security Perimeter(s).

R4.1. The Responsible Entity shall document and implement anti-virus and malware prevention tools. In the case where anti-virus software and malware prevention tools are not installed, the Responsible Entity shall document compensating measure(s) applied to mitigate risk exposure.

R4.2. The Responsible Entity shall document and implement a process for the update of anti-virus and malware prevention "signatures." The process must address testing and installing the signatures.

R5. Account Management — The Responsible Entity shall establish, implement, and document technical and procedural controls that enforce access authentication of, and accountability for, all user activity, and that minimize the risk of unauthorized system access.

R5.1. The Responsible Entity shall ensure that individual and shared system accounts and authorized access permissions are consistent with the concept of "need to know" with respect to work functions performed.

R5.1.1. The Responsible Entity shall ensure that user accounts are implemented as approved by designated personnel. Refer to Standard CIP-003-4 Requirement R5.

R5.1.2. The Responsible Entity shall establish methods, processes, and procedures that generate logs of sufficient detail to create historical audit trails of individual user account access activity for a minimum of ninety days.

R5.1.3. The Responsible Entity shall review, at least annually, user accounts to verify access privileges are in accordance with Standard CIP-003-4 Requirement R5 and Standard CIP-004-4 Requirement R4.

R5.2. The Responsible Entity shall implement a policy to minimize and manage the scope and acceptable use of administrator, shared, and other generic account privileges including factory default accounts.

R5.2.1. The policy shall include the removal, disabling, or renaming of such accounts where possible. For such accounts that must remain enabled, passwords shall be changed prior to putting any system into service.

R5.2.2. The Responsible Entity shall identify those individuals with access to shared accounts.

R5.2.3. Where such accounts must be shared, the Responsible Entity shall have a policy for managing the use of such accounts that limits access to only those with authorization, an audit trail of the account use (automated or manual), and steps for securing the account in the event of personnel changes (for example, change in assignment or termination).

R5.3. At a minimum, the Responsible Entity shall require and use passwords, subject to the following, as technically feasible:

R5.3.1. Each password shall be a minimum of six characters.

R5.3.2. Each password shall consist of a combination of alpha, numeric, and "special" characters.

R5.3.3. Each password shall be changed at least annually, or more frequently based on risk.

R6. Security Status Monitoring — The Responsible Entity shall ensure that all Cyber Assets within the Electronic Security Perimeter, as technically feasible, implement automated tools or organizational process controls to monitor system events that are related to cyber security.

R6.1. The Responsible Entity shall implement and document the organizational processes and technical and procedural mechanisms for monitoring for security events on all Cyber Assets within the Electronic Security Perimeter.

R6.2. The security monitoring controls shall issue automated or manual alerts for detected Cyber Security Incidents.

R6.3. The Responsible Entity shall maintain logs of system events related to cyber security, where technically feasible, to support incident response as required in Standard CIP-008-4.

R6.4. The Responsible Entity shall retain all logs specified in Requirement R6 for ninety calendar days.

R6.5. The Responsible Entity shall review logs of system events related to cyber security and maintain records documenting review of logs.

R7. Disposal or Redeployment — The Responsible Entity shall establish and implement formal methods, processes, and procedures for disposal or redeployment of Cyber Assets within the Electronic Security Perimeter(s) as identified and documented in Standard CIP-005-4.

R7.1. Prior to the disposal of such assets, the Responsible Entity shall destroy or erase the data storage media to prevent unauthorized retrieval of sensitive cyber security or reliability data.

R7.2. Prior to redeployment of such assets, the Responsible Entity shall, at a minimum, erase the data storage media to prevent unauthorized retrieval of sensitive cyber security or reliability data.

R7.3. The Responsible Entity shall maintain records that such assets were disposed of or redeployed in accordance with documented procedures.

R8. Cyber Vulnerability Assessment — The Responsible Entity shall perform a cyber vulnerability assessment of all Cyber Assets within the Electronic Security Perimeter at least annually. The vulnerability assessment shall include, at a minimum, the following:

R8.1. A document identifying the vulnerability assessment process;

R8.2. A review to verify that only ports and services required for operation of the Cyber Assets within the Electronic Security Perimeter are enabled;

R8.3. A review of controls for default accounts; and,

R8.4. Documentation of the results of the assessment, the action plan to remediate or mitigate vulnerabilities identified in the assessment, and the execution status of that action plan.

R9. Documentation Review and Maintenance — The Responsible Entity shall review and update the documentation specified in Standard CIP-007-4 at least annually. Changes resulting from modifications to the systems or controls shall be documented within thirty calendar days of the change being completed.

C. Measures

M1. The Responsible Entity shall make available documentation of its security test procedures as specified in Requirement R1.

M2. The Responsible Entity shall make available documentation as specified in Requirement R2.

M3. The Responsible Entity shall make available documentation and records of its security patch management program, as specified in Requirement R3.

M4. The Responsible Entity shall make available documentation and records of its malicious software prevention program as specified in Requirement R4.

M5. The Responsible Entity shall make available documentation and records of its account management program as specified in Requirement R5.

M6. The Responsible Entity shall make available documentation and records of its security status monitoring program as specified in Requirement R6.

M7. The Responsible Entity shall make available documentation and records of its program for the disposal or redeployment of Cyber Assets as specified in Requirement R7.

M8. The Responsible Entity shall make available documentation and records of its annual vulnerability assessment of all Cyber Assets within the Electronic Security Perimeters(s) as specified in Requirement R8.

M9. The Responsible Entity shall make available documentation and records demonstrating the review and update as specified in Requirement R9.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

1.2. The RE shall serve as the CEA with the following exceptions:

1.2.1 For entities that do not work for the Regional Entity, the Regional Entity shall serve as the Compliance Enforcement Authority.

1.2.2 For Reliability Coordinators and other functional entities that work for their Regional Entity, the ERO shall serve as the Compliance Enforcement Authority.

1.2.3 For Responsible Entities that are also Regional Entities, the ERO or a Regional Entity approved by the ERO and FERC or other applicable governmental authorities shall serve as the Compliance Enforcement Authority.

1.2.4 For the ERO, a third-party monitor without vested interest in the outcome for the ERO shall serve as the Compliance Enforcement Authority.

1.3. Compliance Monitoring and Enforcement Processes

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints

1.4. Data Retention

1.4.1 The Responsible Entity shall keep all documentation and records from the previous full calendar year unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

1.4.2 The Responsible Entity shall retain security–related system event logs for ninety calendar days, unless longer retention is required pursuant to Standard CIP-008-4 Requirement R2.

1.4.3 The Compliance Enforcement Authority in conjunction with the Registered Entity shall keep the last audit records and all requested and submitted subsequent audit records.

1.5. Additional Compliance Information.

2. Violation Severity Levels (To be developed later.)

E. Regional Variances

None identified.

Version History

Version	Date	Action	Change Tracking
2		Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards.	

		Removal of reasonable business judgment and acceptance of risk. Revised the Purpose of this standard to clarify that Standard CIP-007-2 requires Responsible Entities to define methods, processes, and procedures for securing Cyber Assets and other (non-Critical) Assets within an Electronic Security Perimeter. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. R9 changed ninety (90) days to thirty (30) days Changed compliance monitor to Compliance Enforcement Authority.	
3		Updated version numbers from -2 to -3	
3	12/16/09	Approved by the NERC Board of Trustees	
4	Board approved 01/24/2011	Update version number from “3” to “4”	Update to conform to changes to CIP-002-4 (Project 2008-06)

A. Introduction

1. Title: Cyber Security — Systems Security Management

2. Number: CIP-007-~~3~~4

3. Purpose: Standard CIP-007-~~3~~4 requires Responsible Entities to define methods, processes, and procedures for securing those systems determined to be Critical Cyber Assets, as well as the other (non-critical) Cyber Assets within the Electronic Security Perimeter(s). Standard CIP-007-~~3~~4 should be read as part of a group of standards numbered Standards CIP-002-~~3~~4 through CIP-009-~~3~~4.

4. Applicability:

4.1. Within the text of Standard CIP-007-~~3~~4, "Responsible Entity" shall mean:

4.1.1 Reliability Coordinator.

4.1.2 Balancing Authority.

4.1.3 Interchange Authority.

4.1.4 Transmission Service Provider.

4.1.5 Transmission Owner.

4.1.6 Transmission Operator.

4.1.7 Generator Owner.

4.1.8 Generator Operator.

4.1.9 Load Serving Entity.

4.1.10 NERC.

4.1.11 Regional Entity.

4.2. The following are exempt from Standard CIP-007-~~3~~4:

4.2.1 Facilities regulated by ~~the U.S. Nuclear Regulatory Commission or~~ the Canadian Nuclear Safety Commission.

4.2.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.3 In nuclear plants, the systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F. R. Section 73.54

~~Cyber Assets associated with Cyber Security Plans submitted to and verified by the U. S. Nuclear Regulatory Commission pursuant to 10 C.F.R. Section 73.54.~~

~~4.2.3~~4.2.4 Responsible Entities that, in compliance with Standard CIP-002-~~3~~4, identify that they have no Critical Cyber Assets.

5. Effective Date: The first day of the ~~third~~eighth calendar quarter after applicable regulatory approvals have been received (or the Reliability Standard otherwise becomes effective the first day of the ~~third~~ninth calendar quarter after BOT adoption in those jurisdictions where regulatory approval is not required).

B. Requirements

R1. Test Procedures — The Responsible Entity shall ensure that new Cyber Assets and significant changes to existing Cyber Assets within the Electronic Security Perimeter do not adversely affect existing cyber security controls. For purposes of Standard CIP-007-~~3~~4, a significant

Formatted: Font color: Black

Formatted: Font color: Black

change shall, at a minimum, include implementation of security patches, cumulative service packs, vendor releases, and version upgrades of operating systems, applications, database platforms, or other third-party software or firmware.

R1.1. The Responsible Entity shall create, implement, and maintain cyber security test procedures in a manner that minimizes adverse effects on the production system or its operation.

R1.2. The Responsible Entity shall document that testing is performed in a manner that reflects the production environment.

R1.3. The Responsible Entity shall document test results.

R2. Ports and Services — The Responsible Entity shall establish, document and implement a process to ensure that only those ports and services required for normal and emergency operations are enabled.

R2.1. The Responsible Entity shall enable only those ports and services required for normal and emergency operations.

R2.2. The Responsible Entity shall disable other ports and services, including those used for testing purposes, prior to production use of all Cyber Assets inside the Electronic Security Perimeter(s).

R2.3. In the case where unused ports and services cannot be disabled due to technical limitations, the Responsible Entity shall document compensating measure(s) applied to mitigate risk exposure.

R3. Security Patch Management — The Responsible Entity, either separately or as a component of the documented configuration management process specified in CIP-003–~~3~~4 Requirement R6, shall establish, document and implement a security patch management program for tracking, evaluating, testing, and installing applicable cyber security software patches for all Cyber Assets within the Electronic Security Perimeter(s).

R3.1. The Responsible Entity shall document the assessment of security patches and security upgrades for applicability within thirty calendar days of availability of the patches or upgrades.

R3.2. The Responsible Entity shall document the implementation of security patches. In any case where the patch is not installed, the Responsible Entity shall document compensating measure(s) applied to mitigate risk exposure.

R4. Malicious Software Prevention — The Responsible Entity shall use anti-virus software and other malicious software ("malware") prevention tools, where technically feasible, to detect, prevent, deter, and mitigate the introduction, exposure, and propagation of malware on all Cyber Assets within the Electronic Security Perimeter(s).

R4.1. The Responsible Entity shall document and implement anti-virus and malware prevention tools. In the case where anti-virus software and malware prevention tools are not installed, the Responsible Entity shall document compensating measure(s) applied to mitigate risk exposure.

R4.2. The Responsible Entity shall document and implement a process for the update of anti-virus and malware prevention "signatures." The process must address testing and installing the signatures.

R5. Account Management — The Responsible Entity shall establish, implement, and document technical and procedural controls that enforce access authentication of, and accountability for, all user activity, and that minimize the risk of unauthorized system access.

R5.1. The Responsible Entity shall ensure that individual and shared system accounts and authorized access permissions are consistent with the concept of "need to know" with respect to work functions performed.

R5.1.1. The Responsible Entity shall ensure that user accounts are implemented as approved by designated personnel. Refer to Standard CIP-003-~~3~~4 Requirement R5.

R5.1.2. The Responsible Entity shall establish methods, processes, and procedures that generate logs of sufficient detail to create historical audit trails of individual user account access activity for a minimum of ninety days.

R5.1.3. The Responsible Entity shall review, at least annually, user accounts to verify access privileges are in accordance with Standard CIP-003-~~3~~4 Requirement R5 and Standard CIP-004-~~3~~4 Requirement R4.

R5.2. The Responsible Entity shall implement a policy to minimize and manage the scope and acceptable use of administrator, shared, and other generic account privileges including factory default accounts.

R5.2.1. The policy shall include the removal, disabling, or renaming of such accounts where possible. For such accounts that must remain enabled, passwords shall be changed prior to putting any system into service.

R5.2.2. The Responsible Entity shall identify those individuals with access to shared accounts.

R5.2.3. Where such accounts must be shared, the Responsible Entity shall have a policy for managing the use of such accounts that limits access to only those with authorization, an audit trail of the account use (automated or manual), and steps for securing the account in the event of personnel changes (for example, change in assignment or termination).

R5.3. At a minimum, the Responsible Entity shall require and use passwords, subject to the following, as technically feasible:

R5.3.1. Each password shall be a minimum of six characters.

R5.3.2. Each password shall consist of a combination of alpha, numeric, and "special" characters.

R5.3.3. Each password shall be changed at least annually, or more frequently based on risk.

R6. Security Status Monitoring — The Responsible Entity shall ensure that all Cyber Assets within the Electronic Security Perimeter, as technically feasible, implement automated tools or organizational process controls to monitor system events that are related to cyber security.

R6.1. The Responsible Entity shall implement and document the organizational processes and technical and procedural mechanisms for monitoring for security events on all Cyber Assets within the Electronic Security Perimeter.

R6.2. The security monitoring controls shall issue automated or manual alerts for detected Cyber Security Incidents.

R6.3. The Responsible Entity shall maintain logs of system events related to cyber security, where technically feasible, to support incident response as required in Standard CIP-008-~~3~~4.

R6.4. The Responsible Entity shall retain all logs specified in Requirement R6 for ninety calendar days.

R6.5. The Responsible Entity shall review logs of system events related to cyber security and maintain records documenting review of logs.

R7. Disposal or Redeployment — The Responsible Entity shall establish and implement formal methods, processes, and procedures for disposal or redeployment of Cyber Assets within the Electronic Security Perimeter(s) as identified and documented in Standard CIP-005-~~3~~4.

R7.1. Prior to the disposal of such assets, the Responsible Entity shall destroy or erase the data storage media to prevent unauthorized retrieval of sensitive cyber security or reliability data.

R7.2. Prior to redeployment of such assets, the Responsible Entity shall, at a minimum, erase the data storage media to prevent unauthorized retrieval of sensitive cyber security or reliability data.

R7.3. The Responsible Entity shall maintain records that such assets were disposed of or redeployed in accordance with documented procedures.

R8. Cyber Vulnerability Assessment — The Responsible Entity shall perform a cyber vulnerability assessment of all Cyber Assets within the Electronic Security Perimeter at least annually. The vulnerability assessment shall include, at a minimum, the following:

R8.1. A document identifying the vulnerability assessment process;

R8.2. A review to verify that only ports and services required for operation of the Cyber Assets within the Electronic Security Perimeter are enabled;

R8.3. A review of controls for default accounts; and,

R8.4. Documentation of the results of the assessment, the action plan to remediate or mitigate vulnerabilities identified in the assessment, and the execution status of that action plan.

R9. Documentation Review and Maintenance — The Responsible Entity shall review and update the documentation specified in Standard CIP-007-~~3~~4 at least annually. Changes resulting from modifications to the systems or controls shall be documented within thirty calendar days of the change being completed.

C. Measures

M1. The Responsible Entity shall make available documentation of its security test procedures as specified in Requirement R1.

M2. The Responsible Entity shall make available documentation as specified in Requirement R2.

M3. The Responsible Entity shall make available documentation and records of its security patch management program, as specified in Requirement R3.

M4. The Responsible Entity shall make available documentation and records of its malicious software prevention program as specified in Requirement R4.

M5. The Responsible Entity shall make available documentation and records of its account management program as specified in Requirement R5.

M6. The Responsible Entity shall make available documentation and records of its security status monitoring program as specified in Requirement R6.

M7. The Responsible Entity shall make available documentation and records of its program for the disposal or redeployment of Cyber Assets as specified in Requirement R7.

M8. The Responsible Entity shall make available documentation and records of its annual vulnerability assessment of all Cyber Assets within the Electronic Security Perimeters(s) as specified in Requirement R8.

M9. The Responsible Entity shall make available documentation and records demonstrating the review and update as specified in Requirement R9.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

1.2. The RE shall serve as the CEA with the following exceptions:

1.2.1 For entities that do not work for the Regional Entity ~~for Responsible Entities that do not perform delegated tasks~~, the Regional Entity shall serve as the Compliance Enforcement Authority.

~~1.1.1~~1.2.2 For Reliability Coordinators and other functional entities that work for their Regional Entity, the ERO shall serve as the Compliance Enforcement Authority.

~~**1.1.2 ERO for Regional Entity.**~~

1.2.3 ~~Third~~For Responsible Entities that are also Regional Entities, the ERO or a Regional Entity approved by the ERO and FERC or other applicable governmental authorities shall serve as the Compliance Enforcement Authority.

~~**1.1.3**~~ For the ERO, a third-party monitor without vested interest in the outcome for ~~NERC.~~

~~**1.2.** the ERO shall serve as the~~ Compliance ~~**Monitoring Period and Reset Time Frame**~~

1.2.4 ~~Not applicable~~Enforcement Authority.

1.3. Compliance Monitoring and Enforcement Processes

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints

1.4. Data Retention

1.4.1 The Responsible Entity shall keep all documentation and records from the previous full calendar year unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

1.4.2 The Responsible Entity shall retain security–related system event logs for ninety calendar days, unless longer retention is required pursuant to Standard CIP-008-~~3~~4 Requirement R2.

1.4.3 The Compliance Enforcement Authority in conjunction with the Registered Entity shall keep the last audit records and all requested and submitted subsequent audit records.

1.5. Additional Compliance Information.

2. Violation Severity Levels (To be developed later.)

E. Regional Variances

Formatted: Font: Not Bold

Formatted: List Number, Outline numbered + Level: 3 + Numbering Style: 1, 2, 3, … + Start at: 1 + Alignment: Left + Aligned at: 1" + Tab after: 1.5" + Indent at: 1.5"

Formatted: Font: Bold

None identified.

Version History

Version	Date	Action	Change Tracking
2		Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment and acceptance of risk. Revised the Purpose of this standard to clarify that Standard CIP-007-2 requires Responsible Entities to define methods, processes, and procedures for securing Cyber Assets and other (non-Critical) Assets within an Electronic Security Perimeter. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. R9 changed ninety (90) days to thirty (30) days Changed compliance monitor to Compliance Enforcement Authority.	
3		Updated version numbers from -2 to -3	
3	12/16/09	Approved by the NERC Board of Trustees	
4	Board approved 01/24/2011	Update version number from “3” to “4”	Update to conform to changes to CIP-002-4 (Project 2008-06)

CIP-008-4 Clean and Redline

A. Introduction

1. Title: Cyber Security — Incident Reporting and Response Planning

2. Number: CIP-008-4

3. Purpose: Standard CIP-008-4 ensures the identification, classification, response, and reporting of Cyber Security Incidents related to Critical Cyber Assets. Standard CIP-008-4 should be read as part of a group of standards numbered Standards CIP-002-4 through CIP-009-4.

4. Applicability

4.1. Within the text of Standard CIP-008-4, "Responsible Entity" shall mean:

4.1.1 Reliability Coordinator.

4.1.2 Balancing Authority.

4.1.3 Interchange Authority.

4.1.4 Transmission Service Provider.

4.1.5 Transmission Owner.

4.1.6 Transmission Operator.

4.1.7 Generator Owner.

4.1.8 Generator Operator.

4.1.9 Load Serving Entity.

4.1.10 NERC.

4.1.11 Regional Entity.

4.2. The following are exempt from Standard CIP-008-4:

4.2.1 Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.3 In nuclear plants, the systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F. R. Section 73.54

4.2.4 Responsible Entities that, in compliance with Standard CIP-002-4, identify that they have no Critical Cyber Assets.

5. Effective Date: The first day of the eighth calendar quarter after applicable regulatory approvals have been received (or the Reliability Standard otherwise becomes effective the first day of the ninth calendar quarter after BOT adoption in those jurisdictions where regulatory approval is not required).

B. Requirements

R1. Cyber Security Incident Response Plan — The Responsible Entity shall develop and maintain a Cyber Security Incident response plan and implement the plan in response to Cyber Security Incidents. The Cyber Security Incident response plan shall address, at a minimum, the following:

R1.1. Procedures to characterize and classify events as reportable Cyber Security Incidents.

R1.2. Response actions, including roles and responsibilities of Cyber Security Incident response teams, Cyber Security Incident handling procedures, and communication plans.

R1.3. Process for reporting Cyber Security Incidents to the Electricity Sector Information Sharing and Analysis Center (ES-ISAC). The Responsible Entity must ensure that all reportable Cyber Security Incidents are reported to the ES-ISAC either directly or through an intermediary.

R1.4. Process for updating the Cyber Security Incident response plan within thirty calendar days of any changes.

R1.5. Process for ensuring that the Cyber Security Incident response plan is reviewed at least annually.

R1.6. Process for ensuring the Cyber Security Incident response plan is tested at least annually. A test of the Cyber Security Incident response plan can range from a paper drill, to a full operational exercise, to the response to an actual incident.

R2. Cyber Security Incident Documentation — The Responsible Entity shall keep relevant documentation related to Cyber Security Incidents reportable per Requirement R1.1 for three calendar years.

C. Measures

M1. The Responsible Entity shall make available its Cyber Security Incident response plan as indicated in Requirement R1 and documentation of the review, updating, and testing of the plan.

M2. The Responsible Entity shall make available all documentation as specified in Requirement R2.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

1.2. The RE shall serve as the CEA with the following exceptions:

1.2.1 For entities that do not work for the Regional Entity, the Regional Entity shall serve as the Compliance Enforcement Authority.

1.2.2 For Reliability Coordinators and other functional entities that work for their Regional Entity, the ERO shall serve as the Compliance Enforcement Authority.

1.2.3 For Responsible Entities that are also Regional Entities, the ERO or a Regional Entity approved by the ERO and FERC or other applicable governmental authorities shall serve as the Compliance Enforcement Authority.

1.2.4 For the ERO, a third-party monitor without vested interest in the outcome for the ERO shall serve as the Compliance Enforcement Authority.

1.3. Compliance Monitoring and Enforcement Processes

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints

1.4. Data Retention

1.4.1 The Responsible Entity shall keep documentation other than that required for reportable Cyber Security Incidents as specified in Standard CIP-008-4 for the previous full calendar year unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

1.4.2 The Compliance Enforcement Authority in conjunction with the Registered Entity shall keep the last audit records and all requested and submitted subsequent audit records.

1.5. Additional Compliance Information

1.5.1 The Responsible Entity may not take exception in its cyber security policies to the creation of a Cyber Security Incident response plan.

1.5.2 The Responsible Entity may not take exception in its cyber security policies to reporting Cyber Security Incidents to the ES ISAC.

2. Violation Severity Levels (To be developed later.)

E. Regional Variances

None identified.

Version History

Version	Date	Action	Change Tracking
2		Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3		Updated Version number from -2 to -3 In Requirement 1.6, deleted the sentence pertaining to removing component or system from service in order to perform testing, in response to FERC order issued September 30, 2009.	
3	12/16/09	Approved by NERC Board of Trustees	Update
4	Board approved 01/24/2011	Update version number from “3” to “4”	Update to conform to changes to CIP-002-4 (Project 2008-06)

A. Introduction

1. Title: Cyber Security — Incident Reporting and Response Planning

2. Number: CIP-008-~~3~~4

3. Purpose: Standard CIP-008-~~3~~4 ensures the identification, classification, response, and reporting of Cyber Security Incidents related to Critical Cyber Assets. Standard CIP-008-~~23~~4 should be read as part of a group of standards numbered Standards CIP-002-~~3~~4 through CIP-009-~~3~~4.

4. Applicability

4.1. Within the text of Standard CIP-008-~~3~~4, "Responsible Entity" shall mean:

4.1.1 Reliability Coordinator.

4.1.2 Balancing Authority.

4.1.3 Interchange Authority.

4.1.4 Transmission Service Provider.

4.1.5 Transmission Owner.

4.1.6 Transmission Operator.

4.1.7 Generator Owner.

4.1.8 Generator Operator.

4.1.9 Load Serving Entity.

4.1.10 NERC.

4.1.11 Regional Entity.

4.2. The following are exempt from Standard CIP-008-~~3~~4:

4.2.1 Facilities regulated by ~~the U.S. Nuclear Regulatory Commission or~~ the Canadian Nuclear Safety Commission.

4.2.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.3 In nuclear plants, the systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F. R. Section 73.54

~~4.2.3~~4.2.4 Responsible Entities that, in compliance with Standard CIP-002-~~3~~4, identify that they have no Critical Cyber Assets.

5. Effective Date: The first day of the ~~third~~eighth calendar quarter after applicable regulatory approvals have been received (or the Reliability Standard otherwise becomes effective the first day of the ~~third~~ninth calendar quarter after BOT adoption in those jurisdictions where regulatory approval is not required).

B. Requirements

R1. Cyber Security Incident Response Plan — The Responsible Entity shall develop and maintain a Cyber Security Incident response plan and implement the plan in response to Cyber Security Incidents. The Cyber Security Incident response plan shall address, at a minimum, the following:

R1.1. Procedures to characterize and classify events as reportable Cyber Security Incidents.

R1.2. Response actions, including roles and responsibilities of Cyber Security Incident response teams, Cyber Security Incident handling procedures, and communication plans.

R1.3. Process for reporting Cyber Security Incidents to the Electricity Sector Information Sharing and Analysis Center (ES-ISAC). The Responsible Entity must ensure that all reportable Cyber Security Incidents are reported to the ES-ISAC either directly or through an intermediary.

R1.4. Process for updating the Cyber Security Incident response plan within thirty calendar days of any changes.

R1.5. Process for ensuring that the Cyber Security Incident response plan is reviewed at least annually.

R1.6. Process for ensuring the Cyber Security Incident response plan is tested at least annually. A test of the Cyber Security Incident response plan can range from a paper drill, to a full operational exercise, to the response to an actual incident.

R2. Cyber Security Incident Documentation — The Responsible Entity shall keep relevant documentation related to Cyber Security Incidents reportable per Requirement R1.1 for three calendar years.

C. Measures

M1. The Responsible Entity shall make available its Cyber Security Incident response plan as indicated in Requirement R1 and documentation of the review, updating, and testing of the plan.

M2. The Responsible Entity shall make available all documentation as specified in Requirement R2.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

1.2. The RE shall serve as the CEA with the following exceptions:

1.2.1 For entities that do not work for the Regional Entity ~~for Responsible Entities that do not perform delegated tasks~~, the Regional Entity shall serve as the Compliance Enforcement Authority.

~~1.1.1~~1.2.2 For Reliability Coordinators and other functional entities that work for their Regional Entity, the ERO shall serve as the Compliance Enforcement Authority.

~~**1.1.2 ERO for Regional Entity.**~~

1.2.3 ~~Third~~For Responsible Entities that are also Regional Entities, the ERO or a Regional Entity approved by the ERO and FERC or other applicable governmental authorities shall serve as the Compliance Enforcement Authority.

~~**1.1.3**~~ For the ERO, a third-party monitor without vested interest in the outcome for ~~NERC.~~

~~**1.2.**~~ the ERO shall serve as the Compliance ~~**Monitoring Period and Reset Time Frame**~~

1.2.4 ~~Not applicable~~Enforcement Authority.

1.3. Compliance Monitoring and Enforcement Processes

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints

1.4. Data Retention

1.4.1 The Responsible Entity shall keep documentation other than that required for reportable Cyber Security Incidents as specified in Standard CIP-008-~~3~~4 for the previous full calendar year unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

1.4.2 The Compliance Enforcement Authority in conjunction with the Registered Entity shall keep the last audit records and all requested and submitted subsequent audit records.

1.5. Additional Compliance Information

1.5.1 The Responsible Entity may not take exception in its cyber security policies to the creation of a Cyber Security Incident response plan.

1.5.2 The Responsible Entity may not take exception in its cyber security policies to reporting Cyber Security Incidents to the ES ISAC.

2. Violation Severity Levels (To be developed later.)

E. Regional Variances

None identified.

Version History

Version	Date	Action	Change Tracking
2		Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3		Updated Version number from -2 to -3 In Requirement 1.6, deleted the sentence pertaining to removing component or system from service in order to perform testing, in response to FERC order issued	

		September 30, 2009.	
3	12/16/09	Approved by NERC Board of Trustees	Update
4	Board approved 01/24/2011	Update version number from “3” to “4”	Update to conform to changes to CIP-002-4 (Project 2008-06)

CIP-009-4 Clean and Redline

A. Introduction

1. Title: Cyber Security — Recovery Plans for Critical Cyber Assets

2. Number: CIP-009-4

3. Purpose: Standard CIP-009-4 ensures that recovery plan(s) are put in place for Critical Cyber Assets and that these plans follow established business continuity and disaster recovery techniques and practices. Standard CIP-009-4 should be read as part of a group of standards numbered Standards CIP-002-4 through CIP-009-4.

4. Applicability:

4.1. Within the text of Standard CIP-009-3, "Responsible Entity" shall mean:

4.1.1 Reliability Coordinator

4.1.2 Balancing Authority

4.1.3 Interchange Authority

4.1.4 Transmission Service Provider

4.1.5 Transmission Owner

4.1.6 Transmission Operator

4.1.7 Generator Owner

4.1.8 Generator Operator

4.1.9 Load Serving Entity

4.1.10 NERC

4.1.11 Regional Entity

4.2. The following are exempt from Standard CIP-009-4:

4.2.1 Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.3 In nuclear plants, the systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F. R. Section 73.54

4.2.4 Responsible Entities that, in compliance with Standard CIP-002-4, identify that they have no Critical Cyber Assets.

5. Effective Date: The first day of the eighth calendar quarter after applicable regulatory approvals have been received (or the Reliability Standard otherwise becomes effective the first day of the ninth calendar quarter after BOT adoption in those jurisdictions where regulatory approval is not required).

B. Requirements

R1. Recovery Plans — The Responsible Entity shall create and annually review recovery plan(s) for Critical Cyber Assets. The recovery plan(s) shall address at a minimum the following:

R1.1. Specify the required actions in response to events or conditions of varying duration and severity that would activate the recovery plan(s).

R1.2. Define the roles and responsibilities of responders.

R2. Exercises — The recovery plan(s) shall be exercised at least annually. An exercise of the recovery plan(s) can range from a paper drill, to a full operational exercise, to recovery from an actual incident.

R3. Change Control — Recovery plan(s) shall be updated to reflect any changes or lessons learned as a result of an exercise or the recovery from an actual incident. Updates shall be communicated to personnel responsible for the activation and implementation of the recovery plan(s) within thirty calendar days of the change being completed.

R4. Backup and Restore — The recovery plan(s) shall include processes and procedures for the backup and storage of information required to successfully restore Critical Cyber Assets. For example, backups may include spare electronic components or equipment, written documentation of configuration settings, tape backup, etc.

R5. Testing Backup Media — Information essential to recovery that is stored on backup media shall be tested at least annually to ensure that the information is available. Testing can be completed off site.

C. Measures

M1. The Responsible Entity shall make available its recovery plan(s) as specified in Requirement R1.

M2. The Responsible Entity shall make available its records documenting required exercises as specified in Requirement R2.

M3. The Responsible Entity shall make available its documentation of changes to the recovery plan(s), and documentation of all communications, as specified in Requirement R3.

M4. The Responsible Entity shall make available its documentation regarding backup and storage of information as specified in Requirement R4.

M5. The Responsible Entity shall make available its documentation of testing of backup media as specified in Requirement R5.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

1.2. The RE shall serve as the CEA with the following exceptions:

1.2.1 For entities that do not work for the Regional Entity, the Regional Entity shall serve as the Compliance Enforcement Authority.

1.2.2 For Reliability Coordinators and other functional entities that work for their Regional Entity, the ERO shall serve as the Compliance Enforcement Authority.

1.2.3 For Responsible Entities that are also Regional Entities, the ERO or a Regional Entity approved by the ERO and FERC or other applicable governmental authorities shall serve as the Compliance Enforcement Authority.

1.2.4 For the ERO, a third-party monitor without vested interest in the outcome for the ERO shall serve as the Compliance Enforcement Authority.

1.3. Compliance Monitoring and Enforcement Processes

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints

1.4. Data Retention

1.4.1 The Responsible Entity shall keep documentation required by Standard CIP-009-4 from the previous full calendar year unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

1.4.2 The Compliance Enforcement Authority in conjunction with the Registered Entity shall keep the last audit records and all requested and submitted subsequent audit records.

1.5. Additional Compliance Information

2. Violation Severity Levels (To be developed later.)

E. Regional Variances

None identified.

Version History

Version	Date	Action	Change Tracking
2		Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Communication of revisions to the recovery plan changed from 90 days to 30 days. Changed compliance monitor to Compliance Enforcement Authority.	
3		Updated version numbers from -2 to -3	
3	12/16/09	Approved by the NERC Board of Trustees	Update
4	Board approved 01/24/2011	Update version number from “3” to “4”	Update to conform to changes to CIP-002-4 (Project 2008-06)

A. Introduction

1. Title: Cyber Security — Recovery Plans for Critical Cyber Assets

2. Number: CIP-009-~~3~~4

3. Purpose: Standard CIP-009-~~3~~4 ensures that recovery plan(s) are put in place for Critical Cyber Assets and that these plans follow established business continuity and disaster recovery techniques and practices. Standard CIP-009-~~3~~4 should be read as part of a group of standards numbered Standards CIP-002-~~3~~4 through CIP-009-~~3~~4.

4. Applicability:

4.1. Within the text of Standard CIP-009-3, "Responsible Entity" shall mean:

4.1.1 Reliability Coordinator

4.1.2 Balancing Authority

4.1.3 Interchange Authority

4.1.4 Transmission Service Provider

4.1.5 Transmission Owner

4.1.6 Transmission Operator

4.1.7 Generator Owner

4.1.8 Generator Operator

4.1.9 Load Serving Entity

4.1.10 NERC

4.1.11 Regional Entity

4.2. The following are exempt from Standard CIP-009-~~3~~4:

4.2.1 Facilities regulated by ~~the U.S. Nuclear Regulatory Commission or~~ the Canadian Nuclear Safety Commission.

4.2.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

~~4.2.3~~ In nuclear plants, the systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F. R. Section 73.54~~Cyber Assets associated with Cyber Security Plans submitted to and verified by the U. S. Nuclear Regulatory Commission pursuant to 10 C.F.R. Section 73.54.~~

~~4.2.3~~4.2.4 Responsible Entities that, in compliance with Standard CIP-002-~~3~~4, identify that they have no Critical Cyber Assets.

5. Effective Date: The first day of the ~~third~~eighth calendar quarter after applicable regulatory approvals have been received (or the Reliability Standard otherwise becomes effective the first day of the ~~third~~ninth calendar quarter after BOT adoption in those jurisdictions where regulatory approval is not required).

B. Requirements

R1. Recovery Plans — The Responsible Entity shall create and annually review recovery plan(s) for Critical Cyber Assets. The recovery plan(s) shall address at a minimum the following:

R1.1. Specify the required actions in response to events or conditions of varying duration and severity that would activate the recovery plan(s).

Formatted: Font color: Black

Formatted: Font color: Black

R1.2. Define the roles and responsibilities of responders.

R2. Exercises — The recovery plan(s) shall be exercised at least annually. An exercise of the recovery plan(s) can range from a paper drill, to a full operational exercise, to recovery from an actual incident.

R3. Change Control — Recovery plan(s) shall be updated to reflect any changes or lessons learned as a result of an exercise or the recovery from an actual incident. Updates shall be communicated to personnel responsible for the activation and implementation of the recovery plan(s) within thirty calendar days of the change being completed.

R4. Backup and Restore — The recovery plan(s) shall include processes and procedures for the backup and storage of information required to successfully restore Critical Cyber Assets. For example, backups may include spare electronic components or equipment, written documentation of configuration settings, tape backup, etc.

R5. Testing Backup Media — Information essential to recovery that is stored on backup media shall be tested at least annually to ensure that the information is available. Testing can be completed off site.

C. Measures

M1. The Responsible Entity shall make available its recovery plan(s) as specified in Requirement R1.

M2. The Responsible Entity shall make available its records documenting required exercises as specified in Requirement R2.

M3. The Responsible Entity shall make available its documentation of changes to the recovery plan(s), and documentation of all communications, as specified in Requirement R3.

M4. The Responsible Entity shall make available its documentation regarding backup and storage of information as specified in Requirement R4.

M5. The Responsible Entity shall make available its documentation of testing of backup media as specified in Requirement R5.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

1.2. The RE shall serve as the CEA with the following exceptions:

1.2.1 For entities that do not work for the Regional Entity ~~for Responsible Entities that do not perform delegated tasks~~, the Regional Entity shall serve as the Compliance Enforcement Authority.

~~1.1.1~~1.2.2 For Reliability Coordinators and other functional entities that work for their Regional Entity, the ERO shall serve as the Compliance Enforcement Authority.

~~**1.1.2 ERO for Regional Entities.**~~

1.2.3 ~~Third~~For Responsible Entities that are also Regional Entities, the ERO or a Regional Entity approved by the ERO and FERC or other applicable governmental authorities shall serve as the Compliance Enforcement Authority.

~~**1.1.3**~~ For the ERO, a third-party monitor without vested interest in the outcome for ~~NERC.~~

~~**1.2.**~~ the ERO shall serve as the Compliance ~~**Monitoring Period and Reset Time Frame**~~

Formatted: Font: Not Bold

1.2.4 ~~Not applicable~~Enforcement Authority.

1.3. Compliance Monitoring and Enforcement Processes

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints

1.4. Data Retention

1.4.1 The Responsible Entity shall keep documentation required by Standard CIP-009-~~3~~4 from the previous full calendar year unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

1.4.2 The Compliance Enforcement Authority in conjunction with the Registered Entity shall keep the last audit records and all requested and submitted subsequent audit records.

1.5. Additional Compliance Information

2. Violation Severity Levels (To be developed later.)

E. Regional Variances

None identified.

Formatted: List Number, Outline numbered + Level: 3 + Numbering Style: 1, 2, 3, … + Start at: 1 + Alignment: Left + Aligned at: 1" + Tab after: 1.5" + Indent at: 1.5"

Formatted: Font: Bold

Version History

Version	Date	Action	Change Tracking
2		Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Communication of revisions to the recovery plan changed from 90 days to 30 days. Changed compliance monitor to Compliance Enforcement Authority.	
3		Updated version numbers from -2 to -3	
3	12/16/09	Approved by the NERC Board of Trustees	Update
4	Board approved 01/24/2011	Update version number from "3" to "4"	Update to conform to changes to CIP-002-4 (Project 2008-06)

Exhibit B

Implementation Plan for Version 4 Cyber Security Standards CIP-002-4 through CIP-009-4

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Implementation Plan for Version 4 of Cyber Security Standards CIP-002-4 through CIP-009-4

Prerequisite Approvals

There are no other reliability standards or Standard Authorization Requests (SARs), in progress or approved, that must be implemented before

The term Blackstart Resource, used in CIP-002-4 Attachment 1, was submitted for regulatory approval with Project 2006-03 – System Restoration and Blackstart. The effective date of EOP-005-2 is the date that Criteria 1.4 and 1.5 will be used to determine Critical Assets for Responsible Entity.

Applicable Standards

The following standards are covered by this Implementation Plan:
CIP–002–4 —Cyber Security — Critical Cyber Asset Identification
CIP–003–4 — Cyber Security — Security Management Controls
CIP–004–4 — Cyber Security — Personnel and Training
CIP–005–4 — Cyber Security — Electronic Security Perimeter(s)
CIP–006–4 — Cyber Security — Physical Security
CIP–007–4 —Cyber Security — Systems Security Management
CIP–008–4 — Cyber Security — Incident Reporting and Response Planning
CIP–009–4 — Cyber Security — Recovery Plans for Critical Cyber Assets

These standards are posted for ballot by NERC together with this Implementation Plan. When these standards become effective, all prior versions of these standards are retired.

Compliance with Standards

Once these standards become effective, the Responsible Entities identified in the Applicability section of the standard must comply with the requirements. These Responsible Entities include:
• Reliability Coordinator
• Balancing Authority
• Interchange Authority
• Transmission Service Provider
• Transmission Owner
• Transmission Operator
• Generator Owner
• Generator Operator
• Load Serving Entity
• NERC
• Regional Entity

116-390 Village Blvd.
Princeton, NJ 08540
609.452.8060 | www.nerc.com

Proposed Effective Date for CIP-002-4 through CIP-009-4

All Facilities Other Than U.S. Nuclear Power Plant Facilities
Responsible Entities shall be compliant with the requirements of CIP-002-4 through CIP-009-4 on the later of (i) the Effective Date specified in the Standard or (ii) the compliance milestones specified in version 3 of the *Implementation Plan for Newly Identified Critical Cyber Asset and Newly Registered Entities.*

U.S. Nuclear Power Plant Facilities
For Owners and Operators of U.S. Nuclear Power Plants, Critical Cyber Assets associated with U.S. Nuclear Power Plants identified as Critical Assets shall be compliant with CIP-002-4 through CIP-009-4 by the later of (i) the Effective Date in CIP-002-4 through CIP-009-4, (ii) 6 months following the completion of the first refueling outage beyond the Effective Date of CIP-002-4 for those requirements requiring a refueling outage, or (iii) the compliance milestones specified in version 3 of the *Implementation Plan for Newly Identified Critical Cyber Asset and Newly Registered Entities.*

Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities

Concurrently submitted with version 4 of Cyber Security Standards CIP-002-4 through CIP-009-4 is a separate Implementation Plan document that would be used by the Responsible Entities to bring any Critical Cyber Assets identified after the effective date of CIP-002-4 into compliance with the Cyber Security Standards, as those assets are identified. The Implementation Plan for newly identified Critical Cyber Assets provides a reasonable schedule for the Responsible Entity to achieve the 'Compliant' state for those newly identified Critical Cyber Assets.
The Implementation Plan for newly identified Critical Cyber Assets also addresses how to achieve the 'Compliant' state for: 1) Responsible Entities that merge with or are acquired by other Responsible Entities; and 2) Responsible Entities that register in the NERC Compliance Registry during or following the completion of the Implementation Plan for Version 4 of the NERC Cyber Security Standards CIP-002-4 to CIP-009-4.

Exhibit C

Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities for CIP Reliability Standards submitted for Approval

Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities

This Implementation Plan applies to Cyber Security Standards CIP-002-4 through CIP-009-4.

The term "Compliant" in this Implementation Plan is used in the same way that it is used in the (Revised) Implementation Plan for Cyber Security Standards CIP-002-1 through CIP-009-1: "Compliant means the entity meets the full intent of the requirements and is beginning to maintain required 'data,' 'documents,' 'documentation,' 'logs,' and 'records.'"

The Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities (hereafter referred to as 'this Implementation Plan') defines the schedule for compliance with the requirements of Version 4 of the NERC Reliability Standards CIP-003 through CIP-009[1] on Cyber Security for (a) newly Registered Entities and (b) newly identified Critical Cyber Assets by an existing Registered Entity after the Registered Entity's applicable *Compliant* milestone date has already passed based upon the scenarios identified in the Version 4 CIP-002-4 through CIP-009-4 Implementation Plan.

There are no *Compliant* milestones specified in Table 2 of this Implementation Plan for compliance with NERC Standard CIP-002, since all Responsible Entities are required to be compliant with NERC Standard CIP-002 based on a previous or existing version-specific Implementation Plan[2].

Implementation Plan for Newly Identified Critical Cyber Assets

This Implementation Plan defines the *Compliant* milestone dates in terms of the number of calendar months after designation of the newly identified Cyber Asset as a Critical Cyber Asset, following the process stated in NERC Standard CIP-002. These *Compliant* Milestone dates are included in Table 2 of this Implementation Plan.

The term 'newly identified Critical Cyber Asset' is used when a Registered Entity has been required to be compliant with NERC Reliability Standard CIP-002 for at least one application of the "Critical Asset Criteria" for the identification of Critical Assets. Upon a subsequent annual application of the Critical Asset identification in compliance with requirements of NERC Reliability Standard CIP-002, either a previously non-critical asset has now been determined to be a Critical Asset, and its associated essential Cyber Assets have now been determined to be Critical Cyber Assets, or Cyber Assets associated with an existing Critical Asset have now been identified as Critical Cyber Assets. These newly determined Critical Cyber Assets are referred to in this Implementation Plan as 'newly identified Critical Cyber Assets'.

[1] The reference in this Implementation Plan to 'NERC Standards CIP-002 through CIP-009' is to all versions (i.e., Version 1, Version 2, Version 3, and Version 4) of those standards. If reference to only a specific version of a standard or set of standards is required, a version number (i.e., '-1', '-2','-3', or '-4') will be applied to that particular reference.

[2] Each version of NERC Standards CIP-002 through CIP-009 has its own implementation plan and/or designated effective date when approved by the NERC Board of Trustees or appropriate government authorities.

Table 2 defines the *Compliant* milestone dates for all of the requirements defined in the NERC Reliability Standards CIP-003 through CIP-009 in terms of the number of months following the designation of a newly identified Critical Cyber Asset a Responsible Entity has to become compliant with that requirement. Table 2 further defines the *Compliant* milestone dates for the NERC Reliability Standards CIP-003 through CIP-009 based on the 'Milestone Category', which characterizes the scenario by which the Critical Cyber Asset was identified.

For those NERC Reliability Standard requirements that have an entry in Table 2 annotated as *existing*, the designation of a newly identified Critical Cyber Asset has no bearing on its *Compliant* milestone date, since Responsible Entities are required to be compliant with those requirements as part of an existing CIP compliance implementation program[3], independent of the determination of a newly identified Critical Cyber Asset.

Implementation Plan for Newly Registered Entities

A newly Registered Entity is one that has registered with NERC as of the Effective Date of the CIP-002-4 Standard or thereafter and has not previously undergone the NERC CIP-002 Critical Asset Identification Process. As such, it is presumed that no Critical Cyber Assets have been previously identified and no previously established CIP compliance implementation program exists. The *Compliant* milestone schedule defined in Table 3 of this Implementation Plan document defines the applicable compliance schedule for the newly Registered Entity to the NERC Reliability Standards CIP-002 through CIP-009.

Implementation Milestone Categories

The Implementation Plan milestones and schedule to achieve compliance with the NERC Reliability Standards CIP-002 through CIP-009 for newly identified Critical Cyber Assets and newly Registered Entities are provided in Tables 2 and 3 of this Implementation Plan document.

The Implementation Plan milestones defined in Table 2 are divided into categories based on the scenario by which the Critical Cyber Asset was newly identified. The scenarios that represent the milestone categories are briefly defined as follows:

1. A Cyber Asset is designated as the first Critical Cyber Asset by a Responsible Entity according to the process defined in NERC Reliability Standard CIP-002. No existing CIP compliance implementation program for Standards CIP-003 through CIP-009 is assumed to exist at the Responsible Entity. This category would also apply in the case of a newly Registered Entity (not resulting from a merger or acquisition), if any Critical Cyber Asset was identified according to the process defined in NERC Reliability Standard CIP-002.

2. An existing Cyber Asset becomes subject to the NERC Reliability Standards CIP-003 through CIP-009, *not due to a planned change in the electric system or Cyber Assets by*

[3] The term 'CIP compliance implementation program' is used to mean that a Responsible Entity has programs and procedures in place to comply with the requirements of NERC Reliability Standards CIP-003 through CIP-009 for Critical Cyber Assets. All entities are required to be Compliant with NERC Reliability Standard CIP-002 according to a version specific Implementation Plan.

the Responsible Entity (unplanned changes due to emergency response are handled separately). A CIP compliance implementation program already exists at the Responsible Entity.

3. A new or existing Cyber Asset becomes subject to the NERC Reliability Standards CIP-003 through CIP-009, *due to a planned change in the electric system or Cyber Assets by the Responsible Entity*. A CIP compliance implementation program already exists at the Responsible Entity.

Note that the phrase 'Cyber Asset becomes subject to the NERC Reliability Standards CIP-003 through CIP-009' as used above applies to all Critical Cyber Assets, as well as other (non-critical) Cyber Assets within an Electronic Security Perimeter that must comply with the applicable requirements of NERC Reliability Standards CIP-003 through CIP-009.

Note also that the phrase 'planned change in the electric system or Cyber Assets by the Responsible Entity' refers to any changes of the electric system or Cyber Assets which were planned and implemented by the Responsible Entity.

For example, if a particular transmission substation has been designated a Critical Asset, but there are no Cyber Assets at that transmission substation, then there are no Critical Cyber Assets associated with the Critical Asset at the transmission substation. If an automation modernization activity is performed at that same transmission substation, whereby Cyber Assets are installed that meet the requirements as Critical Cyber Assets, then those newly identified Critical Cyber Assets have been implemented as a result of a planned change of the Critical Asset, and must therefore be in Compliance with NERC Reliability Standards CIP-003 through CIP-009 upon the commissioning of the modernized transmission substation.(Compliant Upon Commissioning below.)

If, however, a particular transmission substation with Cyber Assets does not meet the criteria as a Critical Asset, its associated Cyber Assets are *not* Critical Cyber Assets, as described in the requirements of NERC Reliability Standard CIP-002. Further, if an action is performed outside of that particular transmission substation, such as a transmission line is constructed or retired, a generation plant is modified changing its rated output, or load patterns shift resulting in corresponding transmission flow changes through that transmission substation, that unchanged transmission substation may become a Critical Asset based on the established criteria in the CIP-002-4 *Attachment 1 Critical Asset Criteria* through the application of the Critical Asset identification (required by CIP-002 R1). (Note that the actions that cause the change in power flows may have been performed by a neighboring entity without the full knowledge of the affected Responsible Entity.) Application of those Critical Asset criteria is required annually (by CIP-002 R1), and, as such, it may not be immediately apparent that that particular transmission substation has become a Critical Asset until after the required annual application of the identification methodology. Category 1 Scenario below applies if there was no pre-existing Critical Cyber Assets subject to the standard, and therefore, there was no existing full CIP program. Category 2 Scenario below applies if a CIP program for existing Critical Cyber Assets has been implemented for that Registered Entity.

Figure 1 shows an overall process flow for determining which milestone category a Critical Cyber Asset identification scenario must follow. Following the figure is a more detailed description of each category.

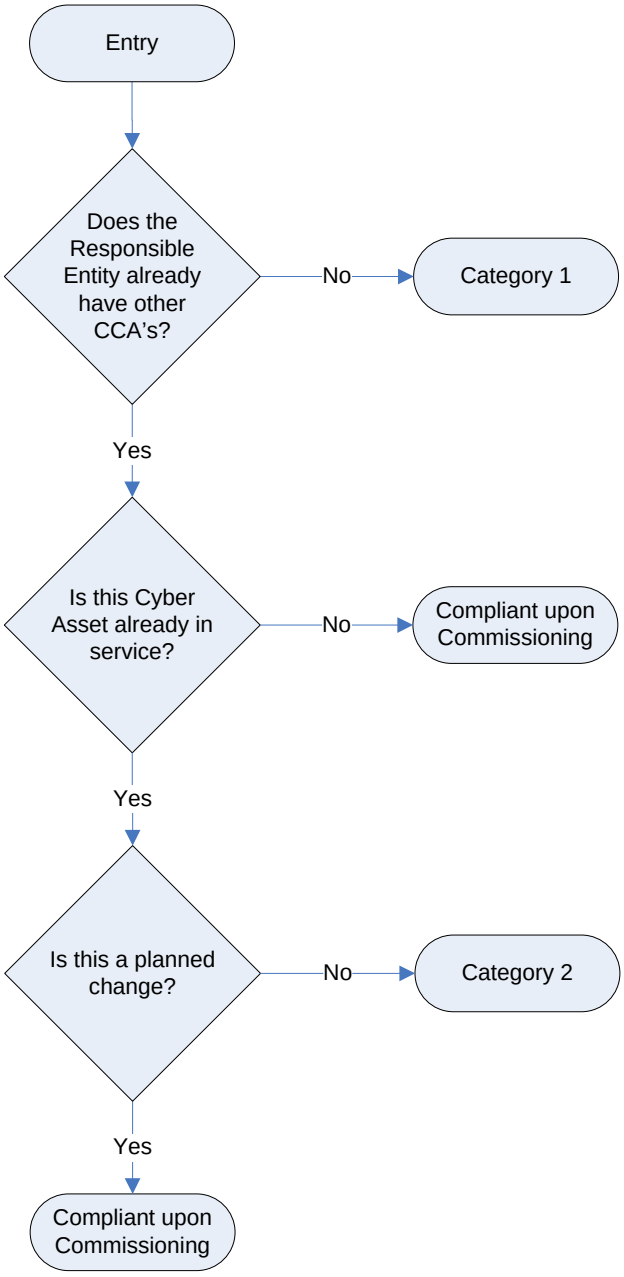


Figure 1: Category Selection Process Flow

Implementation Milestone Categories and Schedules

Based on the Critical Cyber Asset identification scenarios identified above, the implementation milestone categories and schedules for those scenarios are defined and distinguished below for entities with existing registrations in the NERC Compliance Registry. Scenarios resulting from the formation of newly Registered Entities are discussed in a subsequent section of this Implementation Plan.

1. **Category 1 Scenario**: A Responsible Entity that previously has undergone the NERC Reliability Standard CIP-002 Critical Asset identification process for at least one annual review and approval period without ever having previously identified any Critical Cyber Assets associated with Critical Assets, but has now identified one or more Critical Cyber Assets. As such, it is presumed that the Responsible Entity does not have a previously established CIP compliance implementation program.

   The *Compliant* milestones defined for this Category are defined in Table 2 (Milestone Category 1) of this Implementation Plan document.

2. **Category 2 Scenario**: A Responsible Entity has an established NERC Reliability Standards CIP compliance implementation program in place, and has newly identified additional existing Cyber Assets that need to be added to its Critical Cyber Asset list and therefore subject to compliance to the NERC Reliability CIP Standards due to unplanned changes in the electric system or the Cyber Assets. Since the Responsible Entity already has a CIP compliance implementation program, it needs only to implement the NERC Reliability CIP standards for the newly identified Critical Cyber Asset(s). The existing Critical Cyber Assets may remain in service while the relevant requirements of the NERC Reliability CIP Standards are implemented for the newly identified Critical Cyber Asset(s).

   This category applies only when additional in-service Critical Cyber Assets or applicable other Cyber Assets are *identified* as Critical Cyber Assets according to the process defined in the NERC Reliability Standard CIP-002. This category does not apply if the newly identified Critical Cyber Assets are not already in-service, or if the additional Critical Cyber Assets resulted from planned changes to the electric system or the Cyber Assets. In the case where the Critical Cyber Asset is not in service, the Responsible Entity must be compliant with the NERC Reliability Standards CIP-003 through CIP-009 upon commissioning of the new cyber or electric system assets (see "Compliant upon Commissioning" below).

   Unplanned changes due to emergency response, disaster recovery or system restoration activities are handled separately (see "Disaster Recovery and Restoration Activities" below).

3. **Compliant upon Commissioning**: When a Responsible Entity has an established NERC Reliability Standards CIP compliance implementation program and implements a new or replacement Critical Cyber Asset associated with a previously identified or newly

constructed Critical Asset, the Critical Cyber Asset shall be compliant when it is commissioned or activated. This scenario shall apply for the following scenarios:

a) 'Greenfield' construction of an asset that will be declared a Critical Asset (based on the Critical Asset criteria in CIP-002-4 Attachment 1) upon its commissioning or activation
b) Replacement or upgrade of an existing Critical Cyber Asset (or other Cyber Asset within an Electronic Security Perimeter) associated with a previously identified Critical Asset
c) Upgrade or replacement of an existing non-cyber asset with a Cyber Asset (e.g., replacement of an electro-mechanical relay with a microprocessor-based relay) associated with a previously identified Critical Asset and meets other criteria for identification as a Critical Cyber Asset
d) Planned addition of:
    i. a Critical Cyber Asset, or,
    ii. another (i.e., non-critical) Cyber Asset within an established Electronic Security Perimeter

In summary, this scenario applies in any case where a Critical Cyber Asset or applicable other Cyber Asset is being added or modified associated with an existing or new Critical Asset and where that Entity has an established NERC Reliability Standard CIP compliance implementation program.

A special case of a 'greenfield' construction exists where the asset under construction was planned and construction started under the assumption that the asset would not be a Critical Asset. During construction, conditions changed, and the asset will now be a Critical Asset upon its commissioning. In this case, the Responsible Entity must follow the Category 2 milestones from the date of the determination that the asset is a Critical Asset.

Since the assets must be compliant with the NERC Reliability Standards CIP-003 through CIP-009 upon commissioning, no implementation milestones or schedules are provided herein.

Disaster Recovery and Restoration Activities

A special case of restoration as part of a disaster recovery situation (such as storm restoration) shall follow the emergency provisions of the Responsible Entity's policy required by CIP-003 R1.1.

The rationale for this is that the primary task following a disaster is the restoration of the power system, and the ability to serve customer load. Cyber security provisions are implemented to support reliability and operations. If restoration were to be slowed to ensure full implementation of the CIP compliance implementation program, restoration could be hampered, and reliability could be harmed.

However, following the completion of the restoration activities, the entity is obligated to implement the CIP compliance implementation program at the restored facilities, and be able to demonstrate full compliance in a spot-check or audit; or, file a self-report of non-compliance with a mitigation plan describing how and when full compliance will be achieved.

Newly Registered Entity Scenarios

Based on the Critical Cyber Asset identification scenarios identified above, the implementation milestone categories and schedules for those scenarios as they apply to newly Registered Entities are defined and distinguished below.

The following examples of business merger and asset acquisition scenarios may be helpful in explaining the expectations in each of the scenarios. Note that in each case, the predecessor Registered Entities are assumed to already be in compliance with NERC Reliability Standard CIP-002-4.

1. **Newly Registered Entity Scenario 1 (Application of Category 1 Milestones):**

   A Merger of Two or More Registered Entities where None of the Predecessor Registered Entities has Identified any Critical Cyber Asset
   In the case of a business merger or asset acquisition, because there are no identified Critical Cyber Assets in any of the predecessor Registered Entities, a CIP compliance implementation program is not assumed to exist. The only program component required is a Critical Asset and Critical Cyber Asset identification process per NERC Reliability Standard CIP-002-4.

   If either predecessor Registered Entities has identified Critical Assets (but without associated Critical Cyber Assets), the merged Registered Entity must continue to perform annual application of the Critical Asset identification as required in CIP-002 R1, as well as to annually verify whether associated Cyber Assets meet the requirements as newly identified Critical Cyber Assets as required by CIP-002 R2. If newly identified Critical Cyber Assets are found at any point in this process (i.e., during the one calendar year allowance period, or after that one calendar year allowance period), then the implementation milestones, categories and schedules of this Implementation Plan apply regardless of when this newly identified Critical Cyber Assets are determined, and independent of any merger and acquisition discussions contained in this Implementation Plan.

2. **Newly Registered Entity Scenario 2:**

   A Merger of Two or More Registered Entities where Only One of the Predecessor Registered Entities has Identified at Least One Critical Cyber Asset
   Since only one of the predecessor Registered Entities has previously identified Critical Cyber Assets, it is assumed that none of the other predecessor Registered Entities have CIP compliance implementation programs (since they are not required to have them). In

this case, the CIP compliance implementation program from the predecessor Registered Entity with the previously identified Critical Cyber Asset would be expected to be implemented as the CIP compliance implementation program for the merged Registered Entity, and would be expected to apply to any Critical Cyber Assets identified after the effective date of the merger. Since the other predecessor Registered Entities did not have any Critical Cyber Assets, this should present no conflict in any CIP compliance implementation programs.

Note that the discussion of the disposition of any NERC Reliability Standard CIP-002 Critical Asset identification process from Scenario 1 above would apply in this case as well.

3. **Newly Registered Entity Scenario 3:**

A Merger of Two or More Registered Entities where Two or More of the Predecessor Registered Entities has Identified at Least One Critical Cyber Asset
This scenario is the most complicated of the three, since it applies to a merged Registered Entity that has more than one CIP compliance implementation program, which are most likely not in complete agreement with each other. These differences could be due to any number of issues, ranging from something as 'simple' as selection of different anti-virus tools, to something as 'complicated' as the access authorization process.

The merged Responsible Entity has one calendar year from the effective date of the business merger to continue to operate the separate CIP compliance implementation programs while determining how to either combine the CIP compliance implementation programs, or at a minimum, operate the CIP compliance implementation programs under a common Senior Manager and governance structure.

Following the one year analysis period, if the decision is made to continue the operation of separate CIP compliance implementation programs under a common Senior Manager and governance structure, the merged Responsible Entity must update any required Senior Manager and governance issues, and clearly identify which CIP compliance implementation program components apply to each individual Critical Cyber Asset. This is essential to the implementation of the CIP compliance implementation program at the merged Responsible Entity, so that the correct and proper program components are implemented on the appropriate Critical Cyber Assets, as well as to allow the ERO compliance program (in a spot-check or audit) to determine if the CIP compliance implementation program has been properly implemented for each Critical Cyber Asset. Absent this clear identification, it would be possible for the wrong CIP compliance implementation program to be applied to a Critical Cyber Asset, or the wrong CIP compliance implementation program be evaluated in a spot-check or audit, leading to a possible technical non-compliance without real cause.

However, if after the one year analysis period, the decision is made to combine the operation of the separate CIP compliance implementation programs into a single CIP

compliance implementation program, the merged Responsible Entity must develop a plan for merging of the separate CIP compliance implementation programs into a single CIP compliance implementation program, with a schedule and milestones for completion. The programs should be combined as expeditiously as possible, but without causing harm to reliability or operability of the Bulk power System. This 'merged plan' must be made available to the ERO compliance program upon request, and as documentation for any spot-check or audit conducted while the merged plan is being performed. Progress towards meeting milestones and completing the merged plan will be verified during any spot-checks or audits conducted while the plan is being executed.

Example Scenarios

Note that there are no implementation milestones or schedules specified for a Responsible Entity that has a newly identified Critical Asset, but no newly identified Critical Cyber Assets. This situation exists because no action is required by the Responsible Entity upon identification of a Critical Asset without associated Critical Cyber Assets. Only upon identification of Critical Cyber Assets does a Responsible Entity need to become compliant with the NERC Reliability Standards CIP-003 through CIP-009.

As an example, Table 1 provides some sample scenarios, and provides the milestone category for each of the described situations.

Table 1: Example Scenarios

Scenarios	CIP Compliance Implementation Program:	
	No Program (note 1)	Existing Program
Existing asset becomes Critical Asset; associated Cyber Assets become Critical Cyber Assets	Category 1	Category 2
New asset comes online as a Critical Asset; associated Cyber Assets become Critical Cyber Asset	Category 1	Compliant upon Commissioning
Existing Cyber Asset moves into the Electronic Security Perimeter due to network reconfiguration	N/A	Compliant upon Commissioning
New Cyber Asset – never before in service and not a replacement for an existing Cyber Asset – added into a new or existing Electronic Security Perimeter	Category 1	Compliant upon Commissioning
New Cyber Asset replacing an existing Cyber Asset within the Electronic Security Perimeter	N/A	Compliant upon Commissioning
Planned modification or upgrade to existing Cyber Asset that causes it to be reclassified as a Critical Cyber Asset	Category 1	Compliant upon Commissioning
Asset under construction as another (non-critical) asset becomes declared as a Critical Asset during construction	Category 1	Category 2

Scenarios	CIP Compliance Implementation Program:	
	No Program (note 1)	Existing Program
Unplanned modification such as emergency restoration invoked under a disaster recovery situation or storm restoration	N/A	Per emergency provisions as required by CIP-003 R1.1

Note: 1) assumes the entity is already compliant with CIP-002

Table 2 provides the compliance milestones for each of the two identified milestone categories.

Table 2: Implementation milestones for Newly Identified Critical Cyber Assets[4]

CIP Standard Requirement	Milestone Category 1	Milestone Category 2
Standard CIP-002-4 — Critical Cyber Asset Identification		
R1	*N/A*	*N/A*
R2	*N/A*	*N/A*
R3	*N/A*	*N/A*
Standard CIP-003-4 — Security Management Controls		
R1	24 months	*existing*
R2	*N/A*	*existing*
R3	24 months	*existing*
R4	24 months	6 months
R5	24 months	6 months
R6	24 months	6 months
Standard CIP-004-4 — Personnel and Training		
R1	24 months	*existing*
R2	24 months	18 months
R3	24 months	18 months
R4	24 months	18 months
Standard CIP-005-4 — Electronic Security Perimeter		
R1	24 months	12 months
R2	24 months	12 months
R3	24 months	12 months
R4	24 months	12 months
R5	24 months	12 months
R6	24 months	12 months
Standard CIP-006-4 — Physical Security		
R1	24 months	12 months
R2	24 months	12 months
R3	24 months	12 months
R4	24 months	12 months
R5	24 months	12 months
R6	24 months	12 months
R7	24 months	12 months
R8	24 months	12 months

[4] For Owners and Operators of U.S. Nuclear Power Plants, Critical Cyber Assets associated with U.S. Nuclear Power Plants identified as Critical Assets shall be compliant with CIP-002-4 through CIP-009-4 by the later of (i) the milestone date listed in Table 2, or (ii) 6 months following the completion date of the first refueling outage beyond the milestone date in Table 2 for those requirements requiring a refueling outage,

CIP Standard Requirement	Milestone Category 1	Milestone Category 2
Standard CIP-007-4 — Systems Security Management		
R1	24 months	12 months
R2	24 months	12 months
R3	24 months	12 months
R4	24 months	12 months
R5	24 months	12 months
R6	24 months	12 months
R7	24 months	12 months
R8	24 months	12 months
R9	24 months	12 months
Standard CIP-008-4 — Incident Reporting and Response Planning		
R1	24 months	6 months
R2	24 months	6 months
Standard CIP-009-4 — Recovery Plans for Critical Cyber Assets		
R1	24 months	6 months
R2	24 months	12 months
R3	24 months	12 months
R4	24 months	6 months
R5	24 months	6 months

Table 3[5][6] Compliance Schedule for Standards CIP-002-4 through CIP-009-4 For Entities Registering in April 2008 and Thereafter		
Requirements	**Registration + 12 months**	**Registration + 24 months**
Standard CIP-002-4 — Critical Cyber Assets		
All Requirements		Compliant
Standard CIP-003-4 — Security Management Controls		
All Requirements Except R2		Compliant
R2	Compliant	
Standard CIP-004-4 — Personnel & Training		
All Requirements		Compliant
Standard CIP-005-4 — Electronic Security		
All Requirements		Compliant
Standard CIP-006-4 — Physical Security		
All Requirements		Compliant
Standard CIP-007-4 — Systems Security Management		
All Requirements		Compliant
Standard CIP-008-4 — Incident Reporting and Response Planning		
All Requirements		Compliant
Standard CIP-009-4 — Recovery Plans		
All Requirements		Compliant

[5] Note: This table only specifies a 'Compliant' date, consistent with the convention used elsewhere in this Implementation Plan. The Compliant dates are consistent with those specified in Table 4 of the Version 1 Implementation Plan. Other compliance states referenced in the Version 1 Implementation Plan are no longer used.
[6] For Owners and Operators of U.S. Nuclear Power Plants, Critical Cyber Assets associated with U.S. Nuclear Power Plants identified as Critical Assets shall be compliant with CIP-002-4 through CIP-009-4 by the later of (i) the milestone date listed in Table 3, or (ii) 6 months following the completion date of the first refueling outage beyond the milestone date in Table 3 for those requirements requiring a refueling outage.

Exhibit D

Standard Drafting Team Roster for Project 2008-06 Cyber Security
Order 706

Cyber Security Order 706 Standard Drafting Team (Project 2008-06)

1. **Chairman**	John Lim, CISSP Department Manager, IT Infrastructure Planning	Consolidated Edison Co. of New York 4 Irving Place Rm 349-S New York, New York 10003	(212) 460-2712 (212) 387-2100 Fx limj@coned.com
2. Vice Chairman	Philip Huff Manager, IT Security and Compliance	Arkansas Electric Cooperative Corporation 1 Cooperative Way Little Rock, Arkansas 72119	(501) 570-2444 phuff@aecc.com
3. Members	Robert Antonishen Protection and Control Manager, Hydro Engineering Division	Ontario Power Generation Inc. 14000 Niagara Parkway Niagara-on the-Lake, Ontario L0S 1J0	(905) 262-2674 (905) 262-2686 Fx rob.antonishen@opg.com
4.	Jim Brenton, CISSP-ISSAP Director, CIP Standards Development	Electric Reliability Council of Texas, Inc. 2705 West Lake Drive Taylor, Texas 76574	(512) 248-3043 (512) 248-3993 Fx jbrenton@ercot.com
5.	Jackie Collett Cyber Security Operations Engineer	Manitoba Hydro 1565 Willson Place P.O. Box 815 Winnipeg, Manitoba R3C 2P4	(204) 477-7709 jcollett@hydro.mb.ca
6.	Jay S. Cribb Information Security Analyst, Principal	Southern Company Services, Inc. 241 Ralph McGill Boulevard N.E. Bin 10034 Atlanta, Georgia 30308	(404) 506-3854 jscribb@southernco.com
7.	Joe Doetzl Manager, Information Security	Kansas City Power & Light Co. 1201 Walnut Kansas City, Missouri 64106	(816) 556-2280 joe.doetzl@kcpl.com
8.	Sharon Edwards Project Manager	Duke Energy 139 E. 4th Streets 4th & Main Cincinnati, Ohio 45202	(513) 508-1285 -cell (513) 287-1564 sharon.edwards@duke-energy.com
9.	Gerald S. Freese Director, Enterprise Information Security	American Electric Power 1 Riverside Plaza Columbus, Ohio 43215	(614) 716-2351 (614) 716-1144 Fx gsfreese@aep.com
10.	William Gross	Nuclear Energy Institute	(202) 739-8123 wrg@nei.org
11.	Jeffrey Hoffman Chief Architect IT Policy & Security Division	U.S. Bureau of Reclamation Denver Federal Center Bldg. 67, Rm. 380 PO Box 25007 (84-21200) Denver, CO 80225	(303) 445-3341 (303) 445-6307 Fx JHoffman@usbr.gov

12.	Doug Johnson Operations Support Group Transmission Operations & Planning	Exelon - Commonwealth Edison 1N301 Swift Road Lombard, IL 60148	(630) 691-4593 douglas.johnson@comed.com
13.	Patricio Leon-Alvarado Engineer, E&TS Compliance and Quality	Southern California Edison One Innovation Way Pomona, CA 91768	(909) 274-1697 (909) 274-1692 Fx Patricio.leon-alvarado@sce.com
14.	Richard Kinas Manager of Standards Compliance	Orlando Utilities Commission 6113 Pershing Avenue Orlando, Florida 32822	(407) 384-4063 rkinas@ouc.com
15.	David L. Norton Policy Consultant - CIP	Entergy Corporation 639 Loyola Avenue MS: L-MOB-17A New Orleans, Louisiana 70113	(504) 576-5469 (504) 576-5123 Fx dnorto1@entergy.com
16.	David S Revill Group Lead, Electronic Maintenance	Georgia Transmission Corporation 2100 East Exchange Place Tucker, Georgia 30084	(770) 270-7815 david.revill@gatrans.com
17.	Scott Rosenberger Director, Security and Compliance	Luminant 1601 Bryan Street 46th Floor Dallas, TX 75201	(214) 812-2412 scott.rosenberger@energyfutureholdings.com
18.	Kevin Sherlin Manager, Business Technology Operations	Sacramento Municipal Utility District 6201 S Street Sacramento, California 95817	(916) 732-6452 csherli@smud.org
19.	Jon Stanford Chief Information Security Officer	Bonneville Power Administration 905 NE 11th Avenue, JB-B1 Portland, Oregon 97232	(503) 230-4222 jkstanford@bpa.gov
20.	Thomas Stevenson Gen Supv Engineering Projects Generation Services Dept	Constellation Energy 1005 Brandon Shores Rd Baltimore, MD 21226	(410) 787-5260 (410) 227-3728 - cell Thomas.W.Stevenson@constellation.com
21.	Keith Stouffer Program Manager, Industrial Control System Security	National Institute of Standards & Technology 100 Bureau Drive Mail Stop 8230 Gaithersburg, Maryland 20899-8230	(301) 975-3877 (301) 990-9688 Fx keith.stouffer@nist.gov
22.	John Van Boxtel CIP Compliance Engineer	Western Electricity Coordinating Council Suite #201 7600 NE 41st Street Vancouver, WA 98662	(360) 713-9090 jvanboxtel@wecc.biz
23.	John D. Varnell Director, Asset Operations Analysis	Tenaska Power Services Co. 1701 East Lamar Blvd. Arlington, Texas 76006	(817) 462-1037 (817) 462-1035 Fx jvarnell@tnsk.com

24.	William Winters IS Senior Systems Consultant	Arizona Public Service Co. 502 S. 2nd Avenue Mail Station 2387 Phoenix, Arizona 85003	(602) 250-1117 William.Winters@ aps.com
25.	Bradley (Brad) Yeates IT Security Analyst, Principal	Southern Nuclear Operating Company 241 Ralph McGill Blvd. Bin 10030 Atlanta, Ga. 30308	(404) 314-4096 blyeates@southernco .com
Consultant to NERC	Hal Beardall	Florida State University Morgan Building, Suite 236 2035 East Paul Dirac Drive P.O. Box 3062777 Tallahassee, Florida 32310-4161	(850) 644-4945 (850) 644-4968 Fx hbeardall@fsu.edu
Consultant to NERC	Joseph Bucciero President and Executive Consultant	Bucciero Consulting, LLC 3011 Samantha Way Gilbertsville, Pennsylvania 19525	(267) 981-5445 joe.bucciero@ gmail.com
Consultant to NERC	Robert M. Jones Director Florida Conflict Resolution Consortium	Florida State University Morgan Building, Suite 236 2035 East Paul Dirac Drive Tallahassee, Florida 32310-4161	(850) 644-6320 (850) 644-4968 Fx rmjones@fsu.edu
Consultant to NERC	Stuart Langton, PhD Senior Fellow	Florida State University 2010 Wild Lime Drive Sanibel, Florida 33957	(239) 395-9694 (239) 395-3230 Fx slangton@ mindspring.com
NERC Staff	Herb Schrayshuen Vice President and Director of Standards	North American Electric Reliability Corporation 116-390 Village Boulevard Princeton, New Jersey 08540-5721	(609) 452-8060 (609) 452-9550 Fx Herb.schrayshuen@ nerc.net
NERC Staff	Howard L. Gugel Standards Development Coordinator	North American Electric Reliability Corporation 116-390 Village Boulevard Princeton, New Jersey 08540-5721	(609) 452-8060 (609) 452-9550 Fx howard.gugel@ nerc.net
NERC Staff	Roger Lampila Regional Compliance Auditor	North American Electric Reliability Corporation 116-390 Village Boulevard Princeton, New Jersey 08540-5721	(609) 452-8060 (609) 452-9550 Fx roger.lampila@ nerc.net
NERC Staff	Scott R Mix Manager Infrastructure Security	North American Electric Reliability Corporation 116-390 Village Boulevard Princeton, New Jersey 08540-5721	(215) 853-8204 (609) 452-9550 Fx Scott.Mix@ nerc.net
NERC Staff	David Taylor Director of Standards Development	North American Electric Reliability Corporation 116-390 Village Boulevard Princeton, New Jersey 08540-5721	(609) 452-8060 (609) 452-9550 Fx david.taylor@ nerc.net
NERC Staff	Todd Thompson Compliance Investigator	North American Electric Reliability Corporation 116-390 Village Boulevard Princeton, New Jersey 08540-5721	(609) 452-8060 (609) 452-9550 Fx todd.thompson@ nerc.net

CORRECTED Exhibit F

Table of CIP Version 4 Violation Risk Factors and Violation Severity Levels Proposed for Approval - Clean and Redline

CIP Version 4 Violation Severity Levels and Violation Risk Factors

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
CIP-002-4	R1.	Critical Asset Identification — The Responsible Entity shall develop a list of its identified Critical Assets determined through an annual application of the criteria contained in *CIP-002-4 Attachment 1 – Critical Asset Criteria*. The Responsible Entity shall update this list as necessary, and review it at least annually.	N/A	N/A	The Responsible Entity has developed a list of Critical Assets but the list has not been reviewed and updated annually as required.	The Responsible Entity did not develop a list of its identified Critical Assets even if such list is null.
CIP-002-4	R2.	Critical Cyber Asset Identification— Using the list of Critical Assets developed pursuant to Requirement R1, the Responsible Entity shall develop a list of associated Critical Cyber Assets essential to the operation of the Critical Asset. The Responsible Entity shall update this list as necessary, and review it at least annually. For each group of generating units (including nuclear generation) at a single plant location identified in Attachment 1, criterion 1.1, the only Cyber Assets that must be considered are those shared Cyber Assets that could, within 15 minutes, adversely impact the reliable operation of any combination of units that in aggregate equal or exceed Attachment 1, criterion 1.1. For the purpose of Standard CIP 002-4, Critical Cyber Assets are further qualified to be those having at least	N/A	N/A	The Responsible Entity has developed a list of associated Critical Cyber Assets essential to the operation of the Critical Asset list as per requirement R2 but the list has not been reviewed and updated annually as required.	The Responsible Entity did not develop a list of associated Critical Cyber Assets essential to the operation of the Critical Asset list as per requirement R2 even if such list is null. OR A Cyber Asset essential to the operation of the Critical Asset was identified that met at least one of the bulleted characteristics in this requirement but was not included in the Critical Cyber Asset List.

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		one of the following characteristics: • The Cyber Asset uses a routable protocol to communicate outside the Electronic Security Perimeter; or, • The Cyber Asset uses a routable protocol within a control center; or, • The Cyber Asset is dial-up accessible.				
CIP-002-4	R3.	Annual Approval —The senior manager or delegate(s) shall approve annually the list of Critical Assets and the list of Critical Cyber Assets. Based on Requirements R1 and R2 the Responsible Entity may determine that it has no Critical Assets or Critical Cyber Assets. The Responsible Entity shall keep a signed and dated record of the senior manager or delegate(s)'s approval of the list of Critical Assets and the list of Critical Cyber Assets (even if such lists are null.)	N/A	N/A	The Responsible Entity does not have a signed and dated record of the senior manager or delegate(s)'s annual approval of the list of Critical Assets. OR The Responsible Entity does not have a signed and dated record of the senior manager or delegate(s)'s annual approval of the list of Critical Cyber Assets (even if such lists are null.)	The Responsible Entity does not have a signed and dated record of the senior manager or delegate(s)'s annual approval of both the list of Critical Assets and the list of Critical Cyber Assets (even if such lists are null.)
CIP-003-4	R1.	Cyber Security Policy — The Responsible Entity shall document and implement a cyber security policy that represents management's commitment and ability to secure its Critical Cyber	N/A	N/A	N/A	The Responsible Entity has not documented or implemented a cyber security

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		Assets. The Responsible Entity shall, at minimum, ensure the following:				policy.
CIP-003-4	R1.1.	The cyber security policy addresses the requirements in Standards CIP-002-4 through CIP-009-4, including provision for emergency situations.	N/A	N/A	N/A	The Responsible Entity's cyber security policy does not address all the requirements in Standards CIP-002 through CIP-009, including provision for emergency situations.
CIP-003-4	R1.2.	The cyber security policy is readily available to all personnel who have access to, or are responsible for, Critical Cyber Assets.	N/A	N/A	N/A	The Responsible Entity's cyber security policy is not readily available to all personnel who have access to, or are responsible for, Critical Cyber Assets.
CIP-003-4	R1.3	Annual review and approval of the cyber security policy by the senior manager assigned pursuant to R2.	N/A	N/A	N/A	The Responsible Entity's senior manager, assigned pursuant to R2, did not complete the annual review and approval of its cyber security policy.
CIP-003-4	R2.	Leadership — The Responsible Entity shall assign a senior manager with overall responsibility for leading and managing the entity's implementation of, and adherence to, Standards CIP-002-4 through CIP-009-4.	N/A	N/A	N/A	The Responsible Entity has not assigned a single senior manager with overall responsibility and authority for leading and

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						managing the entity's implementation of, and adherence to, Standards CIP-002 through CIP-009.
CIP-003-4	R2.1.	The senior manager shall be identified by name, title, and date of designation.	N/A	N/A	N/A	Identification of the senior manager is missing one of the following: name, title, or date of designation.
CIP-003-4	R2.2.	Changes to the senior manager must be documented within thirty calendar days of the effective date.	N/A	N/A	N/A	Changes to the senior manager were not documented within 30 days of the effective date.
CIP-003-4	R2.3.	Where allowed by Standards CIP-002-4 through CIP-009-4, the senior manager may delegate authority for specific actions to a named delegate or delegates. These delegations shall be documented in the same manner as R2.1 and R2.2, and approved by the senior manager.	N/A	N/A	The identification of a senior manager's delegate does not include at least one of the following; name, title, or date of the designation, OR The document is not approved by the senior manager, OR	A senior manager's delegate is not identified by name, title, and date of designation; the document delegating the authority does not identify the authority being delegated; the document delegating the authority is not approved by the senior manager;

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
					Changes to the delegated authority are not documented within thirty calendar days of the effective date.	AND changes to the delegated authority are not documented within thirty calendar days of the effective date.
CIP-003-4	R2.4	The senior manager or delegate(s), shall authorize and document any exception from the requirements of the cyber security policy.	N/A	N/A	N/A	The senior manager or delegate(s) did not authorize and document any exceptions from the requirements of the cyber security policy as required.
CIP-003-4	R3.	Exceptions — Instances where the Responsible Entity cannot conform to its cyber security policy must be documented as exceptions and authorized by the senior manager or delegate(s).	N/A	N/A	In Instances where the Responsible Entity cannot conform to its cyber security policy, in R1, exceptions were documented, **but** were not authorized by the senior manager or delegate(s).	In Instances where the Responsible Entity cannot conform to its cyber security policy, in R1, exceptions were not documented.
CIP-003-4	R3.1.	Exceptions to the Responsible Entity's cyber security policy must be documented within thirty days of being approved by the senior manager or delegate(s).	N/A	N/A	N/A	Exceptions to the Responsible Entity's cyber security policy were not documented within 30 days of being approved by the senior manager or

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						delegate(s).
CIP-003-4	R3.2.	Documented exceptions to the cyber security policy must include an explanation as to why the exception is necessary and any compensating measures.	N/A	N/A	The Responsible Entity has a documented exception to the cyber security policy in R1 but did not include **either**: 1) an explanation as to why the exception is necessary, or 2) any compensating measures.	The Responsible Entity has a documented exception to the cyber security policy in R1 but did not include **both:** 1) an explanation as to why the exception is necessary, and 2) any compensating measures.
CIP-003-4	R3.3.	Authorized exceptions to the cyber security policy must be reviewed and approved annually by the senior manager or delegate(s) to ensure the exceptions are still required and valid. Such review and approval shall be documented.	N/A	N/A	N/A	Exceptions to the cyber security policy were not reviewed **or** were not approved on an annual basis by the senior manager or delegate(s) to ensure the exceptions are still required and valid or the review and approval is not documented.
CIP-003-4	R4.	Information Protection — The Responsible Entity shall implement and document a program to identify, classify, and protect information associated with Critical Cyber Assets.	N/A	N/A	N/A	The Responsible Entity did not implement or did not document a program to identify, classify, and protect

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						information associated with Critical Cyber Assets.
CIP-003-4	R4.1.	The Critical Cyber Asset information to be protected shall include, at a minimum and regardless of media type, operational procedures, lists as required in Standard CIP-002-4, network topology or similar diagrams, floor plans of computing centers that contain Critical Cyber Assets, equipment layouts of Critical Cyber Assets, disaster recovery plans, incident response plans, and security configuration information.	N/A	N/A	The information protection program does not include one of the minimum information types to be protected as detailed in R4.1.	The information protection program does not include two or more of the minimum information types to be protected as detailed in R4.1.
CIP-003-4	R4.2.	The Responsible Entity shall classify information to be protected under this program based on the sensitivity of the Critical Cyber Asset information.	N/A	N/A	N/A	The Responsible Entity did not classify the information to be protected under this program based on the sensitivity of the Critical Cyber Asset information.
CIP-003-4	R4.3.	The Responsible Entity shall, at least annually, assess adherence to its Critical Cyber Asset information protection program, document the assessment results, and implement an action plan to remediate deficiencies identified during the assessment.	N/A	N/A	N/A	The Responsible Entity did not annually assess adherence to its Critical Cyber Asset information protection program, including documentation of the assessment results, OR

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						The Responsible Entity did not implement an action plan to remediate deficiencies identified during the assessment.
CIP-003-4	R5.	Access Control — The Responsible Entity shall document and implement a program for managing access to protected Critical Cyber Asset information.	N/A	N/A	N/A	The Responsible Entity did not implement or did not document a program for managing access to protected Critical Cyber Asset information.
CIP-003-4	R5.1.	The Responsible Entity shall maintain a list of designated personnel who are responsible for authorizing logical or physical access to protected information.	N/A	N/A	The Responsible Entity maintained a list of designated personnel for authorizing either logical or physical access but not both.	The Responsible Entity did not maintain a list of designated personnel who are responsible for authorizing logical or physical access to protected information.
CIP-003-4	R5.1.1.	Personnel shall be identified by name, title, and the information for which they are responsible for authorizing access.	N/A	N/A	The Responsible Entity did identify the personnel by name, title, and the information for which they are responsible for authorizing access, but the business	Personnel are not identified by name, title, or the information for which they are responsible for authorizing access.

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
					phone is missing.	
CIP-003-4	R5.1.2.	The list of personnel responsible for authorizing access to protected information shall be verified at least annually.	N/A	N/A	N/A	The Responsible Entity did not verify at least annually the list of personnel responsible for authorizing access to protected information.
CIP-003-4	R5.2.	The Responsible Entity shall review at least annually the access privileges to protected information to confirm that access privileges are correct and that they correspond with the Responsible Entity's needs and appropriate personnel roles and responsibilities.	N/A	N/A	N/A	The Responsible Entity did not review at least annually the access privileges to protected information to confirm that access privileges are correct and that they correspond with the Responsible Entity's needs and appropriate personnel roles and responsibilities.
CIP-003-4	R5.3.	The Responsible Entity shall assess and document at least annually the processes for controlling access privileges to protected information.	N/A	N/A	N/A	The Responsible Entity did not assess and document at least annually the processes for controlling access privileges to protected information.
CIP-003-4	R6.	Change Control and Configuration Management — The Responsible	N/A	N/A	N/A	The Responsible Entity has not

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		Entity shall establish and document a process of change control and configuration management for adding, modifying, replacing, or removing Critical Cyber Asset hardware or software, and implement supporting configuration management activities to identify, control and document all entity or vendor related changes to hardware and software components of Critical Cyber Assets pursuant to the change control process.				established or documented a change control process for the activities required in R6, OR The Responsible Entity has not established or documented a configuration management process for the activities required in R6.
CIP-004-4	R1.	Awareness — The Responsible Entity shall establish, document, implement, and maintain a security awareness program to ensure personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets receive on-going reinforcement in sound security practices. The program shall include security awareness reinforcement on at least a quarterly basis using mechanisms such as: • Direct communications (e.g. emails, memos, computer based training, etc.); • Indirect communications	N/A	N/A	The Responsible[1] Entity did not provide security awareness reinforcement on at least a quarterly basis.	The Responsible Entity did not establish, implement, maintain, or document a security awareness program to ensure personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets receive on-going reinforcement in sound security

[1] Please note that FERC's January 20, 2011 Order on Version 2 And Version 3 Violation Risk Factors And Violation Severity Levels For Critical Infrastructure Protection Reliability Standards dictated "Responsible Entity" to be changed to "Responsibility Entity." NERC assumes FERC intended the VSL to read "Responsible Entity" and therefore is not making this change. NERC proposes to remove this footnote from the final approved list of VSLs.

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		(e.g. posters, intranet, brochures, etc.); • Management support and reinforcement (e.g., presentations, meetings, etc.).				practices.
CIP-004-4	R2.	Training — The Responsible Entity shall establish, document, implement, and maintain an annual cyber security training program for personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets. The cyber security training program shall be reviewed annually, at a minimum, and shall be updated whenever necessary.	N/A	N/A	The Responsible[2] Entity did not review the training program on an annual basis.	The Responsible Entity did not establish, implement, maintain, or document an annual cyber security training program for personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets.
CIP-004-4	R2.1.	This program will ensure that all personnel having such access to Critical Cyber Assets, including contractors and service vendors, are trained prior to their being granted such access except in specified circumstances such as an emergency.	N/A	N/A	N/A	Not all personnel having authorized cyber or unescorted physical access to Critical Cyber Assets, including contractors and service vendors, were trained prior to their being granted such access except in specified circumstances such as an emergency.

[2] Please see previous footnote. NERC proposes to remove this footnote from the final approved list of VSLs.

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
CIP-004-4	R2.2.	Training shall cover the policies, access controls, and procedures as developed for the Critical Cyber Assets covered by CIP-004-4, and include, at a minimum, the following required items appropriate to personnel roles and responsibilities:	N/A	N/A	N/A	The training does not include one or more of the minimum topics as detailed in R2.2.1, R2.2.2, R2.2.3, R2.2.4.
CIP-004-4	R2.2.1.	The proper use of Critical Cyber Assets;	N/A	N/A	N/A	N/A
CIP-004-4	R2.2.2.	Physical and electronic access controls to Critical Cyber Assets;	N/A	N/A	N/A	N/A
CIP-004-4	R2.2.3.	The proper handling of Critical Cyber Asset information; and,	N/A	N/A	N/A	N/A
CIP-004-4	R2.2.4.	Action plans and procedures to recover or re-establish Critical Cyber Assets and access thereto following a Cyber Security Incident.	N/A	N/A	N/A	N/A
CIP-004-4	R2.3.	The Responsible Entity shall maintain documentation that training is conducted at least annually, including the date the training was completed and attendance records.	N/A	N/A	The Responsible Entity did maintain documentation that training is conducted at least annually, but did not include attendance records.	The Responsible Entity did not maintain documentation that training is conducted at least annually, including the date the training was completed and attendance records.
CIP-004-4	R3.	Personnel Risk Assessment —The Responsible Entity shall have a documented personnel risk assessment program, in accordance with federal, state, provincial, and local laws, and subject to existing collective bargaining unit agreements, for personnel having	N/A	The Responsible Entity has a personnel risk assessment program, as stated in R3, for personnel having authorized	The Responsible Entity has a personnel risk assessment program as stated in R3, but conducted the personnel risk	The Responsible Entity does not have a documented personnel risk assessment program, as stated in R3, for personnel

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		authorized cyber or authorized unescorted physical access to Critical Cyber Assets. A personnel risk assessment shall be conducted pursuant to that program prior to such personnel being granted such access except in specified circumstances such as an emergency. The personnel risk assessment program shall at a minimum include:		cyber or authorized unescorted physical access, but the program is not documented.	assessment pursuant to that program after such personnel were granted such access except in specified circumstances such as an emergency.	having authorized cyber or authorized unescorted physical access. OR The Responsible Entity did not conduct the personnel risk assessment pursuant to that program for personnel granted such access except in specified circumstances such as an emergency.
CIP-004-4	R3.1.	The Responsible Entity shall ensure that each assessment conducted include, at least, identity verification (e.g., Social Security Number verification in the U.S.) and seven year criminal check. The Responsible Entity may conduct more detailed reviews, as permitted by law and subject to existing collective bargaining unit agreements, depending upon the criticality of the position.	N/A	N/A	The Responsible Entity did not ensure that an assessment conducted included an identity verification (e.g., Social Security Number verification in the U.S.) or a seven-year criminal check.	The Responsible Entity did not ensure that each assessment conducted include, at least, identity verification (e.g., Social Security Number verification in the U.S.) and seven-year criminal check.
CIP-004-4	R3.2.	The Responsible Entity shall update each personnel risk assessment at least every seven years after the initial personnel risk assessment or for cause.	N/A	The Responsible Entity did not update each personnel risk assessment at least	The Responsible Entity did not update each personnel risk assessment for	The Responsible Entity did not update each personnel risk assessment at least

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
				every seven years after the initial personnel risk assessment but did update it for cause when applicable.	cause (when applicable) but did at least updated it every seven years after the initial personnel risk assessment.	every seven years after the initial personnel risk assessment nor was it updated for cause when applicable.
CIP-004-4	R3.3.	The Responsible Entity shall document the results of personnel risk assessments of its personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets, and that personnel risk assessments of contractor and service vendor personnel with such access are conducted pursuant to Standard CIP-004-4.	The Responsible Entity did not document the results of personnel risk assessments for at least one individual but less than 5% of all personnel with authorized cyber or authorized unescorted physical access to Critical Cyber Assets, pursuant to Standard CIP-004.	The Responsible Entity did not document the results of personnel risk assessments for 5% or more but less than 10% of all personnel with authorized cyber or authorized unescorted physical access to Critical Cyber Assets, pursuant to Standard CIP-004.	The Responsible Entity did not document the results of personnel risk assessments for 10% or more but less than 15% of all personnel with authorized cyber or authorized unescorted physical access to Critical Cyber Assets, pursuant to Standard CIP-004.	The Responsible Entity did not document the results of personnel risk assessments for 15% or more of all personnel with authorized cyber or authorized unescorted physical access to Critical Cyber Assets, pursuant to Standard CIP-004.
CIP-004-4	R4.	Access — The Responsible Entity shall maintain list(s) of personnel with authorized cyber or authorized unescorted physical access to Critical Cyber Assets, including their specific electronic and physical access rights to Critical Cyber Assets.	The Responsible Entity did not maintain complete list(s) of personnel with authorized cyber or authorized unescorted physical access to Critical Cyber Assets, including their specific electronic and physical access rights to Critical	The Responsible Entity did not maintain complete list(s) of personnel with authorized cyber or authorized unescorted physical access to Critical Cyber Assets, including their specific electronic and physical access rights to Critical	The Responsible Entity did not maintain complete list(s) of personnel with authorized cyber or authorized unescorted physical access to Critical Cyber Assets, including their specific electronic and physical access rights to Critical	The Responsible Entity did not maintain complete list(s) of personnel with authorized cyber or authorized unescorted physical access to Critical Cyber Assets, including their specific electronic and physical access rights to Critical

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
			Cyber Assets, missing at least one individual but less than 5% of the authorized personnel.	Cyber Assets, missing 5% or more but less than 10% of the authorized personnel.	Cyber Assets, missing 10% or more but less than 15%of the authorized personnel.	Cyber Assets, missing 15% or more of the authorized personnel.
CIP-004-4	R4.1.	The Responsible Entity shall review the list(s) of its personnel who have such access to Critical Cyber Assets quarterly, and update the list(s) within seven calendar days of any change of personnel with such access to Critical Cyber Assets, or any change in the access rights of such personnel. The Responsible Entity shall ensure access list(s) for contractors and service vendors are properly maintained.	N/A	The Responsible Entity did not review the list(s) of its personnel who have access to Critical Cyber Assets quarterly.	The Responsible Entity did not update the list(s) within seven calendar days of any change of personnel with such access to Critical Cyber Assets, nor any change in the access rights of such personnel.	The Responsible Entity did not review the list(s) of all personnel who have access to Critical Cyber Assets quarterly, nor update the list(s) within seven calendar days of any change of personnel with such access to Critical Cyber Assets, nor any change in the access rights of such personnel.
CIP-004-4	R4.2.	The Responsible Entity shall revoke such access to Critical Cyber Assets within 24 hours for personnel terminated for cause and within seven calendar days for personnel who no longer require such access to Critical Cyber Assets.	N/A	The Responsible Entity did not revoke access within seven calendar days for personnel who no longer require such access to Critical Cyber Assets.	The Responsible Entity did not revoke access to Critical Cyber Assets within 24 hours for personnel terminated for cause.	The Responsible Entity did not revoke access to Critical Cyber Assets within 24 hours for personnel terminated for cause nor within seven calendar days for personnel who no longer require such access to Critical Cyber Assets.

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
CIP-005-4	R1.	Electronic Security Perimeter — The Responsible Entity shall ensure that every Critical Cyber Asset resides within an Electronic Security Perimeter. The Responsible Entity shall identify and document the Electronic Security Perimeter(s) and all access points to the perimeter(s).	N/A	N/A	N/A	The Responsible Entity did not ensure that every Critical Cyber Asset resides within an Electronic Security Perimeter. OR The Responsible Entity did not identify and document the Electronic Security Perimeter(s) and all access points to the perimeter(s).
CIP-005-4	R1.1.	Access points to the Electronic Security Perimeter(s) shall include any externally connected communication end point (for example, dial-up modems) terminating at any device within the Electronic Security Perimeter(s).	N/A	N/A	N/A	Access points to the Electronic Security Perimeter(s) do not include all externally connected communication end point (for example, dial-up modems) terminating at any device within the Electronic Security Perimeter(s).
CIP-005-4	R1.2.	For a dial-up accessible Critical Cyber Asset that uses a non-routable protocol, the Responsible Entity shall define an Electronic Security Perimeter for that single access point at the dial-up device.	N/A	N/A	N/A	For one or more dial-up accessible Critical Cyber Assets that use a non-routable protocol, the Responsible Entity did not define an Electronic

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						Security Perimeter for that single access point at the dial-up device.
CIP-005-4	R1.3.	Communication links connecting discrete Electronic Security Perimeters shall not be considered part of the Electronic Security Perimeter. However, end points of these communication links within the Electronic Security Perimeter(s) shall be considered access points to the Electronic Security Perimeter(s).	N/A	N/A	N/A	At least one end point of a communication link within the Electronic Security Perimeter(s) connecting discrete Electronic Security Perimeters was not considered an access point to the Electronic Security Perimeter.
CIP-005-4	R1.4.	Any non-critical Cyber Asset within a defined Electronic Security Perimeter shall be identified and protected pursuant to the requirements of Standard CIP-005-4.	N/A	N/A	N/A	One or more noncritical Cyber Asset within a defined Electronic Security Perimeter is not identified. OR Is not protected pursuant to the requirements of Standard CIP-005.
CIP-005-4	R1.5.	Cyber Assets used in the access control and/or monitoring of the Electronic Security Perimeter(s) shall be afforded the protective measures as a specified in Standard CIP-003-4; Standard CIP-004-4 Requirement R3; Standard CIP-005-4 Requirements R2	N/A	N/A	N/A	A Cyber Asset used in the access control and/or monitoring of the Electronic Security Perimeter(s) was not afforded one (1) or

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		and R3; Standard CIP-006-4 Requirement R3; Standard CIP-007-4 Requirements R1 and R3 through R9; Standard CIP-008-4; and Standard CIP-009-4.				more of the protective measures as specified in Standard CIP-003-4; Standard CIP-004-4 Requirement R3; Standard CIP-005-4 Requirements R2 and R3; Standard CIP-006-4c Requirements R3; Standard CIP-007-4 Requirements R1 and R3 through R9; Standard CIP-008-4; and Standard CIP-009-4.
CIP-005-4	R1.6.	The Responsible Entity shall maintain documentation of Electronic Security Perimeter(s), all interconnected Critical and non-critical Cyber Assets within the Electronic Security Perimeter(s), all electronic access points to the Electronic Security Perimeter(s) and the Cyber Assets deployed for the access control and monitoring of these access points.	N/A	N/A	N/A	The Responsible Entity did not maintain documentation of one or more of the following: Electronic Security Perimeter(s), interconnected Critical and noncritical Cyber Assets within the Electronic Security Perimeter(s), electronic access points to the Electronic Security Perimeter(s) and Cyber Assets deployed for the

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						access control and monitoring of these access points.
CIP-005-4	R2.	Electronic Access Controls — The Responsible Entity shall implement and document the organizational processes and technical and procedural mechanisms for control of electronic access at all electronic access points to the Electronic Security Perimeter(s).	N/A	N/A	N/A	The Responsible Entity did not implement or did not document the organizational processes and technical and procedural mechanisms for control of electronic access at all electronic access points to the Electronic Security Perimeter(s).
CIP-005-4	R2.1.	These processes and mechanisms shall use an access control model that denies access by default, such that explicit access permissions must be specified.	N/A	N/A	N/A	The processes and mechanisms did not use an access control model that denies access by default, such that explicit access permissions must be specified.
CIP-005-4	R2.2.	At all access points to the Electronic Security Perimeter(s), the Responsible Entity shall enable only ports and services required for operations and for monitoring Cyber Assets within the Electronic Security Perimeter, and shall document, individually or by specified grouping,	N/A	N/A	N/A	At one or more access points to the Electronic Security Perimeter(s), the Responsible Entity enabled ports and services not required for operations and for

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		the configuration of those ports and services.				monitoring Cyber Assets within the Electronic Security Perimeter, or did not document, individually or by specified grouping, the configuration of those ports and services.
CIP-005-4	R2.3.	The Responsible Entity shall implement and maintain a procedure for securing dial-up access to the Electronic Security Perimeter(s).	N/A	N/A	N/A	The Responsible Entity did not implement or maintain a procedure for securing dial-up access to the Electronic Security Perimeter(s) where applicable.
CIP-005-4	R2.4.	Where external interactive access into the Electronic Security Perimeter has been enabled, the Responsible Entity shall implement strong procedural or technical controls at the access points to ensure authenticity of the accessing party, where technically feasible.	N/A	N/A	N/A	Where external interactive access into the Electronic Security Perimeter has been enabled the Responsible Entity did not implement strong procedural or technical controls at the access points to ensure authenticity of the accessing party, where technically feasible.
CIP-005-4	R2.5.	The required documentation shall, at	N/A	N/A	N/A	The required

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		least, identify and describe:				documentation for R2 did not include one or more of the elements described in R2.5.1 through R2.5.4.
CIP-005-4	R2.5.1.	The processes for access request and authorization.	N/A	N/A	N/A	N/A
CIP-005-4	R2.5.2.	The authentication methods.	N/A	N/A	N/A	N/A
CIP-005-4	R2.5.3.	The review process for authorization rights, in accordance with Standard CIP-004-4 Requirement R4.	N/A	N/A	N/A	N/A
CIP-005-4	R2.5.4.	The controls used to secure dial-up accessible connections.	N/A	N/A	N/A	N/A
CIP-005-4	R2.6.	Appropriate Use Banner — Where technically feasible, electronic access control devices shall display an appropriate use banner on the user screen upon all interactive access attempts. The Responsible Entity shall maintain a document identifying the content of the banner.	The Responsible Entity did not maintain a document identifying the content of the banner. OR Where technically feasible less than 5% electronic access control devices did not display an appropriate use banner on the user screen upon all interactive access attempts.	Where technically feasible 5% but less than 10% of electronic access control devices did not display an appropriate use banner on the user screen upon all interactive access attempts.	Where technically feasible 10% but less than 15% of electronic access control devices did not display an appropriate use banner on the user screen upon all interactive access attempts.	Where technically feasible, 15% or more electronic access control devices did not display an appropriate use banner on the user screen upon all interactive access attempts.
CIP-005-4	R3.	Monitoring Electronic Access — The Responsible Entity shall implement	N/A	N/A	N/A	The Responsible Entity did not

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		and document an electronic or manual process(es) for monitoring and logging access at access points to the Electronic Security Perimeter(s) twenty-four hours a day, seven days a week.				implement or did not document electronic or manual processes monitoring and logging access points.
CIP-005-4	R3.1.	For dial-up accessible Critical Cyber Assets that use non-routable protocols, the Responsible Entity shall implement and document monitoring process(es) at each access point to the dial-up device, where technically feasible.	N/A	N/A	N/A	Where technically feasible, the Responsible Entity did not implement or did not document electronic or manual processes for monitoring at one or more access points to dial-up devices.
CIP-005-4	R3.2.	Where technically feasible, the security monitoring process(es) shall detect and alert for attempts at or actual unauthorized accesses. These alerts shall provide for appropriate notification to designated response personnel. Where alerting is not technically feasible, the Responsible Entity shall review or otherwise assess access logs for attempts at or actual unauthorized accesses at least every ninety calendar days.	N/A	N/A	N/A	Where technically feasible, the Responsible Entity did not implement security monitoring process(es) to detect and alert for attempts at or actual unauthorized accesses. OR The above alerts do not provide for appropriate notification to designated response personnel. OR

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						Where alerting is not technically feasible, the Responsible Entity did not review or otherwise assess access logs for attempts at or actual unauthorized accesses at least every ninety calendar days.
CIP-005-4	R4.	Cyber Vulnerability Assessment — The Responsible Entity shall perform a cyber vulnerability assessment of the electronic access points to the Electronic Security Perimeter(s) at least annually. The vulnerability assessment shall include, at a minimum, the following:	N/A	N/A	N/A	The Responsible Entity did not perform a Vulnerability Assessment at least annually for one or more of the access points to the Electronic Security Perimeter(s). OR The vulnerability assessment did not include one (1) or more of the subrequirements R4.1, R4.2, R4.3, R4.4, R4.5.
CIP-005-4	R4.1.	A document identifying the vulnerability assessment process;	N/A	N/A	N/A	N/A
CIP-005-4	R4.2.	A review to verify that only ports and services required for operations at these access	N/A	N/A	N/A	N/A

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		points are enabled;				
CIP-005-4	R4.3.	The discovery of all access points to the Electronic Security Perimeter;	N/A	N/A	N/A	N/A
CIP-005-4	R4.4.	A review of controls for default accounts, passwords, and network management community strings;	N/A	N/A	N/A	N/A
CIP-005-4	R4.5.	Documentation of the results of the assessment, the action plan to remediate or mitigate vulnerabilities identified in the assessment, and the execution status of that action plan.	N/A	N/A	N/A	N/A
CIP-005-4	R5.	Documentation Review and Maintenance — The Responsible Entity shall review, update, and maintain all documentation to support compliance with the requirements of Standard CIP-005-4.	The Responsible Entity did not review, update, and maintain at least one but less than or equal to 5% of the documentation to support compliance with the requirements of Standard CIP-005.	The Responsible Entity did not review, update, and maintain greater than 5% but less than or equal to 10% of the documentation to support compliance with the requirements of Standard CIP-005.	The Responsible Entity did not review, update, and maintain greater than 10% but less than or equal to 15% of the documentation to support compliance with the requirements of Standard CIP-005.	The Responsible Entity did not review, update, and maintain greater than 15% of the documentation to support compliance with the requirements of Standard CIP-005.
CIP-005-4	R5.1.	The Responsible Entity shall ensure that all documentation required by Standard CIP-005-4 reflect current configurations and processes and shall review the documents and procedures referenced in Standard CIP-005-4 at least annually.	N/A	The Responsible Entity did not provide evidence of an annual review of the documents and procedures referenced in Standard CIP-005.	The Responsible Entity did not document current configurations and processes referenced in Standard CIP-005.	The Responsible Entity did not document current configurations and processes and did not review the documents and procedures referenced in Standard CIP-005 at least annually.
CIP-005-4	R5.2.	The Responsible Entity shall update	N/A	N/A	N/A	The Responsible

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		the documentation to reflect the modification of the network or controls within ninety calendar days of the change.				Entity did not update documentation to reflect a modification of the network or controls within ninety calendar days of the change.
CIP-005-4	R5.3.	The Responsible Entity shall retain electronic access logs for at least ninety calendar days. Logs related to reportable incidents shall be kept in accordance with the requirements of Standard CIP-008-4.	The Responsible Entity retained electronic access logs for 75 or more calendar days, but for less than 90 calendar days.	The Responsible Entity retained electronic access logs for 60 or more calendar days, but for less than 75 calendar days.	The Responsible Entity retained electronic access logs for 45 or more calendar days, but for less than 60 calendar days.	The Responsible Entity retained electronic access logs for less than 45 calendar days.
CIP-006-4c	R1.	Physical Security Plan — The Responsible Entity shall document, implement, and maintain a physical security plan, approved by the senior manager or delegate(s) that shall address, at a minimum, the following:	N/A	N/A	The Responsible Entity created a physical security plan but did not gain approval by a senior manager or delegate(s). OR The Responsible Entity created and implemented but did not maintain a physical security plan.	The Responsible Entity did not document, implement, and maintain a physical security plan.
CIP-006-4c	R1.1.	All Cyber Assets within an Electronic Security Perimeter shall reside within an identified Physical Security	N/A	N/A	N/A	The Responsible Entity's physical security plan does

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		Perimeter. Where a completely enclosed ("six-wall") border cannot be established, the Responsible Entity shall deploy and document alternative measures to control physical access to such Cyber Assets.				not include processes to ensure and document that all Cyber Assets within an Electronic Security Perimeter also reside within an identified Physical Security Perimeter. OR Where a completely enclosed ("six-wall") border cannot be established, the Responsible Entity has not deployed or documented alternative measures to control physical access to such Cyber Assets within the Electronic Security Perimeter.
CIP-006-4c	R1.2.	Identification of all physical access points through each Physical Security Perimeter and measures to control entry at those access points.	N/A	N/A	N/A	The Responsible Entity's physical security plan does not identify all access points through each Physical Security Perimeter or does not identify measures to control entry at those

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						access points.
CIP-006-4c	R1.3	Processes, tools, and procedures to monitor physical access to the perimeter(s).	N/A	N/A	N/A	The Responsible Entity's physical security plan does not include processes, tools, and procedures to monitor physical access to the perimeter(s).
CIP-006-4c	R1.4	Appropriate use of physical access controls as described in Requirement R4 including visitor pass management, response to loss, and prohibition of inappropriate use of physical access controls.	N/A	N/A	N/A	The Responsible Entity's physical security plan does not address the appropriate use of physical access controls as described in Requirement R4.
CIP-006-4c	R1.5	Review of access authorization requests and revocation of access authorization, in accordance with CIP-004-4 Requirement R4.	N/A	N/A	N/A	The Responsible Entity's physical security plan does not address the review of access authorization requests or the revocation of access authorization, in accordance with CIP-004-4 Requirement R4.
CIP-006-4c	R1.6	A visitor control program for visitors (personnel without authorized unescorted access to a Physical Security Perimeter), containing at a minimum the following:	N/A	N/A	N/A	The Responsible Entity did not include or implement a visitor control program in

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						its physical security plan or it does not meet the requirements of continuous escort.
CIP-006-4c	R1.6.1	Logs (manual or automated) to document the entry and exit of visitors, including the date and time, to and from Physical Security Perimeters.	N/A	N/A	N/A	N/A
CIP-006-4c	R1.6.2	Continuous escorted access of visitors within the Physical Security Perimeter	N/A	N/A	N/A	N/A
CIP-006-4c	R1.7	Update of the physical security plan within thirty calendar days of the completion of any physical security system redesign or reconfiguration, including, but not limited to, addition or removal of access points through the Physical Security Perimeter, physical access controls, monitoring controls, or logging controls.	N/A	N/A	N/A	The Responsible Entity's physical security plan does not address r updating the physical security plan within-thirty calendar days of the completion of a physical security system redesign or within thirty calendar days of the completion of a reconfiguration. OR The plan was not updated within thirty calendar days of the completion of

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						a physical security system redesign or reconfiguration
CIP-006-4c	R1.8	Annual review of the physical security plan.	N/A	N/A	N/A	The Responsible Entity's physical security plan does not address a process for ensuring that the physical security plan is reviewed at least annually.
CIP-006-4c	R2	Protection of Physical Access Control Systems — Cyber Assets that authorize and/or log access to the Physical Security Perimeter(s), exclusive of hardware at the Physical Security Perimeter access point such as electronic lock control mechanisms and badge readers, shall:	N/A	N/A	N/A	A Cyber Asset that authorizes and/or logs access to the Physical Security Perimeter(s), exclusive of hardware at the Physical Security Perimeter access point such as electronic lock control mechanisms and badge readers, was not protected from unauthorized physical access. OR A Cyber Asset that authorizes and/or logs access to the Physical Security Perimeter(s),

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						exclusive of hardware at the Physical Security Perimeter access point such as electronic lock control mechanisms and badge readers was not afforded the protective measures specified in Standard CIP-003-4; Standard CIP-004-4 Requirement R3; Standard CIP-005-4 Requirements R2 and R3; Standard CIP-006-4c Requirements R4 and R5; Standard CIP-007-4; Standard CIP-008-4; and Standard CIP-009-4.
CIP-006-4c	R2.1.	Be protected from unauthorized physical access.	N/A	N/A	N/A	N/A
CIP-006-4c	R2.2.	Be afforded the protective measures specified in Standard CIP-003-4; Standard CIP-004-4 Requirement R3; Standard CIP-005-4 Requirements R2 and R3; Standard CIP-006-4a Requirements R4 and R5; Standard CIP-007-4; Standard CIP-008-4; and Standard CIP-009-4.	N/A	N/A	N/A	N/A
CIP-006-4c	R3	Protection of Electronic Access Control Systems — Cyber Assets	N/A	N/A	N/A	A Cyber Assets used in the access control

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		used in the access control and/or monitoring of the Electronic Security Perimeter(s) shall reside within an identified Physical Security Perimeter.				and/or monitoring of the Electronic Security Perimeter(s) does not reside within an identified Physical Security Perimeter.
CIP-006-4c	R4	Physical Access Controls — The Responsible Entity shall document and implement the operational and procedural controls to manage physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week. The Responsible Entity shall implement one or more of the following physical access methods: • Card Key: A means of electronic access where the access rights of the card holder are predefined in a computer database. Access rights may differ from one perimeter to another. • Special Locks: These include, but are not limited to, locks with "restricted key" systems, magnetic locks that can be operated remotely, and "man-trap" systems. • Security Personnel: Personnel responsible for controlling physical access who may reside on-site or at a monitoring station.	N/A	N/A	N/A	The Responsible Entity has not documented or has not implemented the operational and procedural controls to manage physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week using one or more of the following physical access methods: • Card Key: A means of electronic access where the access rights of the card holder are predefined in a computer database. Access rights may differ from one perimeter to another. • Special Locks: These include, but

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		• Other Authentication Devices: Biometric, keypad, token, or other equivalent devices that control physical access to the Critical Cyber Assets				are not limited to, locks with "restricted key" systems, magnetic locks that can be operated remotely, and "man-trap" systems. • Security Personnel: Personnel responsible for controlling physical access who may reside on-site or at a monitoring station. • Other Authentication Devices: Biometric, keypad, token, or other equivalent devices that control physical access to the Critical Cyber Assets.
CIP-006-4c	R5	Monitoring Physical Access — The Responsible Entity shall document and implement the technical and procedural controls for monitoring physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week. Unauthorized access attempts shall be reviewed immediately and handled in accordance with the procedures specified in Requirement CIP-008-4.	N/A	N/A.	N/A	The Responsible Entity **has not documented or has not implemented** the technical and procedural controls for monitoring physical access at all access points to the Physical Security Perimeter(s)

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		One or more of the following monitoring methods shall be used: • Alarm Systems: Systems that alarm to indicate a door, gate or window has been opened without authorization. These alarms must provide for immediate notification to personnel responsible for response. • Human Observation of Access Points: Monitoring of physical access points by authorized personnel as specified in Requirement R4.				twenty-four hours a day, seven days a week using one or more of the following monitoring methods: • Alarm Systems: Systems that alarm to indicate a door, gate or window has been opened without authorization. These alarms must provide for immediate notification to personnel responsible for response. • Human Observation of Access Points: Monitoring of physical access points by authorized personnel as specified in Requirement R4. OR An unauthorized access attempt was not reviewed immediately and

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						handled in accordance with CIP-008-4.
CIP-006-4c	R6	Logging Physical Access — Logging shall record sufficient information to uniquely identify individuals and the time of access twenty-four hours a day, seven days a week. The Responsible Entity shall implement and document the technical and procedural mechanisms for logging physical entry at all access points to the Physical Security Perimeter(s) using one or more of the following logging methods or their equivalent: • Computerized Logging: Electronic logs produced by the Responsible Entity's selected access control and monitoring method. • Video Recording: Electronic capture of video images of sufficient quality to determine identity. • Manual Logging: A log book or sign-in sheet, or other record of physical access maintained by security or other personnel authorized to control and monitor physical access as specified in Requirement R4		N/A	N/A	The Responsible Entity **has not implemented or has not documented** the technical and procedural mechanisms for logging physical entry at all access points to the Physical Security Perimeter(s) using one or more of the following logging methods or their equivalent: • Computerized Logging: Electronic logs produced by the Responsible Entity's selected access control and monitoring method, • Video Recording: Electronic capture of video images of sufficient quality to determine identity, or • Manual Logging: A log book or sign-in sheet, or other record of physical access maintained

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						by security or other personnel authorized to control and monitor physical access as specified in Requirement R4. OR The Responsible Entity has not recorded sufficient information to uniquely identify individuals and the time of access twenty-four hours a day, seven days a week.
CIP-006-4c	R7	Access Log Retention — The responsible entity shall retain physical access logs for at least ninety calendar days. Logs related to reportable incidents shall be kept in accordance with the requirements of Standard CIP-008-4.	N/A	N/A	N/A	The responsible entity did not retain physical access logs for at least ninety calendar days.
CIP-006-4c	R8	Maintenance and Testing — The Responsible Entity shall implement a maintenance and testing program to ensure that all physical security systems under Requirements R4, R5, and R6 function properly. The program must include, at a minimum, the following:	N/A	N/A	N/A	The Responsible Entity has not implemented a maintenance and testing program to ensure that all physical security systems under Requirements R4,

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						R5, and R6 function properly. OR The implemented program does not include one or more of the requirements; R8.1, R8.2, and R8.3.
CIP-006-4c	R8.1	Testing and maintenance of all physical security mechanisms on a cycle no longer than three years.	N/A	N/A	N/A	N/A
CIP-006-4c	R8.2	Retention of testing and maintenance records for the cycle determined by the Responsible Entity in Requirement R8.1.	N/A	N/A	N/A	N/A
CIP-006-4c	R8.3	Retention of outage records regarding access controls, logging, and monitoring for a minimum of one calendar year.	N/A	N/A	N/A	N/A
CIP-007-4	R1.	Test Procedures — The Responsible Entity shall ensure that new Cyber Assets and significant changes to existing Cyber Assets within the Electronic Security Perimeter do not adversely affect existing cyber security controls. For purposes of Standard CIP-007-4, a significant change shall, at a minimum, include implementation of security patches, cumulative service packs, vendor releases, and version upgrades of operating systems, applications, database platforms, or other third-	N/A	N/A	N/A	The Responsible Entity did not ensure the prevention of adverse affects described in R1, by not including the required minimum significant changes. OR The Responsible Entity did not address one or more of the following:

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		party software or firmware.				R1.1, R1.2, R1.3.
CIP-007-4	R1.1.	The Responsible Entity shall create, implement, and maintain cyber security test procedures in a manner that minimizes adverse effects on the production system or its operation.	N/A	N/A	N/A	N/A
CIP-007-4	R1.2.	The Responsible Entity shall document that testing is performed in a manner that reflects the production environment.	N/A	N/A	N/A	N/A
CIP-007-4	R1.3.	The Responsible Entity shall document test results.	N/A	N/A	N/A	N/A
CIP-007-4	R2.	Ports and Services — The Responsible Entity shall establish, document and implement a process to ensure that only those ports and services required for normal and emergency operations are enabled.	N/A	N/A	N/A	The Responsible Entity did not establish (implement) or did not document a process to ensure that only those ports and services required for normal and emergency operations are enabled.
CIP-007-4	R2.1.	The Responsible Entity shall enable only those ports and services required for normal and emergency operations.	N/A	N/A	N/A	The Responsible Entity enabled one or more ports or services not required for normal and emergency operations on Cyber Assets inside the Electronic Security Perimeter(s).

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
CIP-007-4	R2.2.	The Responsible Entity shall disable other ports and services, including those used for testing purposes, prior to production use of all Cyber Assets inside the Electronic Security Perimeter(s).	N/A	N/A	N/A	The Responsible Entity did not disable one or more other ports or services, including those used for testing purposes, prior to production use for Cyber Assets inside the Electronic Security Perimeter(s).
CIP-007-4	R2.3.	In the case where unused ports and services cannot be disabled due to technical limitations, the Responsible Entity shall document compensating measure(s) applied to mitigate risk exposure.	N/A	N/A	N/A	For cases where unused ports and services cannot be disabled due to technical limitations, the Responsible Entity did not document compensating measure(s) applied to mitigate risk.
CIP-007-4	R3.	Security Patch Management — The Responsible Entity, either separately or as a component of the documented configuration management process specified in CIP-003-4 Requirement R6, shall establish, document and implement a security patch management program for tracking, evaluating, testing, and installing applicable cyber security software patches for all Cyber Assets within the Electronic Security Perimeter(s).	N/A	N/A	N/A	The Responsible Entity **did not establish (implement) or did not document**, either separately or as a component of the documented configuration management process specified in CIP-003-4 Requirement R6, a

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						security patch management program for tracking, evaluating, testing, and installing applicable cyber security software patches for all Cyber Assets within the Electronic Security Perimeter(s).
CIP-007-4	R3.1.	The Responsible Entity shall document the assessment of security patches and security upgrades for applicability within thirty calendar days of availability of the patches or upgrades.	N/A	N/A	N/A	The Responsible Entity did not document the assessment of security patches and security upgrades for applicability as required in Requirement R3 within 30 calendar days after the availability of the patches and upgrades.
CIP-007-4	R3.2.	The Responsible Entity shall document the implementation of security patches. In any case where the patch is not installed, the Responsible Entity shall document compensating measure(s) applied to mitigate risk exposure.	N/A	N/A	N/A	The Responsible Entity did not document the implementation of applicable security patches as required in R3. OR Where an applicable patch was not

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						installed, the Responsible Entity did not document the compensating measure(s) applied to mitigate risk.
CIP-007-4	R4.	Malicious Software Prevention — The Responsible Entity shall use anti-virus software and other malicious software ("malware") prevention tools, where technically feasible, to detect, prevent, deter, and mitigate the introduction, exposure, and propagation of malware on all Cyber Assets within the Electronic Security Perimeter(s).	N/A	N/A	N/A	The Responsible Entity, where technically feasible, did not use anti-virus software or other malicious software ("malware") prevention tools, on one or more Cyber Assets within the Electronic Security Perimeter(s).
CIP-007-4	R4.1.	The Responsible Entity shall document and implement anti-virus and malware prevention tools. In the case where anti-virus software and malware prevention tools are not installed, the Responsible Entity shall document compensating measure(s) applied to mitigate risk exposure.	N/A	N/A	N/A	The Responsible Entity did not document the implementation of antivirus and malware prevention tools for cyber assets within the electronic security perimeter. OR The Responsible Entity did not document the implementation of

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						compensating measure(s) applied to mitigate risk exposure where antivirus and malware prevention tools are not installed.
CIP-007-4	R4.2.	The Responsible Entity shall document and implement a process for the update of anti-virus and malware prevention "signatures." The process must address testing and installing the signatures.	N/A	N/A	N/A	The Responsible Entity **did not document or did not implement** a process including addressing testing and installing the signatures for the update of anti-virus and malware prevention "signatures."
CIP-007-4	R5.	Account Management — The Responsible Entity shall establish, implement, and document technical and procedural controls that enforce access authentication of, and accountability for, all user activity, and that minimize the risk of unauthorized system access.	N/A	N/A	N/A	The Responsible Entity did not document or did not implement technical and procedural controls that enforce access authentication of, and accountability for, all user activity.
CIP-007-4	R5.1.	The Responsible Entity shall ensure that individual and shared system accounts and authorized access permissions are consistent with the concept of "need to know" with respect to work functions	N/A	N/A	N/A	The Responsible Entity did not ensure that individual and shared system accounts and authorized access

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		performed.				permissions are consistent with the concept of "need to know" with respect to work functions performed.
CIP-007-4	R5.1.1.	The Responsible Entity shall ensure that user accounts are implemented as approved by designated personnel. Refer to Standard CIP-003-4 Requirement R5.	N/A	N/A	N/A	One or more user accounts implemented by the Responsible Entity were not implemented as approved by designated personnel.
CIP-007-4	R5.1.2.	The Responsible Entity shall establish methods, processes, and procedures that generate logs of sufficient detail to create historical audit trails of individual user account access activity for a minimum of ninety days.	N/A	The Responsible Entity generated logs with sufficient detail to create historical audit trails of individual user account access activity, however the logs do not contain activity for a minimum of 90 days.	The Responsible Entity generated logs with insufficient detail to create historical audit trails of individual user account access activity.	The Responsible Entity did not generate logs of individual user account access activity.
CIP-007-4	R5.1.3.	The Responsible Entity shall review, at least annually, user accounts to verify access privileges are in accordance with Standard CIP-003-4 Requirement R5 and Standard CIP-004-4 Requirement R4.	N/A	N/A	N/A	The Responsible Entity did not review, at least annually, user accounts to verify access privileges are in accordance with Standard CIP-003-4 Requirement

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						R5 and Standard CIP-004-4 Requirement R4.
CIP-007-4	R5.2.	The Responsible Entity shall implement a policy to minimize and manage the scope and acceptable use of administrator, shared, and other generic account privileges including factory default accounts.	N/A	N/A	N/A	The Responsible Entity did not implement a policy to minimize and manage the scope and acceptable use of administrator, shared, and other generic account privileges including factory default accounts.
CIP-007-4	R5.2.1.	The policy shall include the removal, disabling, or renaming of such accounts where possible. For such accounts that must remain enabled, passwords shall be changed prior to putting any system into service.	N/A	N/A	The Responsible Entity's policy did not include the removal, disabling, or renaming of such accounts where possible, however for accounts that must remain enabled, passwords were changed prior to putting any system into service.	For accounts that must remain enabled, the Responsible Entity did not change passwords prior to putting any system into service.
CIP-007-4	R5.2.2.	The Responsible Entity shall identify those individuals with access to shared accounts.	N/A	N/A	N/A	The Responsible Entity did not identify all individuals with access to shared accounts.
CIP-007-4	R5.2.3.	Where such accounts must be shared, the Responsible Entity shall	N/A	N/A	N/A	Where such

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		have a policy for managing the use of such accounts that limits access to only those with authorization, an audit trail of the account use (automated or manual), and steps for securing the account in the event of personnel changes (for example, change in assignment or termination).				accounts must be shared, the Responsible Entity has not implemented (one or more components of) a policy for managing the use of such accounts that limits access to only those with authorization, an audit trail of the account use (automated or manual), and steps for securing the account in the event of personnel changes (for example, change in assignment or termination).
CIP-007-4	R5.3.	At a minimum, the Responsible Entity shall require and use passwords, subject to the following, as technically feasible:	N/A	N/A	N/A	The Responsible Entity **does not require passwords** subject to R5.3.1, R5.3.2, R5.3.3. OR **Does not use passwords** subject to R5.3.1, R5.3.2, R5.3.3.
CIP-007-4	R5.3.1.	Each password shall be a minimum of six characters.	N/A	N/A	N/A	N/A

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
CIP-007-4	R5.3.2.	Each password shall consist of a combination of alpha, numeric, and “special” characters.	N/A	N/A	N/A	N/A
CIP-007-4	R5.3.3.	Each password shall be changed at least annually, or more frequently based on risk.	N/A	N/A	N/A	N/A
CIP-007-4	R6.	Security Status Monitoring — The Responsible Entity shall ensure that all Cyber Assets within the Electronic Security Perimeter, as technically feasible, implement automated tools or organizational process controls to monitor system events that are related to cyber security.	N/A	N/A	N/A	The Responsible Entity as technically feasible, did not implement automated tools or organizational process controls, to monitor system events that are related to cyber security on one or more of Cyber Assets inside the Electronic Security Perimeter(s).
CIP-007-4	R6.1.	The Responsible Entity shall implement and document the organizational processes and technical and procedural mechanisms for monitoring for security events on all Cyber Assets within the Electronic Security Perimeter.	N/A	N/A	N/A	The Responsible Entity **did not implement or did not document** the organizational processes and technical and procedural mechanisms for monitoring for security events on all Cyber Assets within the Electronic Security Perimeter.
CIP-007-4	R6.2.	The security monitoring controls	N/A	N/A	N/A	The Responsible

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		shall issue automated or manual alerts for detected Cyber Security Incidents.				entity's security monitoring controls do not issue automated or manual alerts for detected Cyber Security Incidents.
CIP-007-4	R6.3.	The Responsible Entity shall maintain logs of system events related to cyber security, where technically feasible, to support incident response as required in Standard CIP-008-4.	N/A	N/A	N/A	The Responsible Entity did not maintain logs of system events related to cyber security, where technically feasible, to support incident response as required in Standard CIP-008.
CIP-007-4	R6.4.	The Responsible Entity shall retain all logs specified in Requirement R6 for ninety calendar days.	N/A	N/A	N/A	The Responsible Entity did not retain one or more of the logs specified in Requirement R6 for at least 90 calendar days.
CIP-007-4	R6.5.	The Responsible Entity shall review logs of system events related to cyber security and maintain records documenting review of logs.	N/A	N/A	N/A	The Responsible Entity did not review logs of system events related to cyber security nor maintain records documenting review of logs.
CIP-007-4	R7.	Disposal or Redeployment — The Responsible Entity shall establish	N/A	N/A	The Responsible Entity established	The Responsible Entity did not

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		and implement formal methods, processes, and procedures for disposal or redeployment of Cyber Assets within the Electronic Security Perimeter(s) as identified and documented in Standard CIP-005-4.			and implemented formal methods, processes, and procedures for redeployment of Cyber Assets within the Electronic Security Perimeter(s) as identified and documented in Standard CIP-005-4 **but** did not address redeployment as specified in R7.2.	establish or implement formal methods, processes, and procedures for disposal or redeployment of Cyber Assets within the Electronic Security Perimeter(s) as identified and documented in Standard CIP-005-4. OR The Responsible Entity established formal methods, processes, and procedures for redeployment of Cyber Assets within the Electronic Security Perimeter(s) as identified and documented in Standard CIP-005-4 but did not address disposal as specified in R7.1. OR The Responsible Entity did not

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						maintain records pertaining to disposal or[3] redeployment as specified in R7.3.
CIP-007-4	R7.1.	Prior to the disposal of such assets, the Responsible Entity shall destroy or erase the data storage media to prevent unauthorized retrieval of sensitive cyber security or reliability data.	N/A	N/A	N/A	N/A
CIP-007-4	R7.2.	Prior to redeployment of such assets, the Responsible Entity shall, at a minimum, erase the data storage media to prevent unauthorized retrieval of sensitive cyber security or reliability data.	N/A	N/A	N/A	N/A
CIP-007-4	R7.3.	The Responsible Entity shall maintain records that such assets were disposed of or redeployed in accordance with documented procedures.	N/A	N/A	N/A	N/A
CIP-007-4	R8	Cyber Vulnerability Assessment — The Responsible Entity shall perform a cyber vulnerability assessment of all Cyber Assets within the Electronic Security Perimeter at least annually. The vulnerability assessment shall include, at a minimum, the following:	N/A	N/A	N/A	The Responsible Entity did not perform a Vulnerability Assessment on one or more Cyber Assets within the Electronic Security Perimeter at least annually.

[3] Please note that FERC's January 20, 2011 Order on Version 2 And Version 3 Violation Risk Factors And Violation Severity Levels For Critical Infrastructure Protection Reliability Standards dictated that this should read "…records pertaining to disposal **of** redeployment as specified in R7.3." (Emphasis added) It has come to NERC's attention that it should read "…records pertaining to disposal **or** redeployment as specified in R7.3." (emphasis added) and NERC has made this change accordingly. NERC proposes to remove this footnote from the final approved list of VSLs.

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						OR The vulnerability assessment did not include one (1) or more of the subrequirements 8.1, 8.2, 8.3, 8.4.
CIP-007-4	R8.1.	A document identifying the vulnerability assessment process;	N/A	N/A	N/A	N/A
CIP-007-4	R8.2.	A review to verify that only ports and services required for operation of the Cyber Assets within the Electronic Security Perimeter are enabled;	N/A	N/A	N/A	N/A
CIP-007-4	R8.3.	A review of controls for default accounts; and,	N/A	N/A	N/A	N/A
CIP-007-4	R8.4.	Documentation of the results of the assessment, the action plan to remediate or mitigate vulnerabilities identified in the assessment, and the execution status of that action plan.	N/A	N/A	N/A	N/A
CIP-007-4	R9	Documentation Review and Maintenance — The Responsible Entity shall review and update the documentation specified in Standard CIP-007-4 at least annually. Changes resulting from modifications to the systems or controls shall be documented within thirty calendar days of the change being completed.	N/A	N/A	The Responsible Entity did not review and update the documentation specified in Standard CIP-007-4 at least annually. OR The Responsible Entity did not document changes resulting from modifications to the	The Responsible Entity did not review and update the documentation specified in Standard CIP-007-4 at least annually **and** changes resulting from modifications to the systems or controls were not documented within thirty calendar days of the change being

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
					systems or controls within thirty calendar days of the change being completed.	completed.
CIP-008-4	R1.	Cyber Security Incident Response Plan — The Responsible Entity shall develop and maintain a Cyber Security Incident response plan and implement the plan in response to Cyber Security Incidents. The Cyber Security Incident response plan shall address, at a minimum, the following:	N/A	N/A	The Responsible Entity has developed a Cyber Security Incident response plan that addresses all of the components required by R1.1 through R1.6 but has not maintained the plan in accordance with those components.	The Responsible Entity has not developed a Cyber Security Incident response plan that addresses all of the components required by R1.1 through R1.6, or has not implemented the plan in response to a Cyber Security Incident.
CIP-008-4	R1.1.	Procedures to characterize and classify events as reportable Cyber Security Incidents.	N/A	N/A	N/A	N/A
CIP-008-4	R1.2.	Response actions, including roles and responsibilities of Cyber Security Incident response teams, Cyber Security Incident handling procedures, and communication plans.	N/A	N/A	N/A	N/A
CIP-008-4	R1.3.	Process for reporting Cyber Security Incidents to the Electricity Sector Information Sharing and Analysis Center (ES-ISAC). The Responsible Entity must ensure that all reportable Cyber Security Incidents are reported to the ES-ISAC either directly or through an intermediary.	N/A	N/A	N/A	N/A
CIP-008-4	R1.4.	Process for updating the Cyber	N/A	N/A	N/A	N/A

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		Security Incident response plan within thirty calendar days of any changes.				
CIP-008-4	R1.5.	Process for ensuring that the Cyber Security Incident response plan is reviewed at least annually.	N/A	N/A	N/A	N/A
CIP-008-4	R1.6.	Process for ensuring the Cyber Security Incident response plan is tested at least annually. A test of the Cyber Security Incident response plan can range from a paper drill, to a full operational exercise, to the response to an actual incident.	N/A	N/A	N/A	N/A
CIP-008-4	R2	Cyber Security Incident Documentation — The Responsible Entity shall keep relevant documentation related to Cyber Security Incidents reportable per Requirement R1.1 for three calendar years.	N/A	N/A	N/A	The Responsible Entity has not kept relevant documentation related to Cyber Security Incidents reportable per Requirement R1.1 for at least three calendar years.
CIP-009-4	R1	Recovery Plans — The Responsible Entity shall create and annually review recovery plan(s) for Critical Cyber Assets. The recovery plan(s) shall address at a minimum the following:	N/A	N/A	N/A	The Responsible Entity has not created or has not annually reviewed their recovery plan(s) for Critical Cyber Assets OR has created a plan but did not address one or more of the requirements CIP-009-4 R1.1 **and** R1.2.

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
CIP-009-4	R1.1.	Specify the required actions in response to events or conditions of varying duration and severity that would activate the recovery plan(s).	N/A	N/A	N/A	N/A
CIP-009-4	R1.2.	Define the roles and responsibilities of responders.	N/A	N/A	N/A	N/A
CIP-009-4	R2	Exercises — The recovery plan(s) shall be exercised at least annually. An exercise of the recovery plan(s) can range from a paper drill, to a full operational exercise, to recovery from an actual incident.	N/A	N/A	N/A	The Responsible Entity's recovery plan(s) have not been exercised at least annually.
CIP-009-4	R3	Change Control — Recovery plan(s) shall be updated to reflect any changes or lessons learned as a result of an exercise or the recovery from an actual incident. Updates shall be communicated to personnel responsible for the activation and implementation of the recovery plan(s) within thirty calendar days of the change being completed.	N/A	N/A	N/A	The Responsible Entity's recovery plan(s) have not been updated to reflect any changes or lessons learned as a result of an exercise or the recovery from an actual incident. OR The Responsible Entity's recovery plan(s) have been updated to reflect any changes or lessons learned as a result of an exercise or the recovery from an actual incident but the updates

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						were not communicated to personnel responsible for the activation and implementation of the recovery plan(s) within thirty calendar days of the change.
CIP-009-4	R4	Backup and Restore — The recovery plan(s) shall include processes and procedures for the backup and storage of information required to successfully restore Critical Cyber Assets. For example, backups may include spare electronic components or equipment, written documentation of configuration settings, tape backup, etc.	N/A	N/A	N/A	The Responsible Entity's recovery plan(s) do not include processes and procedures for the backup and storage of information required to successfully restore Critical Cyber Assets.
CIP-009-4	R5	Testing Backup Media — Information essential to recovery that is stored on backup media shall be tested at least annually to ensure that the information is available. Testing can be completed off site.	N/A	N/A	N/A	The Responsible Entity's information essential to recovery that is stored on backup media has not been tested at least annually to ensure that the information is available.

Standard Number	Requirement Number	Text of Requirement	VRF
CIP-002-4	R1.	Critical Asset Identification — The Responsible Entity shall develop a list of its identified Critical Assets determined through an annual application of the criteria contained in *CIP-002-4 Attachment 1 – Critical Asset Criteria*. The Responsible Entity shall update this list as necessary, and review it at least annually.	HIGH
CIP-002-4	R2.	Critical Cyber Asset Identification— Using the list of Critical Assets developed pursuant to Requirement R1, the Responsible Entity shall develop a list of associated Critical Cyber Assets essential to the operation of the Critical Asset. The Responsible Entity shall update this list as necessary, and review it at least annually. For each group of generating units (including nuclear generation) at a single plant location identified in Attachment 1, criterion 1.1, the only Cyber Assets that must be considered are those shared Cyber Assets that could, within 15 minutes, adversely impact the reliable operation of any combination of units that in aggregate equal or exceed Attachment 1, criterion For the purpose of Standard CIP 002-4, Critical Cyber Assets are further qualified to be those having at least one of the following characteristics: • The Cyber Asset uses a routable protocol to communicate outside the Electronic Security Perimeter; or, • The Cyber Asset uses a routable protocol within a control center; or, • The Cyber Asset is dial-up accessible.	HIGH
CIP-002-4	R3.	Annual Approval —The senior manager or delegate(s) shall approve annually the list of Critical Assets and the list of Critical Cyber Assets. Based on Requirements R1 and R2 the Responsible Entity may determine that it has no Critical Assets or Critical Cyber Assets. The Responsible Entity shall keep a signed and dated record of the senior manager or delegate(s)'s	LOWER

Standard Number	Requirement Number	Text of Requirement	VRF
		approval of the list of Critical Assets and the list of Critical Cyber Assets (even if such lists are null.)	
CIP-003-4	R1.	Cyber Security Policy — The Responsible Entity shall document and implement a cyber security policy that represents management's commitment and ability to secure its Critical Cyber Assets. The Responsible Entity shall, at minimum, ensure the following:	MEDIUM
CIP-003-4	R1.1.	The cyber security policy addresses the requirements in Standards CIP-002-4 through CIP-009-4, including provision for emergency situations.	LOWER
CIP-003-4	R1.2.	The cyber security policy is readily available to all personnel who have access to, or are responsible for, Critical Cyber Assets.	LOWER
CIP-003-4	R1.3	Annual review and approval of the cyber security policy by the senior manager assigned pursuant to R2.	LOWER
CIP-003-4	R2.	Leadership — The Responsible Entity shall assign a senior manager with overall responsibility for leading and managing the entity's implementation of, and adherence to, Standards CIP-002-4 through CIP-009-4.	MEDIUM
CIP-003-4	R2.1.	The senior manager shall be identified by name, title, and date of designation.	LOWER
CIP-003-4	R2.2.	Changes to the senior manager must be documented within thirty calendar days of the effective date.	LOWER
CIP-003-4	R2.3.	Where allowed by Standards CIP-002-4 through CIP-009-4, the senior manager may delegate authority for specific actions to a named delegate or delegates. These delegations shall be documented in the same manner as R2.1 and R2.2, and approved by the senior manager.	LOWER
CIP-003-4	R2.4	The senior manager or delegate(s), shall authorize and document any exception from the requirements of the cyber security policy.	LOWER
CIP-003-4	R3.	Exceptions — Instances where the Responsible Entity cannot conform to its cyber security policy must be documented as exceptions and authorized by the senior manager or delegate(s).	LOWER
CIP-003-4	R3.1.	Exceptions to the Responsible Entity's cyber security policy must be documented within thirty days of being approved by the senior manager or delegate(s).	LOWER
CIP-003-4	R3.2.	Documented exceptions to the cyber security policy must include an explanation as to why the exception is necessary and any compensating measures.	LOWER
CIP-003-4	R3.3.	Authorized exceptions to the cyber security policy must be reviewed and approved annually by the senior manager or delegate(s) to ensure the exceptions are still required and valid. Such review and approval shall be documented.	LOWER

Standard Number	Requirement Number	Text of Requirement	VRF
CIP-003-4	R4.	Information Protection — The Responsible Entity shall implement and document a program to identify, classify, and protect information associated with Critical Cyber Assets.	MEDIUM
CIP-003-4	R4.1.	The Critical Cyber Asset information to be protected shall include, at a minimum and regardless of media type, operational procedures, lists as required in Standard CIP-002-4, network topology or similar diagrams, floor plans of computing centers that contain Critical Cyber Assets, equipment layouts of Critical Cyber Assets, disaster recovery plans, incident response plans, and security configuration information.	MEDIUM
CIP-003-4	R4.2.	The Responsible Entity shall classify information to be protected under this program based on the sensitivity of the Critical Cyber Asset information.	LOWER
CIP-003-4	R4.3.	The Responsible Entity shall, at least annually, assess adherence to its Critical Cyber Asset information protection program, document the assessment results, and implement an action plan to remediate deficiencies identified during the assessment.	LOWER
CIP-003-4	R5.	Access Control — The Responsible Entity shall document and implement a program for managing access to protected Critical Cyber Asset information.	LOWER
CIP-003-4	R5.1.	The Responsible Entity shall maintain a list of designated personnel who are responsible for authorizing logical or physical access to protected information.	LOWER
CIP-003-4	R5.1.1.	Personnel shall be identified by name, title, and the information for which they are responsible for authorizing access.	LOWER
CIP-003-4	R5.1.2.	The list of personnel responsible for authorizing access to protected information shall be verified at least annually.	LOWER
CIP-003-4	R5.2.	The Responsible Entity shall review at least annually the access privileges to protected information to confirm that access privileges are correct and that they correspond with the Responsible Entity's needs and appropriate personnel roles and responsibilities.	LOWER
CIP-003-4	R5.3.	The Responsible Entity shall assess and document at least annually the processes for controlling access privileges to protected information.	LOWER
CIP-003-4	R6.	Change Control and Configuration Management — The Responsible Entity shall establish and document a process of change control and configuration management for adding, modifying, replacing, or removing Critical Cyber Asset hardware or software, and implement supporting configuration management activities to identify, control and document all entity or vendor related changes to hardware and software components of Critical Cyber Assets pursuant to the change control process.	LOWER
CIP-004-4	R1.	Awareness — The Responsible Entity shall establish, document, implement, and maintain a security awareness program to ensure personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets receive on-going reinforcement in sound security practices. The program shall include security awareness reinforcement on at least a quarterly basis using mechanisms such as:	LOWER

Standard Number	Requirement Number	Text of Requirement	VRF
		• Direct communications (e.g. emails, memos, computer based training, etc.); • Indirect communications (e.g. posters, intranet, brochures, etc.); • Management support and reinforcement (e.g., presentations, meetings, etc.).	
CIP-004-4	R2.	Training — The Responsible Entity shall establish, document, implement, and maintain an annual cyber security training program for personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets. The cyber security training program shall be reviewed annually, at a minimum, and shall be updated whenever necessary.	LOWER
CIP-004-4	R2.1.	This program will ensure that all personnel having such access to Critical Cyber Assets, including contractors and service vendors, are trained prior to their being granted such access except in specified circumstances such as an emergency.	MEDIUM
CIP-004-4	R2.2.	Training shall cover the policies, access controls, and procedures as developed for the Critical Cyber Assets covered by CIP-004-4, and include, at a minimum, the following required items appropriate to personnel roles and responsibilities:	MEDIUM
CIP-004-4	R2.2.1.	The proper use of Critical Cyber Assets;	LOWER
CIP-004-4	R2.2.2.	Physical and electronic access controls to Critical Cyber Assets;	LOWER
CIP-004-4	R2.2.3.	The proper handling of Critical Cyber Asset information; and,	LOWER
CIP-004-4	R2.2.4.	Action plans and procedures to recover or re-establish Critical Cyber Assets and access thereto following a Cyber Security Incident.	MEDIUM
CIP-004-4	R2.3.	The Responsible Entity shall maintain documentation that training is conducted at least annually, including the date the training was completed and attendance records.	LOWER
CIP-004-4	R3.	Personnel Risk Assessment —The Responsible Entity shall have a documented personnel risk assessment program, in accordance with federal, state, provincial, and local laws, and subject to existing collective bargaining unit agreements, for personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets. A personnel risk assessment shall be conducted pursuant to that program prior to such personnel being granted such access except in specified circumstances such as an emergency. The personnel risk assessment program shall at a minimum include:	MEDIUM
CIP-004-4	R3.1.	The Responsible Entity shall ensure that each assessment conducted include, at least, identity verification (e.g., Social Security Number verification in the U.S.) and seven year criminal check. The Responsible Entity may conduct more detailed reviews, as permitted by law and subject to existing collective bargaining unit agreements, depending upon the criticality of the position.	LOWER

Standard Number	Requirement Number	Text of Requirement	VRF
CIP-004-4	R3.2.	The Responsible Entity shall update each personnel risk assessment at least every seven years after the initial personnel risk assessment or for cause.	LOWER
CIP-004-4	R3.3.	The Responsible Entity shall document the results of personnel risk assessments of its personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets, and that personnel risk assessments of contractor and service vendor personnel with such access are conducted pursuant to Standard CIP-004-4.	LOWER
CIP-004-4	R4.	Access — The Responsible Entity shall maintain list(s) of personnel with authorized cyber or authorized unescorted physical access to Critical Cyber Assets, including their specific electronic and physical access rights to Critical Cyber Assets.	LOWER
CIP-004-4	R4.1.	The Responsible Entity shall review the list(s) of its personnel who have such access to Critical Cyber Assets quarterly, and update the list(s) within seven calendar days of any change of personnel with such access to Critical Cyber Assets, or any change in the access rights of such personnel. The Responsible Entity shall ensure access list(s) for contractors and service vendors are properly maintained.	LOWER
CIP-004-4	R4.2.	The Responsible Entity shall revoke such access to Critical Cyber Assets within 24 hours for personnel terminated for cause and within seven calendar days for personnel who no longer require such access to Critical Cyber Assets.	LOWER
CIP-005-4	R1.	Electronic Security Perimeter — The Responsible Entity shall ensure that every Critical Cyber Asset resides within an Electronic Security Perimeter. The Responsible Entity shall identify and document the Electronic Security Perimeter(s) and all access points to the perimeter(s).	MEDIUM
CIP-005-4	R1.1.	Access points to the Electronic Security Perimeter(s) shall include any externally connected communication end point (for example, dial-up modems) terminating at any device within the Electronic Security Perimeter(s).	MEDIUM
CIP-005-4	R1.2.	For a dial-up accessible Critical Cyber Asset that uses a non-routable protocol, the Responsible Entity shall define an Electronic Security Perimeter for that single access point at the dial-up device.	MEDIUM
CIP-005-4	R1.3.	Communication links connecting discrete Electronic Security Perimeters shall not be considered part of the Electronic Security Perimeter. However, end points of these communication links within the Electronic Security Perimeter(s) shall be considered access points to the Electronic Security Perimeter(s).	MEDIUM
CIP-005-4	R1.4.	Any non-critical Cyber Asset within a defined Electronic Security Perimeter shall be identified and protected pursuant to the requirements of Standard CIP-005-4.	MEDIUM
CIP-005-4	R1.5.	Cyber Assets used in the access control and/or monitoring of the Electronic Security Perimeter(s) shall be afforded the protective measures as a specified in Standard CIP-003-4; Standard CIP-004-4 Requirement R3; Standard CIP-005-4 Requirements R2 and R3; Standard CIP-006-4 Requirement R3; Standard CIP-007-4 Requirements R1 and R3	MEDIUM

Standard Number	Requirement Number	Text of Requirement	VRF
		through R9; Standard CIP-008-4; and Standard CIP-009-4.	
CIP-005-4	R1.6.	The Responsible Entity shall maintain documentation of Electronic Security Perimeter(s), all interconnected Critical and non-critical Cyber Assets within the Electronic Security Perimeter(s), all electronic access points to the Electronic Security Perimeter(s) and the Cyber Assets deployed for the access control and monitoring of these access points.	LOWER
CIP-005-4	R2.	Electronic Access Controls — The Responsible Entity shall implement and document the organizational processes and technical and procedural mechanisms for control of electronic access at all electronic access points to the Electronic Security Perimeter(s).	MEDIUM
CIP-005-4	R2.1.	These processes and mechanisms shall use an access control model that denies access by default, such that explicit access permissions must be specified.	MEDIUM
CIP-005-4	R2.2.	At all access points to the Electronic Security Perimeter(s), the Responsible Entity shall enable only ports and services required for operations and for monitoring Cyber Assets within the Electronic Security Perimeter, and shall document, individually or by specified grouping, the configuration of those ports and services.	MEDIUM
CIP-005-4	R2.3.	The Responsible Entity shall implement and maintain a procedure for securing dial-up access to the Electronic Security Perimeter(s).	MEDIUM
CIP-005-4	R2.4.	Where external interactive access into the Electronic Security Perimeter has been enabled, the Responsible Entity shall implement strong procedural or technical controls at the access points to ensure authenticity of the accessing party, where technically feasible.	MEDIUM
CIP-005-4	R2.5.	The required documentation shall, at least, identify and describe:	LOWER
CIP-005-4	R2.5.1.	The processes for access request and authorization.	LOWER
CIP-005-4	R2.5.2.	The authentication methods.	LOWER
CIP-005-4	R2.5.3.	The review process for authorization rights, in accordance with Standard CIP-004-4 Requirement R4.	LOWER
CIP-005-4	R2.5.4.	The controls used to secure dial-up accessible connections.	LOWER
CIP-005-4	R2.6.	Appropriate Use Banner — Where technically feasible, electronic access control devices shall display an appropriate use banner on the user screen upon all interactive access attempts. The Responsible Entity shall maintain a document identifying the content of the banner.	LOWER
CIP-005-4	R3.	Monitoring Electronic Access — The Responsible Entity shall implement and document an electronic or manual process(es) for monitoring and logging access at access points to the Electronic Security Perimeter(s) twenty-four hours a day, seven days a week.	MEDIUM

Standard Number	Requirement Number	Text of Requirement	VRF
CIP-005-4	R3.1.	For dial-up accessible Critical Cyber Assets that use non-routable protocols, the Responsible Entity shall implement and document monitoring process(es) at each access point to the dial-up device, where technically feasible.	MEDIUM
CIP-005-4	R3.2.	Where technically feasible, the security monitoring process(es) shall detect and alert for attempts at or actual unauthorized accesses. These alerts shall provide for appropriate notification to designated response personnel. Where alerting is not technically feasible, the Responsible Entity shall review or otherwise assess access logs for attempts at or actual unauthorized accesses at least every ninety calendar days.	MEDIUM
CIP-005-4	R4.	Cyber Vulnerability Assessment — The Responsible Entity shall perform a cyber vulnerability assessment of the electronic access points to the Electronic Security Perimeter(s) at least annually. The vulnerability assessment shall include, at a minimum, the following:	MEDIUM
CIP-005-4	R4.1.	A document identifying the vulnerability assessment process;	LOWER
CIP-005-4	R4.2.	A review to verify that only ports and services required for operations at these access points are enabled;	MEDIUM
CIP-005-4	R4.3.	The discovery of all access points to the Electronic Security Perimeter;	MEDIUM
CIP-005-4	R4.4.	A review of controls for default accounts, passwords, and network management community strings;	MEDIUM
CIP-005-4	R4.5.	Documentation of the results of the assessment, the action plan to remediate or mitigate vulnerabilities identified in the assessment, and the execution status of that action plan.	MEDIUM
CIP-005-4	R5.	Documentation Review and Maintenance — The Responsible Entity shall review, update, and maintain all documentation to support compliance with the requirements of Standard CIP-005-4.	LOWER
CIP-005-4	R5.1.	The Responsible Entity shall ensure that all documentation required by Standard CIP-005-4 reflect current configurations and processes and shall review the documents and procedures referenced in Standard CIP-005-4 at least annually.	LOWER
CIP-005-4	R5.2.	The Responsible Entity shall update the documentation to reflect the modification of the network or controls within ninety calendar days of the change.	LOWER
CIP-005-4	R5.3.	The Responsible Entity shall retain electronic access logs for at least ninety calendar days. Logs related to reportable incidents shall be kept in accordance with the requirements of Standard CIP-008-4.	LOWER
CIP-006-4c	R1.	Physical Security Plan — The Responsible Entity shall document, implement, and maintain a physical security plan, approved by the senior manager or delegate(s) that shall address, at a minimum, the following:	MEDIUM

Standard Number	Requirement Number	Text of Requirement	VRF
CIP-006-4c	R1.1.	All Cyber Assets within an Electronic Security Perimeter shall reside within an identified Physical Security Perimeter. Where a completely enclosed ("six-wall") border cannot be established, the Responsible Entity shall deploy and document alternative measures to control physical access to such Cyber Assets.	MEDIUM
CIP-006-4c	R1.2.	Identification of all physical access points through each Physical Security Perimeter and measures to control entry at those access points.	MEDIUM
CIP-006-4c	R1.3	Processes, tools, and procedures to monitor physical access to the perimeter(s).	MEDIUM
CIP-006-4c	R1.4	Appropriate use of physical access controls as described in Requirement R4 including visitor pass management, response to loss, and prohibition of inappropriate use of physical access controls.	MEDIUM
CIP-006-4c	R1.5	Review of access authorization requests and revocation of access authorization, in accordance with CIP-004-4 Requirement R4.	MEDIUM
CIP-006-4c	R1.6	A visitor control program for visitors (personnel without authorized unescorted access to a Physical Security Perimeter), containing at a minimum the following:	MEDIUM
CIP-006-4c	R1.6.1	Logs (manual or automated) to document the entry and exit of visitors, including the date and time, to and from Physical Security Perimeters.	MEDIUM
CIP-006-4c	R1.6.2	Continuous escorted access of visitors within the Physical Security Perimeter	MEDIUM
CIP-006-4c	R1.7	Update of the physical security plan within thirty calendar days of the completion of any physical security system redesign or reconfiguration, including, but not limited to, addition or removal of access points through the Physical Security Perimeter, physical access controls, monitoring controls, or logging controls.	LOWER
CIP-006-4c	R1.8	Annual review of the physical security plan.	LOWER
CIP-006-4c	R2	Protection of Physical Access Control Systems — Cyber Assets that authorize and/or log access to the Physical Security Perimeter(s), exclusive of hardware at the Physical Security Perimeter access point such as electronic lock control mechanisms and badge readers, shall:	MEDIUM
CIP-006-4c	R2.1.	Be protected from unauthorized physical access.	MEDIUM
CIP-006-4c	R2.2.	Be afforded the protective measures specified in Standard CIP-003-4; Standard CIP-004-4 Requirement R3; Standard CIP-005-4 Requirements R2 and R3; Standard CIP-006-4a Requirements R4 and R5; Standard CIP-007-4; Standard CIP-008-4; and Standard CIP-009-4.	MEDIUM
CIP-006-4c	R3	Protection of Electronic Access Control Systems — Cyber Assets used in the access control and/or monitoring of the Electronic Security Perimeter(s) shall reside within an	MEDIUM

Standard Number	Requirement Number	Text of Requirement	VRF
		identified Physical Security Perimeter.	
CIP-006-4c	R4	Physical Access Controls — The Responsible Entity shall document and implement the operational and procedural controls to manage physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week. The Responsible Entity shall implement one or more of the following physical access methods: • Card Key: A means of electronic access where the access rights of the card holder are predefined in a computer database. Access rights may differ from one perimeter to another. • Special Locks: These include, but are not limited to, locks with "restricted key" systems, magnetic locks that can be operated remotely, and "man-trap" systems. • Security Personnel: Personnel responsible for controlling physical access who may reside on-site or at a monitoring station. • Other Authentication Devices: Biometric, keypad, token, or other equivalent devices that control physical access to the Critical Cyber Assets	MEDIUM
CIP-006-4c	R5	Monitoring Physical Access — The Responsible Entity shall document and implement the technical and procedural controls for monitoring physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week. Unauthorized access attempts shall be reviewed immediately and handled in accordance with the procedures specified in Requirement CIP-008-4. One or more of the following monitoring methods shall be used: • Alarm Systems: Systems that alarm to indicate a door, gate or window has been opened without authorization. These alarms must provide for immediate notification to personnel responsible for response. • Human Observation of Access Points: Monitoring of physical access points by authorized personnel as specified in Requirement R4.	MEDIUM
CIP-006-4c	R6	Logging Physical Access — Logging shall record sufficient information to uniquely identify individuals and the time of access twenty-four hours a day, seven days a week. The Responsible Entity shall implement and document the technical and procedural mechanisms for logging physical entry at all access points to the Physical Security Perimeter(s) using one or more of the following logging methods or their equivalent: • Computerized Logging: Electronic logs produced by the Responsible Entity's	LOWER

Standard Number	Requirement Number	Text of Requirement	VRF
		selected access control and monitoring method. • Video Recording: Electronic capture of video images of sufficient quality to determine identity. • Manual Logging: A log book or sign-in sheet, or other record of physical access maintained by security or other personnel authorized to control and monitor physical access as specified in Requirement R4	
CIP-006-4c	R7	Access Log Retention — The responsible entity shall retain physical access logs for at least ninety calendar days. Logs related to reportable incidents shall be kept in accordance with the requirements of Standard CIP-008-4.	LOWER
CIP-006-4c	R8	Maintenance and Testing — The Responsible Entity shall implement a maintenance and testing program to ensure that all physical security systems under Requirements R4, R5, and R6 function properly. The program must include, at a minimum, the following:	MEDIUM
CIP-006-4c	R8.1	Testing and maintenance of all physical security mechanisms on a cycle no longer than three years.	MEDIUM
CIP-006-4c	R8.2	Retention of testing and maintenance records for the cycle determined by the Responsible Entity in Requirement R8.1.	LOWER
CIP-006-4c	R8.3	Retention of outage records regarding access controls, logging, and monitoring for a minimum of one calendar year.	LOWER
CIP-007-4	R1.	Test Procedures — The Responsible Entity shall ensure that new Cyber Assets and significant changes to existing Cyber Assets within the Electronic Security Perimeter do not adversely affect existing cyber security controls. For purposes of Standard CIP-007-4, a significant change shall, at a minimum, include implementation of security patches, cumulative service packs, vendor releases, and version upgrades of operating systems, applications, database platforms, or other third-party software or firmware.	MEDIUM
CIP-007-4	R1.1.	The Responsible Entity shall create, implement, and maintain cyber security test procedures in a manner that minimizes adverse effects on the production system or its operation.	LOWER
CIP-007-4	R1.2.	The Responsible Entity shall document that testing is performed in a manner that reflects the production environment.	LOWER
CIP-007-4	R1.3.	The Responsible Entity shall document test results.	LOWER
CIP-007-4	R2.	Ports and Services — The Responsible Entity shall establish, document and implement a process to ensure that only those ports and services required for normal and emergency operations are enabled.	MEDIUM
CIP-007-4	R2.1.	The Responsible Entity shall enable only those ports and services required for normal	MEDIUM

Standard Number	Requirement Number	Text of Requirement	VRF
		and emergency operations.	
CIP-007-4	R2.2.	The Responsible Entity shall disable other ports and services, including those used for testing purposes, prior to production use of all Cyber Assets inside the Electronic Security Perimeter(s).	MEDIUM
CIP-007-4	R2.3.	In the case where unused ports and services cannot be disabled due to technical limitations, the Responsible Entity shall document compensating measure(s) applied to mitigate risk exposure.	MEDIUM
CIP-007-4	R3.	Security Patch Management — The Responsible Entity, either separately or as a component of the documented configuration management process specified in CIP-003-4 Requirement R6, shall establish, document and implement a security patch management program for tracking, evaluating, testing, and installing applicable cyber security software patches for all Cyber Assets within the Electronic Security Perimeter(s).	LOWER
CIP-007-4	R3.1.	The Responsible Entity shall document the assessment of security patches and security upgrades for applicability within thirty calendar days of availability of the patches or upgrades.	LOWER
CIP-007-4	R3.2.	The Responsible Entity shall document the implementation of security patches. In any case where the patch is not installed, the Responsible Entity shall document compensating measure(s) applied to mitigate risk exposure.	LOWER
CIP-007-4	R4.	Malicious Software Prevention — The Responsible Entity shall use anti-virus software and other malicious software ("malware") prevention tools, where technically feasible, to detect, prevent, deter, and mitigate the introduction, exposure, and propagation of malware on all Cyber Assets within the Electronic Security Perimeter(s).	MEDIUM
CIP-007-4	R4.1.	The Responsible Entity shall document and implement anti-virus and malware prevention tools. In the case where anti-virus software and malware prevention tools are not installed, the Responsible Entity shall document compensating measure(s) applied to mitigate risk exposure.	MEDIUM
CIP-007-4	R4.2.	The Responsible Entity shall document and implement a process for the update of anti-virus and malware prevention "signatures." The process must address testing and installing the signatures.	MEDIUM
CIP-007-4	R5.	Account Management — The Responsible Entity shall establish, implement, and document technical and procedural controls that enforce access authentication of, and accountability for, all user activity, and that minimize the risk of unauthorized system access.	LOWER
CIP-007-4	R5.1.	The Responsible Entity shall ensure that individual and shared system accounts and authorized access permissions are consistent with the concept of "need to know" with respect to work functions performed.	MEDIUM
CIP-007-4	R5.1.1.	The Responsible Entity shall ensure that user accounts are implemented as approved by	LOWER

Standard Number	Requirement Number	Text of Requirement	VRF
		designated personnel. Refer to Standard CIP-003-4 Requirement R5.	
CIP-007-4	R5.1.2.	The Responsible Entity shall establish methods, processes, and procedures that generate logs of sufficient detail to create historical audit trails of individual user account access activity for a minimum of ninety days.	LOWER
CIP-007-4	R5.1.3.	The Responsible Entity shall review, at least annually, user accounts to verify access privileges are in accordance with Standard CIP-003-4 Requirement R5 and Standard CIP-004-4 Requirement R4.	MEDIUM
CIP-007-4	R5.2.	The Responsible Entity shall implement a policy to minimize and manage the scope and acceptable use of administrator, shared, and other generic account privileges including factory default accounts.	LOWER
CIP-007-4	R5.2.1.	The policy shall include the removal, disabling, or renaming of such accounts where possible. For such accounts that must remain enabled, passwords shall be changed prior to putting any system into service.	MEDIUM
CIP-007-4	R5.2.2.	The Responsible Entity shall identify those individuals with access to shared accounts.	LOWER
CIP-007-4	R5.2.3.	Where such accounts must be shared, the Responsible Entity shall have a policy for managing the use of such accounts that limits access to only those with authorization, an audit trail of the account use (automated or manual), and steps for securing the account in the event of personnel changes (for example, change in assignment or termination).	MEDIUM
CIP-007-4	R5.3.	At a minimum, the Responsible Entity shall require and use passwords, subject to the following, as technically feasible:	LOWER
CIP-007-4	R5.3.1.	Each password shall be a minimum of six characters.	LOWER
CIP-007-4	R5.3.2.	Each password shall consist of a combination of alpha, numeric, and “special” characters.	LOWER
CIP-007-4	R5.3.3.	Each password shall be changed at least annually, or more frequently based on risk.	MEDIUM
CIP-007-4	R6.	Security Status Monitoring — The Responsible Entity shall ensure that all Cyber Assets within the Electronic Security Perimeter, as technically feasible, implement automated tools or organizational process controls to monitor system events that are related to cyber security.	LOWER
CIP-007-4	R6.1.	The Responsible Entity shall implement and document the organizational processes and technical and procedural mechanisms for monitoring for security events on all Cyber Assets within the Electronic Security Perimeter.	MEDIUM
CIP-007-4	R6.2.	The security monitoring controls shall issue automated or manual alerts for detected Cyber Security Incidents.	MEDIUM
CIP-007-4	R6.3.	The Responsible Entity shall maintain logs of system events related to cyber security, where technically feasible, to support incident response as required in Standard CIP-008-4.	MEDIUM

Standard Number	Requirement Number	Text of Requirement	VRF
CIP-007-4	R6.4.	The Responsible Entity shall retain all logs specified in Requirement R6 for ninety calendar days.	LOWER
CIP-007-4	R6.5.	The Responsible Entity shall review logs of system events related to cyber security and maintain records documenting review of logs.	LOWER
CIP-007-4	R7.	Disposal or Redeployment — The Responsible Entity shall establish and implement formal methods, processes, and procedures for disposal or redeployment of Cyber Assets within the Electronic Security Perimeter(s) as identified and documented in Standard CIP-005-4.	LOWER
CIP-007-4	R7.1.	Prior to the disposal of such assets, the Responsible Entity shall destroy or erase the data storage media to prevent unauthorized retrieval of sensitive cyber security or reliability data.	LOWER
CIP-007-4	R7.2.	Prior to redeployment of such assets, the Responsible Entity shall, at a minimum, erase the data storage media to prevent unauthorized retrieval of sensitive cyber security or reliability data.	LOWER
CIP-007-4	R7.3.	The Responsible Entity shall maintain records that such assets were disposed of or redeployed in accordance with documented procedures.	LOWER
CIP-007-4	R8	Cyber Vulnerability Assessment — The Responsible Entity shall perform a cyber vulnerability assessment of all Cyber Assets within the Electronic Security Perimeter at least annually. The vulnerability assessment shall include, at a minimum, the following:	LOWER
CIP-007-4	R8.1.	A document identifying the vulnerability assessment process;	LOWER
CIP-007-4	R8.2.	A review to verify that only ports and services required for operation of the Cyber Assets within the Electronic Security Perimeter are enabled;	MEDIUM
CIP-007-4	R8.3.	A review of controls for default accounts; and,	MEDIUM
CIP-007-4	R8.4.	Documentation of the results of the assessment, the action plan to remediate or mitigate vulnerabilities identified in the assessment, and the execution status of that action plan.	MEDIUM
CIP-007-4	R9	Documentation Review and Maintenance — The Responsible Entity shall review and update the documentation specified in Standard CIP-007-4 at least annually. Changes resulting from modifications to the systems or controls shall be documented within thirty calendar days of the change being completed.	LOWER
CIP-008-4	R1.	Cyber Security Incident Response Plan — The Responsible Entity shall develop and maintain a Cyber Security Incident response plan and implement the plan in response to Cyber Security Incidents. The Cyber Security Incident response plan shall address, at a minimum, the following:	LOWER
CIP-008-4	R1.1.	Procedures to characterize and classify events as reportable Cyber Security Incidents.	LOWER

Standard Number	Requirement Number	Text of Requirement	VRF
CIP-008-4	R1.2.	Response actions, including roles and responsibilities of Cyber Security Incident response teams, Cyber Security Incident handling procedures, and communication plans.	LOWER
CIP-008-4	R1.3.	Process for reporting Cyber Security Incidents to the Electricity Sector Information Sharing and Analysis Center (ES-ISAC). The Responsible Entity must ensure that all reportable Cyber Security Incidents are reported to the ES-ISAC either directly or through an intermediary.	LOWER
CIP-008-4	R1.4.	Process for updating the Cyber Security Incident response plan within thirty calendar days of any changes.	LOWER
CIP-008-4	R1.5.	Process for ensuring that the Cyber Security Incident response plan is reviewed at least annually.	LOWER
CIP-008-4	R1.6.	Process for ensuring the Cyber Security Incident response plan is tested at least annually. A test of the Cyber Security Incident response plan can range from a paper drill, to a full operational exercise, to the response to an actual incident.	LOWER
CIP-008-4	R2	Cyber Security Incident Documentation — The Responsible Entity shall keep relevant documentation related to Cyber Security Incidents reportable per Requirement R1.1 for three calendar years.	LOWER
CIP-009-4	R1	Recovery Plans — The Responsible Entity shall create and annually review recovery plan(s) for Critical Cyber Assets. The recovery plan(s) shall address at a minimum the following:	MEDIUM
CIP-009-4	R1.1.	Specify the required actions in response to events or conditions of varying duration and severity that would activate the recovery plan(s).	MEDIUM
CIP-009-4	R1.2.	Define the roles and responsibilities of responders.	MEDIUM
CIP-009-4	R2	Exercises — The recovery plan(s) shall be exercised at least annually. An exercise of the recovery plan(s) can range from a paper drill, to a full operational exercise, to recovery from an actual incident.	LOWER
CIP-009-4	R3	Change Control — Recovery plan(s) shall be updated to reflect any changes or lessons learned as a result of an exercise or the recovery from an actual incident. Updates shall be communicated to personnel responsible for the activation and implementation of the recovery plan(s) within thirty calendar days of the change being completed.	LOWER
CIP-009-4	R4	Backup and Restore — The recovery plan(s) shall include processes and procedures for the backup and storage of information required to successfully restore Critical Cyber Assets. For example, backups may include spare electronic components or equipment, written documentation of configuration settings, tape backup, etc.	LOWER
CIP-009-4	R5	Testing Backup Media — Information essential to recovery that is stored on backup media shall be tested at least annually to ensure that the information is available. Testing can be completed off site.	LOWER

CIP Version 4 Violation Severity Levels and Violation Risk Factors

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
CIP-002-4	R1.	Critical Asset Identification — The Responsible Entity shall develop a list of its identified Critical Assets determined through an annual application of the criteria contained in *CIP-002-4 Attachment 1 – Critical Asset Criteria*. The Responsible Entity shall update this list as necessary, and review it at least annually.	N/A	N/A	The Responsible Entity has developed a list of Critical Assets but the list has not been reviewed and updated annually as required.	The Responsible Entity did not develop a list of its identified Critical Assets even if such list is null.
CIP-002-4	R2.	Critical Cyber Asset Identification— Using the list of Critical Assets developed pursuant to Requirement R1, the Responsible Entity shall develop a list of associated Critical Cyber Assets essential to the operation of the Critical Asset. The Responsible Entity shall update this list as necessary, and review it at least annually. For each group of generating units (including nuclear generation) at a single plant location identified in Attachment 1, criterion 1.1, the only Cyber Assets that must be considered are those shared Cyber Assets that could, within 15 minutes, adversely impact the reliable operation of any combination of units that in aggregate equal or exceed Attachment 1, criterion 1.1. For the purpose of Standard CIP 002-4, Critical Cyber Assets are further qualified to be those having at least	N/A	N/A	The Responsible Entity has developed a list of associated Critical Cyber Assets essential to the operation of the Critical Asset list as per requirement R2 but the list has not been reviewed and updated annually as required.	The Responsible Entity did not develop a list of associated Critical Cyber Assets essential to the operation of the Critical Asset list as per requirement R2 even if such list is null. OR A Cyber Asset essential to the operation of the Critical Asset was identified that met at least one of the bulleted characteristics in this requirement but was not included in the Critical Cyber Asset List.

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		one of the following characteristics: • The Cyber Asset uses a routable protocol to communicate outside the Electronic Security Perimeter; or, • The Cyber Asset uses a routable protocol within a control center; or, • The Cyber Asset is dial-up accessible.				
CIP-002-4	R3.	Annual Approval —The senior manager or delegate(s) shall approve annually the list of Critical Assets and the list of Critical Cyber Assets. Based on Requirements R1 and R2 the Responsible Entity may determine that it has no Critical Assets or Critical Cyber Assets. The Responsible Entity shall keep a signed and dated record of the senior manager or delegate(s)'s approval of the list of Critical Assets and the list of Critical Cyber Assets (even if such lists are null.)	N/A	N/A~~The Responsible Entity does not have a signed and dated record of the senior manager or delegate(s)'s annual approval of the risk-based assessment methodology, the list of Critical Assets or the list of Critical Cyber Assets (even if such lists are null.)~~	The Responsible Entity does not have a signed and dated record of the senior manager or delegate(s)'s annual approval of the list of Critical Assets. OR The Responsible Entity does not have a signed and dated record of the senior manager or delegate(s)'s annual approval of the list of Critical Cyber Assets (even if such lists are null.) ~~The Responsible Entity does not have a signed and dated record of the senior manager or delegate(s)'s annual~~	The Responsible Entity does not have a signed and dated record of the senior manager or delegate(s)'s annual approval of both the list of Critical Assets and the list of Critical Cyber Assets (even if such lists are null.) ~~The Responsible Entity does not have a signed and dated record of the senior manager or delegate(s) annual approval of 1) A risk based assessment methodology for identification of Critical Assets, 2) a signed and dated approval of the list of Critical Assets,~~

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
					~~approval of two of the following: the risk-based assessment methodology, the list of Critical Assets or the list of Critical Cyber Assets (even if such lists are null.)~~	~~nor 3) a signed and dated approval of the list of Critical Cyber Assets (even if such lists are null.)~~
CIP-003-4	R1.	Cyber Security Policy — The Responsible Entity shall document and implement a cyber security policy that represents management's commitment and ability to secure its Critical Cyber Assets. The Responsible Entity shall, at minimum, ensure the following:	N/A	N/A	N/A	The Responsible Entity has not documented or implemented a cyber security policy.
CIP-003-4	R1.1.	The cyber security policy addresses the requirements in Standards CIP-002-4 through CIP-009-4, including provision for emergency situations.	N/A	N/A	N/A	The Responsible Entity's cyber security policy does not address all the requirements in Standards CIP-002 through CIP-009, including provision for emergency situations.
CIP-003-4	R1.2.	The cyber security policy is readily available to all personnel who have access to, or are responsible for, Critical Cyber Assets.	N/A	N/A	N/A	The Responsible Entity's cyber security policy is not readily available to all personnel who have access to, or are responsible for, Critical Cyber Assets.

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
CIP-003-4	R1.3	Annual review and approval of the cyber security policy by the senior manager assigned pursuant to R2.	N/A	N/A	N/A	The Responsible Entity's senior manager, assigned pursuant to R2, did not complete the annual review and approval of its cyber security policy.
CIP-003-4	R2.	Leadership — The Responsible Entity shall assign a senior manager with overall responsibility for leading and managing the entity's implementation of, and adherence to, Standards CIP-002-4 through CIP-009-4.	N/A	N/A	N/A	The Responsible Entity has not assigned a single senior manager with overall responsibility and authority for leading and managing the entity's implementation of, and adherence to, Standards CIP-002 through CIP-009.
CIP-003-4	R2.1.	The senior manager shall be identified by name, title, and date of designation.	N/A	N/A	N/A	~~The senior manager is not identified by name, title, and date of designation.~~ Identification of the senior manager is missing one of the following: name, title, or date of designation.
CIP-003-4	R2.2.	Changes to the senior manager must be documented within thirty calendar days of the effective date.	N/A	N/A	N/A	Changes to the senior manager were not documented within

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						30 days of the effective date.
CIP-003-4	R2.3.	Where allowed by Standards CIP-002-4 through CIP-009-4, the senior manager may delegate authority for specific actions to a named delegate or delegates. These delegations shall be documented in the same manner as R2.1 and R2.2, and approved by the senior manager.	N/A	N/A	The identification of a senior manager's delegate does not include at least one of the following; name, title, or date of the designation, OR The document is not approved by the senior manager, OR Changes to the delegated authority are not documented within thirty calendar days of the effective date.	A senior manager's delegate is not identified by name, title, and date of designation; the document delegating the authority does not identify the authority being delegated; the document delegating the authority is not approved by the senior manager; AND changes to the delegated authority are not documented within thirty calendar days of the effective date.
CIP-003-4	R2.4	The senior manager or delegate(s), shall authorize and document any exception from the requirements of the cyber security policy.	N/A	N/A	N/A	The senior manager or delegate(s) did not authorize and document any exceptions from the requirements of the cyber security policy as required.

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
CIP-003-4	R3.	Exceptions — Instances where the Responsible Entity cannot conform to its cyber security policy must be documented as exceptions and authorized by the senior manager or delegate(s).	N/A	N/A	In Instances where the Responsible Entity cannot conform to its cyber security policy, in R1, exceptions were documented, **but** were not authorized by the senior manager or delegate(s).	In Instances where the Responsible Entity cannot conform to its cyber security policy, in R1, exceptions were not documented.
CIP-003-4	R3.1.	Exceptions to the Responsible Entity's cyber security policy must be documented within thirty days of being approved by the senior manager or delegate(s).	N/A	N/A	N/A	Exceptions to the Responsible Entity's cyber security policy were not documented within 30 days of being approved by the senior manager or delegate(s).
CIP-003-4	R3.2.	Documented exceptions to the cyber security policy must include an explanation as to why the exception is necessary and any compensating measures.	N/A	N/A	The Responsible Entity has a documented exception to the cyber security policy ~~(pertaining to CIP 002 through CIP 009)~~in R1 but did not include **either**: 1) an explanation as to why the exception is necessary, or 2) any compensating	The Responsible Entity has a documented exception to the cyber security policy in R1~~(pertaining to CIP 002 through CIP 009)~~ but did not include **both:** 1) an explanation as to why the exception is necessary, and 2) any compensating measures.

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
					measures.	
CIP-003-4	R3.3.	Authorized exceptions to the cyber security policy must be reviewed and approved annually by the senior manager or delegate(s) to ensure the exceptions are still required and valid. Such review and approval shall be documented.	N/A	N/A	N/A	Exceptions to the cyber security policy were not reviewed **or** were not approved on an annual basis by the senior manager or delegate(s) to ensure the exceptions are still required and valid or the review and approval is not documented.
CIP-003-4	R4.	Information Protection — The Responsible Entity shall implement and document a program to identify, classify, and protect information associated with Critical Cyber Assets.	N/A	N/A	N/A	The Responsible Entity did not implement or did not document a program to identify, classify, and protect information associated with Critical Cyber Assets.
CIP-003-4	R4.1.	The Critical Cyber Asset information to be protected shall include, at a minimum and regardless of media type, operational procedures, lists as required in Standard CIP-002-4, network topology or similar diagrams, floor plans of computing centers that contain Critical Cyber Assets, equipment layouts of Critical Cyber Assets, disaster recovery plans, incident response plans, and security configuration information.	N/A	N/A	The information protection program does not include one of the minimum information types to be protected as detailed in R4.1.	The information protection program does not include two or more of the minimum information types to be protected as detailed in R4.1.

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
CIP-003-4	R4.2.	The Responsible Entity shall classify information to be protected under this program based on the sensitivity of the Critical Cyber Asset information.	N/A	N/A	N/A	The Responsible Entity did not classify the information to be protected under this program based on the sensitivity of the Critical Cyber Asset information.
CIP-003-4	R4.3.	The Responsible Entity shall, at least annually, assess adherence to its Critical Cyber Asset information protection program, document the assessment results, and implement an action plan to remediate deficiencies identified during the assessment.	N/A	N/A	N/A	The Responsible Entity did not annually assess adherence to its Critical Cyber Asset information protection program, including documentation of the assessment results, OR The Responsible Entity did not implement an action plan to remediate deficiencies identified during the assessment.
CIP-003-4	R5.	Access Control — The Responsible Entity shall document and implement a program for managing access to protected Critical Cyber Asset information.	N/A	N/A	N/A	The Responsible Entity did not implement or did not document a program for managing access to protected Critical

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						Cyber Asset information.
CIP-003-4	R5.1.	The Responsible Entity shall maintain a list of designated personnel who are responsible for authorizing logical or physical access to protected information.	N/A	N/A	The Responsible Entity maintained a list of designated personnel for authorizing either logical or physical access but not both.	The Responsible Entity did not maintain a list of designated personnel who are responsible for authorizing logical or physical access to protected information.
CIP-003-4	R5.1.1.	Personnel shall be identified by name, title, and the information for which they are responsible for authorizing access.	N/A	N/A	The Responsible Entity did identify the personnel by name, title, and the information for which they are responsible for authorizing access, but the business phone is missing.	Personnel are not identified by name, title, or the information for which they are responsible for authorizing access.
CIP-003-4	R5.1.2.	The list of personnel responsible for authorizing access to protected information shall be verified at least annually.	N/A	N/A	N/A	The Responsible Entity did not verify at least annually the list of personnel responsible for authorizing access to protected information.
CIP-003-4	R5.2.	The Responsible Entity shall review at least annually the access privileges to protected information to confirm that access privileges are correct and that they	N/A	N/A	N/A	The Responsible Entity did not review at least annually the access privileges to protected

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		correspond with the Responsible Entity's needs and appropriate personnel roles and responsibilities.				information to confirm that access privileges are correct and that they correspond with the Responsible Entity's needs and appropriate personnel roles and responsibilities.
CIP-003-4	R5.3.	The Responsible Entity shall assess and document at least annually the processes for controlling access privileges to protected information.	N/A	N/A	N/A	The Responsible Entity did not assess and document at least annually the processes for controlling access privileges to protected information.
CIP-003-4	R6.	Change Control and Configuration Management — The Responsible Entity shall establish and document a process of change control and configuration management for adding, modifying, replacing, or removing Critical Cyber Asset hardware or software, and implement supporting configuration management activities to identify, control and document all entity or vendor related changes to hardware and software components of Critical Cyber Assets pursuant to the change control process.	N/A	N/A	N/A	The Responsible Entity has not established or documented a change control process for the activities required in R6, OR The Responsible Entity has not established or documented a configuration management process for the activities required in

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						R6.
CIP-004-4	R1.	Awareness — The Responsible Entity shall establish, document, implement, and maintain a security awareness program to ensure personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets receive on-going reinforcement in sound security practices. The program shall include security awareness reinforcement on at least a quarterly basis using mechanisms such as: • Direct communications (e.g. emails, memos, computer based training, etc.); • Indirect communications (e.g. posters, intranet, brochures, etc.); • Management support and reinforcement (e.g., presentations, meetings, etc.).	N/A~~The Responsible Entity established, implemented, and maintained but did not document a security awareness program to ensure personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets receive on-going reinforcement in sound security practices.~~	N/A~~The Responsibility Entity did not provide security awareness reinforcement on at least a quarterly basis.~~	~~The Responsible Entity did document but did not establish, implement, nor maintain a security awareness program to ensure personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets receive on-going reinforcement in sound security practices.~~ The Responsible[1] Entity did not provide security awareness reinforcement on at least a quarterly basis.	The Responsible Entity did not establish, implement, maintain, ~~n~~or document a security awareness program to ensure personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets receive on-going reinforcement in sound security practices.
CIP-004-4	R2.	Training — The Responsible Entity shall establish, document, implement, and maintain an annual cyber security training program for personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets. The	N/A~~The Responsible Entity established, implemented, and maintained but did not document an annual cyber security training~~	N/A~~The Responsibility Entity did not review the training program on an annual basis.~~	~~The Responsible Entity did document but did not establish, implement, nor maintain an annual cyber security~~	The Responsible Entity did not establish, implement, maintain, ~~n~~or document an annual cyber security

[1] Please note that FERC's January 20, 2011 Order on Version 2 And Version 3 Violation Risk Factors And Violation Severity Levels For Critical Infrastructure Protection Reliability Standards dictated "Responsible Entity" to be changed to "Responsibility Entity." NERC assumes FERC intended the VSL to read "Responsible Entity" and therefore is not making this change. NERC proposes to remove this footnote from the final approved list of VSLs.

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		cyber security training program shall be reviewed annually, at a minimum, and shall be updated whenever necessary.	~~program for personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets.~~		~~training program for personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets.~~ The Responsible[2] Entity did not review the training program on an annual basis.	training program for personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets.
CIP-004-4	R2.1.	This program will ensure that all personnel having such access to Critical Cyber Assets, including contractors and service vendors, are trained prior to their being granted such access except in specified circumstances such as an emergency.	N/A~~At least one individual but less than 5% of personnel having authorized cyber or unescorted physical access to Critical Cyber Assets, including contractors and service vendors, were not trained prior to their being granted such access except in specified circumstances such as an emergency.~~	N/A~~At least 5% but less than 10% of all personnel having authorized cyber or unescorted physical access to Critical Cyber Assets, including contractors and service vendors, were not trained prior to their being granted such access except in specified circumstances such as an emergency.~~	N/A~~At least 10% but less than 15% of all personnel having authorized cyber or unescorted physical access to Critical Cyber Assets, including contractors and service vendors, were not trained prior to their being granted such access except in specified circumstances such as an emergency.~~	~~15% or more of~~ Not all personnel having authorized cyber or unescorted physical access to Critical Cyber Assets, including contractors and service vendors, were ~~not~~ trained prior to their being granted such access except in specified circumstances such as an emergency.
CIP-004-4	R2.2.	Training shall cover the policies, access controls, and procedures as developed for the Critical Cyber Assets covered by CIP-004-4, and include, at a minimum, the following required items appropriate to	N/A	N/A	N/A	The training does not include one or more of the minimum topics as detailed in R2.2.1, R2.2.2, R2.2.3,

[2] Please see previous footnote. NERC proposes to remove this footnote from the final approved list of VSLs.

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		personnel roles and responsibilities:				R2.2.4.
CIP-004-4	R2.2.1.	The proper use of Critical Cyber Assets;	N/A	N/A	N/A	N/A
CIP-004-4	R2.2.2.	Physical and electronic access controls to Critical Cyber Assets;	N/A	N/A	N/A	N/A
CIP-004-4	R2.2.3.	The proper handling of Critical Cyber Asset information; and,	N/A	N/A	N/A	N/A
CIP-004-4	R2.2.4.	Action plans and procedures to recover or re-establish Critical Cyber Assets and access thereto following a Cyber Security Incident.	N/A	N/A	N/A	N/A
CIP-004-4	R2.3.	The Responsible Entity shall maintain documentation that training is conducted at least annually, including the date the training was completed and attendance records.	N/A	N/A	The Responsible Entity did maintain documentation that training is conducted at least annually, but did not include attendance records.	The Responsible Entity did not maintain documentation that training is conducted at least annually, including the date the training was completed and attendance records.
CIP-004-4	R3.	Personnel Risk Assessment —The Responsible Entity shall have a documented personnel risk assessment program, in accordance with federal, state, provincial, and local laws, and subject to existing collective bargaining unit agreements, for personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets. A personnel risk assessment shall be conducted pursuant to that program prior to such personnel being granted such	N/A	The Responsible Entity has a personnel risk assessment program, ~~in accordance with federal, state, provincial, and local laws, and subject to existing collective bargaining unit agreements,~~ as stated in R3, for personnel having	The Responsible Entity has a personnel risk assessment program as stated in R3, but conducted the personnel risk assessment pursuant to that program after such personnel were granted such access except in specified circumstances such	The Responsible Entity does not have a documented personnel risk assessment program, ~~in accordance with federal, state, provincial, and local laws, and subject to existing collective bargaining unit agreements,~~as stated in R3, ~~-~~for

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		access except in specified circumstances such as an emergency. The personnel risk assessment program shall at a minimum include:		authorized cyber or authorized unescorted physical access, but the program is not documented.	as an emergency.	personnel having authorized cyber or authorized unescorted physical access. OR The Responsible Entity did not conduct the personnel risk assessment pursuant to that program for personnel granted such access except in specified circumstances such as an emergency.
CIP-004-4	R3.1.	The Responsible Entity shall ensure that each assessment conducted include, at least, identity verification (e.g., Social Security Number verification in the U.S.) and seven year criminal check. The Responsible Entity may conduct more detailed reviews, as permitted by law and subject to existing collective bargaining unit agreements, depending upon the criticality of the position.	N/A	N/A	The Responsible Entity did not ensure that an assessment conducted included an identity verification (e.g., Social Security Number verification in the U.S.) or a seven-year criminal check.	The Responsible Entity did not ensure that each assessment conducted include, at least, identity verification (e.g., Social Security Number verification in the U.S.) and seven-year criminal check.
CIP-004-4	R3.2.	The Responsible Entity shall update each personnel risk assessment at least every seven years after the initial personnel risk assessment or	N/A	The Responsible Entity did not update each personnel risk	The Responsible Entity did not update each personnel risk	The Responsible Entity did not update each personnel risk

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		for cause.		assessment at least every seven years after the initial personnel risk assessment but did update it for cause when applicable.	assessment for cause (when applicable) but did at least updated it every seven years after the initial personnel risk assessment.	assessment at least every seven years after the initial personnel risk assessment nor was it updated for cause when applicable.
CIP-004-4	R3.3.	The Responsible Entity shall document the results of personnel risk assessments of its personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets, and that personnel risk assessments of contractor and service vendor personnel with such access are conducted pursuant to Standard CIP-004-4.	The Responsible Entity did not document the results of personnel risk assessments for at least one individual but less than 5% of all personnel with authorized cyber or authorized unescorted physical access to Critical Cyber Assets, pursuant to Standard CIP-004.	The Responsible Entity did not document the results of personnel risk assessments for 5% or more but less than 10% of all personnel with authorized cyber or authorized unescorted physical access to Critical Cyber Assets, pursuant to Standard CIP-004.	The Responsible Entity did not document the results of personnel risk assessments for 10% or more but less than 15% of all personnel with authorized cyber or authorized unescorted physical access to Critical Cyber Assets, pursuant to Standard CIP-004.	The Responsible Entity did not document the results of personnel risk assessments for 15% or more of all personnel with authorized cyber or authorized unescorted physical access to Critical Cyber Assets, pursuant to Standard CIP-004.
CIP-004-4	R4.	Access — The Responsible Entity shall maintain list(s) of personnel with authorized cyber or authorized unescorted physical access to Critical Cyber Assets, including their specific electronic and physical access rights to Critical Cyber Assets.	The Responsible Entity did not maintain complete list(s) of personnel with authorized cyber or authorized unescorted physical access to Critical Cyber Assets, including their specific electronic and physical access	The Responsible Entity did not maintain complete list(s) of personnel with authorized cyber or authorized unescorted physical access to Critical Cyber Assets, including their specific electronic and physical access	The Responsible Entity did not maintain complete list(s) of personnel with authorized cyber or authorized unescorted physical access to Critical Cyber Assets, including their specific electronic and physical access	The Responsible Entity did not maintain complete list(s) of personnel with authorized cyber or authorized unescorted physical access to Critical Cyber Assets, including their specific electronic and physical access

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
			rights to Critical Cyber Assets, missing at least one individual but less than 5% of the authorized personnel.	rights to Critical Cyber Assets, missing 5% or more but less than 10% of the authorized personnel.	rights to Critical Cyber Assets, missing 10% or more but less than 15%of the authorized personnel.	rights to Critical Cyber Assets, missing 15% or more of the authorized personnel.
CIP-004-4	R4.1.	The Responsible Entity shall review the list(s) of its personnel who have such access to Critical Cyber Assets quarterly, and update the list(s) within seven calendar days of any change of personnel with such access to Critical Cyber Assets, or any change in the access rights of such personnel. The Responsible Entity shall ensure access list(s) for contractors and service vendors are properly maintained.	N/A	The Responsible Entity did not review the list(s) of its personnel who have access to Critical Cyber Assets quarterly.	The Responsible Entity did not update the list(s) within seven calendar days of any change of personnel with such access to Critical Cyber Assets, nor any change in the access rights of such personnel.	The Responsible Entity did not review the list(s) of all personnel who have access to Critical Cyber Assets quarterly, nor update the list(s) within seven calendar days of any change of personnel with such access to Critical Cyber Assets, nor any change in the access rights of such personnel.
CIP-004-4	R4.2.	The Responsible Entity shall revoke such access to Critical Cyber Assets within 24 hours for personnel terminated for cause and within seven calendar days for personnel who no longer require such access to Critical Cyber Assets.	N/A	The Responsible Entity did not revoke access within seven calendar days for personnel who no longer require such access to Critical Cyber Assets.	The Responsible Entity did not revoke access to Critical Cyber Assets within 24 hours for personnel terminated for cause.	The Responsible Entity did not revoke access to Critical Cyber Assets within 24 hours for personnel terminated for cause nor within seven calendar days for personnel who no longer require such access to Critical Cyber Assets.

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
CIP-005-4	R1.	Electronic Security Perimeter — The Responsible Entity shall ensure that every Critical Cyber Asset resides within an Electronic Security Perimeter. The Responsible Entity shall identify and document the Electronic Security Perimeter(s) and all access points to the perimeter(s).	N/A	N/A	N/A	The Responsible Entity did not ensure that every Critical Cyber Asset resides within an Electronic Security Perimeter. OR The Responsible Entity did not identify and document the Electronic Security Perimeter(s) and all access points to the perimeter(s).
CIP-005-4	R1.1.	Access points to the Electronic Security Perimeter(s) shall include any externally connected communication end point (for example, dial-up modems) terminating at any device within the Electronic Security Perimeter(s).	N/A	N/A	N/A	Access points to the Electronic Security Perimeter(s) do not include all externally connected communication end point (for example, dial-up modems) terminating at any device within the Electronic Security Perimeter(s).
CIP-005-4	R1.2.	For a dial-up accessible Critical Cyber Asset that uses a non-routable protocol, the Responsible Entity shall define an Electronic Security Perimeter for that single access point at the dial-up device.	N/A	N/A	N/A	For one or more dial-up accessible Critical Cyber Assets that use a non-routable protocol, the Responsible Entity did not define an Electronic

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						Security Perimeter for that single access point at the dial-up device.
CIP-005-4	R1.3.	Communication links connecting discrete Electronic Security Perimeters shall not be considered part of the Electronic Security Perimeter. However, end points of these communication links within the Electronic Security Perimeter(s) shall be considered access points to the Electronic Security Perimeter(s).	N/A	N/A	N/A	At least one end point of a communication link within the Electronic Security Perimeter(s) connecting discrete Electronic Security Perimeters was not considered an access point to the Electronic Security Perimeter.
CIP-005-4	R1.4.	Any non-critical Cyber Asset within a defined Electronic Security Perimeter shall be identified and protected pursuant to the requirements of Standard CIP-005-4.	N/A	N/A	N/A	One or more noncritical Cyber Asset within a defined Electronic Security Perimeter is not identified. OR Is not protected pursuant to the requirements of Standard CIP-005.
CIP-005-4	R1.5.	Cyber Assets used in the access control and/or monitoring of the Electronic Security Perimeter(s) shall be afforded the protective measures as a specified in Standard CIP-003-4; Standard CIP-004-4 Requirement R3; Standard CIP-005-4 Requirements R2	N/A~~A Cyber Asset used in the access control and/or monitoring of the Electronic Security Perimeter(s) is provided with all but~~	N/A~~A Cyber Asset used in the access control and/or monitoring of the Electronic Security Perimeter(s) is provided with all but~~	N/A~~A Cyber Asset used in the access control and/or monitoring of the Electronic Security Perimeter(s) is provided with all but~~	A Cyber Asset used in the access control and/or monitoring of the Electronic Security Perimeter(s) was not afforded ~~is~~

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		and R3; Standard CIP-006-4 Requirement R3; Standard CIP-007-4 Requirements R1 and R3 through R9; Standard CIP-008-4; and Standard CIP-009-4.	~~one (1) of the protective measures as specified in Standard CIP-003-3; Standard CIP-004-3 Requirement R3; Standard CIP-005-3 Requirements R2 and R3; Standard CIP-006-3a Requirements R3, Standard CIP-007-3 Requirements R1 and R3 through R9;, Standard CIP-008-3; and Standard CIP-009-3.~~	~~two (2) of the protective measures as specified in Standard CIP-003-3; Standard CIP-004-3 Requirement R3;, Standard CIP-005-3 Requirements R2 and R3; Standard CIP-006-3a Requirements R3; Standard CIP-007-3 Requirements R1 and R3 through R9;, Standard CIP-008-3; and Standard CIP-009-3.~~	~~three (3) of the protective measures as specified in Standard CIP-003-3; Standard CIP-004-3 Requirement R3; Standard CIP-005-3 Requirements R2 and R3; Standard CIP-006-3a Requirements R3; Standard CIP-007-3 Requirements R1 and R3 through R9; Standard CIP-008-3; and Standard CIP-009-3.~~	~~not provided without four (4)~~ one (1) or more of the protective measures as specified in Standard CIP-003-~~3~~4; Standard CIP-004-~~3~~4 Requirement R3; Standard CIP-005-~~3~~4 Requirements R2 and R3; Standard CIP-006-~~3a~~4c Requirements R3; Standard CIP-007-~~3~~4 Requirements R1 and R3 through R9; Standard CIP-008-~~3~~4; and Standard CIP-009-~~3~~4.
CIP-005-4	R1.6.	The Responsible Entity shall maintain documentation of Electronic Security Perimeter(s), all interconnected Critical and non-critical Cyber Assets within the Electronic Security Perimeter(s), all electronic access points to the Electronic Security Perimeter(s) and the Cyber Assets deployed for the access control and monitoring of these access points.	N/A	N/A	N/A	The Responsible Entity did not maintain documentation of one or more of the following: Electronic Security Perimeter(s), interconnected Critical and noncritical Cyber Assets within the Electronic Security Perimeter(s), electronic access

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						points to the Electronic Security Perimeter(s) and Cyber Assets deployed for the access control and monitoring of these access points.
CIP-005-4	R2.	Electronic Access Controls — The Responsible Entity shall implement and document the organizational processes and technical and procedural mechanisms for control of electronic access at all electronic access points to the Electronic Security Perimeter(s).	N/A	N/A	N/A	The Responsible Entity did not implement or did not document the organizational processes and technical and procedural mechanisms for control of electronic access at all electronic access points to the Electronic Security Perimeter(s).
CIP-005-4	R2.1.	These processes and mechanisms shall use an access control model that denies access by default, such that explicit access permissions must be specified.	N/A	N/A	N/A	The processes and mechanisms did not use an access control model that denies access by default, such that explicit access permissions must be specified.
CIP-005-4	R2.2.	At all access points to the Electronic Security Perimeter(s), the Responsible Entity shall enable only ports and services	N/A	N/A	N/A	At one or more access points to the Electronic Security Perimeter(s), the

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		required for operations and for monitoring Cyber Assets within the Electronic Security Perimeter, and shall document, individually or by specified grouping, the configuration of those ports and services.				Responsible Entity enabled ports and services not required for operations and for monitoring Cyber Assets within the Electronic Security Perimeter, or did not document, individually or by specified grouping, the configuration of those ports and services.
CIP-005-4	R2.3.	The Responsible Entity shall implement and maintain a procedure for securing dial-up access to the Electronic Security Perimeter(s).	N/A	N/A	N/A~~The Responsible Entity did implement but did not maintain a procedure for securing dial-up access to the Electronic Security Perimeter(s) where applicable.~~	The Responsible Entity did not implement ~~n~~or maintain a procedure for securing dial-up access to the Electronic Security Perimeter(s) where applicable.
CIP-005-4	R2.4.	Where external interactive access into the Electronic Security Perimeter has been enabled, the Responsible Entity shall implement strong procedural or technical controls at the access points to ensure authenticity of the accessing party, where technically feasible.	N/A	N/A	N/A	Where external interactive access into the Electronic Security Perimeter has been enabled the Responsible Entity did not implement strong procedural or technical controls at the access points to ensure authenticity

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						of the accessing party, where technically feasible.
CIP-005-4	R2.5.	The required documentation shall, at least, identify and describe:	N/A	N/A	N/A	The required documentation for R2 did not include one or more of the elements described in R2.5.1 through R2.5.4.
CIP-005-4	R2.5.1.	The processes for access request and authorization.	N/A	N/A	N/A	N/A
CIP-005-4	R2.5.2.	The authentication methods.	N/A	N/A	N/A	N/A
CIP-005-4	R2.5.3.	The review process for authorization rights, in accordance with Standard CIP-004-4 Requirement R4.	N/A	N/A	N/A	N/A
CIP-005-4	R2.5.4.	The controls used to secure dial-up accessible connections.	N/A	N/A	N/A	N/A
CIP-005-4	R2.6.	Appropriate Use Banner — Where technically feasible, electronic access control devices shall display an appropriate use banner on the user screen upon all interactive access attempts. The Responsible Entity shall maintain a document identifying the content of the banner.	The Responsible Entity did not maintain a document identifying the content of the banner. OR Where technically feasible less than 5% electronic access control devices did not display an appropriate use banner on the user screen upon all	Where technically feasible 5% but less than 10% of electronic access control devices did not display an appropriate use banner on the user screen upon all interactive access attempts.	Where technically feasible 10% but less than 15% of electronic access control devices did not display an appropriate use banner on the user screen upon all interactive access attempts.	Where technically feasible, 15% or more electronic access control devices did not display an appropriate use banner on the user screen upon all interactive access attempts.

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
			interactive access attempts.			
CIP-005-4	R3.	Monitoring Electronic Access — The Responsible Entity shall implement and document an electronic or manual process(es) for monitoring and logging access at access points to the Electronic Security Perimeter(s) twenty-four hours a day, seven days a week.	N/A	N/A	N/A	The Responsible Entity did not implement or did not document electronic or manual processes monitoring and logging access points.
CIP-005-4	R3.1.	For dial-up accessible Critical Cyber Assets that use non-routable protocols, the Responsible Entity shall implement and document monitoring process(es) at each access point to the dial-up device, where technically feasible.	N/A	N/A	N/A	Where technically feasible, the Responsible Entity did not implement or did not document electronic or manual processes for monitoring at one or more access points to dial-up devices.
CIP-005-4	R3.2.	Where technically feasible, the security monitoring process(es) shall detect and alert for attempts at or actual unauthorized accesses. These alerts shall provide for appropriate notification to designated response personnel. Where alerting is not technically feasible, the Responsible Entity shall review or otherwise assess access logs for attempts at or actual unauthorized accesses at least every ninety calendar days.	N/A	N/A	N/A	Where technically feasible, the Responsible Entity did not implement security monitoring process(es) to detect and alert for attempts at or actual unauthorized accesses. OR The above alerts do not provide for appropriate

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						notification to designated response personnel. OR Where alerting is not technically feasible, the Responsible Entity did not review or otherwise assess access logs for attempts at or actual unauthorized accesses at least every ninety calendar days.
CIP-005-4	R4.	Cyber Vulnerability Assessment — The Responsible Entity shall perform a cyber vulnerability assessment of the electronic access points to the Electronic Security Perimeter(s) at least annually. The vulnerability assessment shall include, at a minimum, the following:	N/A	N/A	N/A	The Responsible Entity did not perform a Vulnerability Assessment at least annually for one or more of the access points to the Electronic Security Perimeter(s). OR The vulnerability assessment did not include one (1) or more of the subrequirements R4.1, R4.2, R4.3, R4.4, R4.5.
CIP-005-4	R4.1.	A document identifying the	N/A	N/A	N/A	N/A

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		vulnerability assessment process;				
CIP-005-4	R4.2.	A review to verify that only ports and services required for operations at these access points are enabled;	N/A	N/A	N/A	N/A
CIP-005-4	R4.3.	The discovery of all access points to the Electronic Security Perimeter;	N/A	N/A	N/A	N/A
CIP-005-4	R4.4.	A review of controls for default accounts, passwords, and network management community strings;	N/A	N/A	N/A	N/A
CIP-005-4	R4.5.	Documentation of the results of the assessment, the action plan to remediate or mitigate vulnerabilities identified in the assessment, and the execution status of that action plan.	N/A	N/A	N/A	N/A
CIP-005-4	R5.	Documentation Review and Maintenance — The Responsible Entity shall review, update, and maintain all documentation to support compliance with the requirements of Standard CIP-005-4.	The Responsible Entity did not review, update, and maintain at least one but less than or equal to 5% of the documentation to support compliance with the requirements of Standard CIP-005.	The Responsible Entity did not review, update, and maintain greater than 5% but less than or equal to 10% of the documentation to support compliance with the requirements of Standard CIP-005.	The Responsible Entity did not review, update, and maintain greater than 10% but less than or equal to 15% of the documentation to support compliance with the requirements of Standard CIP-005.	The Responsible Entity did not review, update, and maintain greater than 15% of the documentation to support compliance with the requirements of Standard CIP-005.
CIP-005-4	R5.1.	The Responsible Entity shall ensure that all documentation required by Standard CIP-005-4 reflect current configurations and processes and shall review the documents and procedures referenced in Standard CIP-005-4 at least annually.	N/A	The Responsible Entity did not provide evidence of an annual review of the documents and procedures referenced in Standard CIP-005.	The Responsible Entity did not document current configurations and processes referenced in Standard CIP-005.	The Responsible Entity did not document current configurations and processes and did not review the documents and procedures

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						referenced in Standard CIP-005 at least annually.
CIP-005-4	R5.2.	The Responsible Entity shall update the documentation to reflect the modification of the network or controls within ninety calendar days of the change.	N/A	N/A	N/A	The Responsible Entity did not update documentation to reflect a modification of the network or controls within ninety calendar days of the change.
CIP-005-4	R5.3.	The Responsible Entity shall retain electronic access logs for at least ninety calendar days. Logs related to reportable incidents shall be kept in accordance with the requirements of Standard CIP-008-4.	The Responsible Entity retained electronic access logs for 75 or more calendar days, but for less than 90 calendar days.	The Responsible Entity retained electronic access logs for 60 or more calendar days, but for less than 75 calendar days.	The Responsible Entity retained electronic access logs for 45 or more calendar days, but for less than 60 calendar days.	The Responsible Entity retained electronic access logs for less than 45 calendar days.
CIP-006-4c	R1.	Physical Security Plan — The Responsible Entity shall document, implement, and maintain a physical security plan, approved by the senior manager or delegate(s) that shall address, at a minimum, the following:	N/A	N/A	The Responsible Entity created a physical security plan but did not gain approval by a senior manager or delegate(s). OR The Responsible Entity created and implemented but did not maintain a physical security	The Responsible Entity did not document, implement, and maintain a physical security plan.

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
					plan.	
CIP-006-4c	R1.1.	All Cyber Assets within an Electronic Security Perimeter shall reside within an identified Physical Security Perimeter. Where a completely enclosed ("six-wall") border cannot be established, the Responsible Entity shall deploy and document alternative measures to control physical access to such Cyber Assets.	N/A	N/AWhere a completely enclosed ("six-wall") border cannot be established, the Responsible Entity has deployed but not documented alternative measures to control physical access to such Cyber Assets within the Electronic Security Perimeter.	N/AWhere a completely enclosed ("six-wall") border cannot be established, the Responsible Entity has not deployed alternative measures to control physical access to such Cyber Assets within the Electronic Security Perimeter.	The Responsible Entity's physical security plan does not include processes to ensure and document that all Cyber Assets within an Electronic Security Perimeter also reside within an identified Physical Security Perimeter. OR Where a completely enclosed ("six-wall") border cannot be established, the Responsible Entity has not deployed and or documented alternative measures to control physical access to the Critical s such Cyber Assets within the Electronic Security Perimeter.
CIP-006-4c	R1.2.	Identification of all physical access points through each Physical Security Perimeter and measures to control entry at those access points.	N/A	N/AThe Responsible Entity's physical security plan includes measures to control entry at access points but	N/AThe Responsible Entity's physical security identifies all access points through each Physical Security	The Responsible Entity's physical security plan does not identify all access points through each

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
				~~does not identify all access points through each Physical Security Perimeter.~~	~~Perimeter but does not identify measures to control entry at those access points.~~	Physical Security Perimeter ~~n~~or does not identify measures to control entry at those access points.
CIP-006-4c	R1.3	Processes, tools, and procedures to monitor physical access to the perimeter(s).	N/A	N/A	N/A	The Responsible Entity's physical security plan does not include processes, tools, and procedures to monitor physical access to the perimeter(s).
CIP-006-4c	R1.4	Appropriate use of physical access controls as described in Requirement R4 including visitor pass management, response to loss, and prohibition of inappropriate use of physical access controls.	N/A	N/A	N/A	The Responsible Entity's physical security plan does not address the appropriate use of physical access controls as described in Requirement R4.
CIP-006-4c	R1.5	Review of access authorization requests and revocation of access authorization, in accordance with CIP-004-4 Requirement R4.	N/A	N/A	N/A~~The Responsible Entity's physical security plan does not address either the process for reviewing access authorization requests or the process for revocation of access authorization, in accordance with~~	The Responsible Entity's physical security plan does not address the ~~process for~~ review~~ing~~ of access authorization requests ~~and~~ or the ~~process for~~ revocation of access authorization, in accordance with

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
					~~CIP-004-3 Requirement R4.~~	CIP-004-~~4~~3 Requirement R4.
CIP-006-4c	R1.6	A visitor control program for visitors (personnel without authorized unescorted access to a Physical Security Perimeter), containing at a minimum the following:	N/A~~The responsible Entity included a visitor control program in its physical security plan, but either did not log the visitor entrance or did not log the visitor exit from the Physical Security Perimeter.~~	~~The responsible Entity included a visitor control program in its physical security plan, but either did not log the visitor or did not log the escort.~~N/A	N/A~~The responsible Entity included a visitor control program in its physical security plan, but either did not log the visitor or did not log the escort.~~	The Responsible Entity did not include or implement a visitor control program in its physical security plan or it does not meet the requirements of continuous escort.~~.~~
CIP-006-4c	R1.6.1	Logs (manual or automated) to document the entry and exit of visitors, including the date and time, to and from Physical Security Perimeters.	N/A	N/A	N/A	N/A
CIP-006-4c	R1.6.2	Continuous escorted access of visitors within the Physical Security Perimeter	N/A	N/A	N/A	N/A
CIP-006-4c	R1.7	Update of the physical security plan within thirty calendar days of the completion of any physical security system redesign or reconfiguration, including, but not limited to, addition or removal of access points through the Physical Security Perimeter, physical access controls, monitoring controls, or logging controls.	N/A	N/A	N/A~~The Responsible Entity's physical security plan addresses a process for updating the physical security plan within thirty calendar days of the completion of any physical security system redesign or reconfiguration **but** the plan was not~~	The Responsible Entity's physical security plan does not address ~~a process for~~ updating the physical security plan within thirty calendar days of the completion of a physical security system redesign or within thirty calendar days of the

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
					~~updated within thirty calendar days of the completion of a physical security system redesign or reconfiguration.~~	completion of a reconfiguration. OR The plan was not updated within thirty calendar days of the completion of a physical security system redesign or reconfiguration
CIP-006-4c	R1.8	Annual review of the physical security plan.	N/A	N/A	N/A	The Responsible Entity's physical security plan does not address a process for ensuring that the physical security plan is reviewed at least annually.
CIP-006-4c	R2	Protection of Physical Access Control Systems — Cyber Assets that authorize and/or log access to the Physical Security Perimeter(s), exclusive of hardware at the Physical Security Perimeter access point such as electronic lock control mechanisms and badge readers, shall:	N/A~~A Cyber Asset that authorizes and/or logs access to the Physical Security Perimeter(s), exclusive of hardware at the Physical Security Perimeter access point such as electronic lock control mechanisms and badge readers was provided with~~	N/A~~A Cyber Asset that authorizes and/or logs access to the Physical Security Perimeter(s), exclusive of hardware at the Physical Security Perimeter access point such as electronic lock control mechanisms and badge readers was provided with~~	~~A~~N/A ~~Cyber Asset that authorizes and/or logs access to the Physical Security Perimeter(s), exclusive of hardware at the Physical Security Perimeter access point such as electronic lock control mechanisms and badge readers was provided with~~	A Cyber Asset that authorizes and/or logs access to the Physical Security Perimeter(s), exclusive of hardware at the Physical Security Perimeter access point such as electronic lock control mechanisms and badge readers, was not protected

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
			~~all but one (1) of the protective measures specified in Standard CIP-003-3; Standard CIP-004-3 Requirement R3; Standard CIP-005-3 Requirements R2 and R3; Standard CIP-006-3a Requirements R4 and R5; Standard CIP-007-3; Standard CIP-008-3; and Standard CIP-009-3.~~	~~all but two (2) of the protective measures specified in Standard CIP-003-3; Standard CIP-004-3 Requirement R3; Standard CIP-005-3 Requirements R2 and R3; Standard CIP-006-3a Requirements R4 and R5; Standard CIP-007-3; Standard CIP-008-3; and Standard CIP-009-3.~~	~~all but three (3) of the protective measures specified in Standard CIP-003-3; Standard CIP-004-3 Requirement R3; Standard CIP-005-3 Requirements R2 and R3; Standard CIP-006-3a Requirements R4 and R5; Standard CIP-007-3; Standard CIP-008-3; and Standard CIP-009-3.~~	from unauthorized physical access. OR A Cyber Asset that authorizes and/or logs access to the Physical Security Perimeter(s), exclusive of hardware at the Physical Security Perimeter access point such as electronic lock control mechanisms and badge readers was ~~provided without~~ not afforded ~~four (4) or more of~~ the protective measures specified in Standard CIP-003-4~~3~~; Standard CIP-004-4~~3~~ Requirement R3; Standard CIP-005-4~~3~~ Requirements R2 and R3; Standard CIP-006-4c~~3a~~ Requirements R4 and R5; Standard CIP-007-4~~3~~; Standard CIP-008-4~~3~~; and

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						Standard CIP-009-4~~3~~.
CIP-006-4c	R2.1.	Be protected from unauthorized physical access.	N/A	N/A	N/A	N/A
CIP-006-4c	R2.2.	Be afforded the protective measures specified in Standard CIP-003-4; Standard CIP-004-4 Requirement R3; Standard CIP-005-4 Requirements R2 and R3; Standard CIP-006-4a Requirements R4 and R5; Standard CIP-007-4; Standard CIP-008-4; and Standard CIP-009-4.	N/A	N/A	N/A	N/A
CIP-006-4c	R3	Protection of Electronic Access Control Systems — Cyber Assets used in the access control and/or monitoring of the Electronic Security Perimeter(s) shall reside within an identified Physical Security Perimeter.	N/A	N/A	N/A	A Cyber Assets used in the access control and/or monitoring of the Electronic Security Perimeter(s) ~~did~~ does not reside within an identified Physical Security Perimeter.
CIP-006-4c	R4	Physical Access Controls — The Responsible Entity shall document and implement the operational and procedural controls to manage physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week. The Responsible Entity shall implement one or more of the following physical access methods: • Card Key: A means of electronic access where the access rights of the card holder are predefined in a	N/A	N/A~~The Responsible Entity **has implemented but not documented** the operational and procedural controls to manage physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week using one or more of~~	N/A~~The Responsible Entity **has documented but not implemented** the operational and procedural controls to manage physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week using one or more of~~	The Responsible Entity has not documented ~~n~~or has not implemented the operational and procedural controls to manage physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week using one or more of

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		computer database. Access rights may differ from one perimeter to another. • Special Locks: These include, but are not limited to, locks with "restricted key" systems, magnetic locks that can be operated remotely, and "man-trap" systems. • Security Personnel: Personnel responsible for controlling physical access who may reside on-site or at a monitoring station. • Other Authentication Devices: Biometric, keypad, token, or other equivalent devices that control physical access to the Critical Cyber Assets		~~the following physical access methods:~~ ~~• Card Key: A means of electronic access where the access rights of the card holder are predefined in a computer database. Access rights may differ from one perimeter to another.~~ ~~• Special Locks: These include, but are not limited to, locks with "restricted key" systems, magnetic locks that can be operated remotely, and "man-trap" systems.~~ ~~• Security Personnel: Personnel responsible for controlling physical access who may reside on-site or at a monitoring station.~~ ~~• Other Authentication Devices: Biometric, keypad, token, or other equivalent~~	~~the following physical access methods:~~ ~~• Card Key: A means of electronic access where the access rights of the card holder are predefined in a computer database. Access rights may differ from one perimeter to another.~~ ~~• Special Locks: These include, but are not limited to, locks with "restricted key" systems, magnetic locks that can be operated remotely, and "man-trap" systems.~~ ~~• Security Personnel: Personnel responsible for controlling physical access who may reside on-site or at a monitoring station.~~ ~~• Other Authentication Devices: Biometric, keypad, token, or other equivalent~~	the following physical access methods: • Card Key: A means of electronic access where the access rights of the card holder are predefined in a computer database. Access rights may differ from one perimeter to another. • Special Locks: These include, but are not limited to, locks with "restricted key" systems, magnetic locks that can be operated remotely, and "man-trap" systems. • Security Personnel: Personnel responsible for controlling physical access who may reside on-site or at a monitoring station. • Other Authentication Devices: Biometric, keypad, token, or other equivalent

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
				~~devices that control physical access to the Critical Cyber Assets.~~	~~devices that control physical access to the Critical Cyber Assets.~~	devices that control physical access to the Critical Cyber Assets.
CIP-006-4c	R5	Monitoring Physical Access — The Responsible Entity shall document and implement the technical and procedural controls for monitoring physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week. Unauthorized access attempts shall be reviewed immediately and handled in accordance with the procedures specified in Requirement CIP-008-4. One or more of the following monitoring methods shall be used: • Alarm Systems: Systems that alarm to indicate a door, gate or window has been opened without authorization. These alarms must provide for immediate notification to personnel responsible for response. • Human Observation of Access Points: Monitoring of physical access points by authorized personnel as specified in Requirement R4.	N/A	N/A~~The Responsible Entity **has implemented but not documented** the technical and procedural controls for monitoring physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week using one or more of the following monitoring methods:~~ ~~• Alarm Systems: Systems that alarm to indicate a door, gate or window has been opened without authorization. These alarms must provide for immediate notification to personnel responsible for response.~~	N/A~~The Responsible Entity **has documented but not implemented** the technical and procedural controls for monitoring physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week using one or more of the following monitoring methods:~~ ~~• Alarm Systems: Systems that alarm to indicate a door, gate or window has been opened without authorization. These alarms must provide for immediate notification to personnel responsible for response.~~	The Responsible Entity **has not documented ~~nor~~ has not implemented** the technical and procedural controls for monitoring physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week using one or more of the following monitoring methods: • Alarm Systems: Systems that alarm to indicate a door, gate or window has been opened without authorization. These alarms must provide for immediate notification to personnel responsible for

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
				~~• Human Observation of Access Points: Monitoring of physical access points by authorized personnel as specified in Requirement R4~~.	~~• Human Observation of Access Points: Monitoring of physical access points by authorized personnel as specified in Requirement R4.~~	response. • Human Observation of Access Points: Monitoring of physical access points by authorized personnel as specified in Requirement R4. OR An unauthorized access attempt was not reviewed immediately and handled in accordance with CIP-008-4~~3~~.
CIP-006-4c	R6	Logging Physical Access — Logging shall record sufficient information to uniquely identify individuals and the time of access twenty-four hours a day, seven days a week. The Responsible Entity shall implement and document the technical and procedural mechanisms for logging physical entry at all access points to the Physical Security Perimeter(s) using one or more of the following logging methods or their equivalent: • Computerized Logging: Electronic logs produced by the Responsible Entity's selected access control and	~~The Responsible Entity has implemented but not documented the technical and procedural mechanisms for logging physical entry at all access points to the Physical Security Perimeter(s) using one or more of the following logging methods or their equivalent:~~ ~~• Computerized~~	N/A~~The Responsible Entity has implemented the technical and procedural mechanisms for logging physical entry at all access points to the Physical Security Perimeter(s) using one or more of the following logging methods or their equivalent:~~ ~~• Computerized Logging: Electronic~~	N/A~~The Responsible Entity **has documented but not implemented** the technical and procedural mechanisms for logging physical entry at all access points to the Physical Security Perimeter(s) using one or more of the following logging methods or their equivalent:~~ ~~• Computerized~~	The Responsible Entity **has not implemented ~~n~~or has not documented** the technical and procedural mechanisms for logging physical entry at all access points to the Physical Security Perimeter(s) using one or more of the following logging methods or their equivalent:

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		monitoring method. • Video Recording: Electronic capture of video images of sufficient quality to determine identity. • Manual Logging: A log book or sign-in sheet, or other record of physical access maintained by security or other personnel authorized to control and monitor physical access as specified in Requirement R4	~~Logging: Electronic logs produced by the Responsible Entity's selected access control and monitoring method,~~ ~~• Video Recording: Electronic capture of video images of sufficient quality to determine identity, or~~ ~~• Manual Logging: A log book or sign-in sheet, or other record of physical access maintained by security or other personnel authorized to control and monitor physical access as specified in Requirement R4, and has provided logging that records sufficient information to uniquely identify individuals and the time of access twenty-four hours a day, seven days a week.~~	~~logs produced by the Responsible Entity's selected access control and monitoring method,~~ ~~• Video Recording: Electronic capture of video images of sufficient quality to determine identity, or~~ ~~• Manual Logging: A log book or sign-in sheet, or other record of physical access maintained by security or other personnel authorized to control and monitor physical access as specified in Requirement R4, **but** has not provided logging that records sufficient information to uniquely identify individuals and the time of access twenty-four hours a day, seven days a week.~~	~~Logging: Electronic logs produced by the Responsible Entity's selected access control and monitoring method,~~ ~~• Video Recording: Electronic capture of video images of sufficient quality to determine identity, or~~ ~~• Manual Logging: A log book or sign-in sheet, or other record of physical access maintained by security or other personnel authorized to control and monitor physical access as specified in Requirement R4.~~	• Computerized Logging: Electronic logs produced by the Responsible Entity's selected access control and monitoring method, • Video Recording: Electronic capture of video images of sufficient quality to determine identity, or • Manual Logging: A log book or sign-in sheet, or other record of physical access maintained by security or other personnel authorized to control and monitor physical access as specified in Requirement R4. OR The Responsible Entity has not recorded sufficient information to uniquely identify individuals and the time of access twenty-four hours a

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						day, seven days a week.
CIP-006-4c	R7	Access Log Retention — The responsible entity shall retain physical access logs for at least ninety calendar days. Logs related to reportable incidents shall be kept in accordance with the requirements of Standard CIP-008-4.	N/AThe Responsible Entity retained physical access logs for 75 or more calendar days, but for less than 90 calendar days.	N/AThe Responsible Entity retained physical access logs for 60 or more calendar days, but for less than 75 calendar days.	N/AThe Responsible Entity retained physical access logs for 45 or more calendar days, but for less than 60 calendar days.	The Responsible Entity retained physical access logs for less than 45 calendar days. The responsible entity did not retain physical access logs for at least ninety calendar days.
CIP-006-4c	R8	Maintenance and Testing — The Responsible Entity shall implement a maintenance and testing program to ensure that all physical security systems under Requirements R4, R5, and R6 function properly. The program must include, at a minimum, the following:	N/AThe Responsible Entity has implemented a maintenance and testing program to ensure that all physical security systems under Requirements R4, R5, and R6 function properly **but** the program does not include one of the Requirements R8.1, R8.2, and R8.3.	N/AThe Responsible Entity has implemented a maintenance and testing program to ensure that all physical security systems under Requirements R4, R5, and R6 function properly **but** the program does not include two of the Requirements R8.1, R8.2, and R8.3.	N/AThe Responsible Entity has implemented a maintenance and testing program to ensure that all physical security systems under Requirements R4, R5, and R6 function properly **but** the program does not include any of the Requirements R8.1, R8.2, and R8.3.	The Responsible Entity has not implemented a maintenance and testing program to ensure that all physical security systems under Requirements R4, R5, and R6 function properly. OR The implemented program does not include one or more of the requirements; R8.1, R8.2, and R8.3.
CIP-006-4c	R8.1	Testing and maintenance of all physical security mechanisms on a cycle no longer than three years.	N/A	N/A	N/A	N/A
CIP-006-4c	R8.2	Retention of testing and	N/A	N/A	N/A	N/A

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		maintenance records for the cycle determined by the Responsible Entity in Requirement R8.1.				
CIP-006-4c	R8.3	Retention of outage records regarding access controls, logging, and monitoring for a minimum of one calendar year.	N/A	N/A	N/A	N/A
CIP-007-4	R1.	Test Procedures — The Responsible Entity shall ensure that new Cyber Assets and significant changes to existing Cyber Assets within the Electronic Security Perimeter do not adversely affect existing cyber security controls. For purposes of Standard CIP-007-4, a significant change shall, at a minimum, include implementation of security patches, cumulative service packs, vendor releases, and version upgrades of operating systems, applications, database platforms, or other third-party software or firmware.	N/A	N/A	N/A	The Responsible Entity did not ensure the prevention of adverse affects described in R1, by not including the required minimum significant changes. OR The Responsible Entity did not address one or more of the following: R1.1, R1.2, R1.3.
CIP-007-4	R1.1.	The Responsible Entity shall create, implement, and maintain cyber security test procedures in a manner that minimizes adverse effects on the production system or its operation.	N/A	N/A	N/A	N/A
CIP-007-4	R1.2.	The Responsible Entity shall document that testing is performed in a manner that reflects the production environment.	N/A	N/A	N/A	N/A
CIP-007-4	R1.3.	The Responsible Entity shall document test results.	N/A	N/A	N/A	N/A
CIP-007-4	R2.	Ports and Services — The Responsible Entity shall establish,	N/A	N/A~~The Responsible~~	N/A~~The Responsible~~	The Responsible

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		document and implement a process to ensure that only those ports and services required for normal and emergency operations are enabled.		~~Entity **established (implemented) but did not document** a process to ensure that only those ports and services required for normal and emergency operations are enabled.~~	~~Entity **documented but did not establish (implement)** a process to ensure that only those ports and services required for normal and emergency operations are enabled.~~	Entity did not establish (implement) ~~n~~or did not document a process to ensure that only those ports and services required for normal and emergency operations are enabled.
CIP-007-4	R2.1.	The Responsible Entity shall enable only those ports and services required for normal and emergency operations.	N/A	N/A	N/A	The Responsible Entity enabled one or more ports or services not required for normal and emergency operations on Cyber Assets inside the Electronic Security Perimeter(s).
CIP-007-4	R2.2.	The Responsible Entity shall disable other ports and services, including those used for testing purposes, prior to production use of all Cyber Assets inside the Electronic Security Perimeter(s).	N/A	N/A	N/A	The Responsible Entity did not disable one or more other ports or services, including those used for testing purposes, prior to production use for Cyber Assets inside the Electronic Security Perimeter(s).
CIP-007-4	R2.3.	In the case where unused ports and services cannot be disabled due to technical	N/A	N/A	N/A	For cases where unused ports and services cannot be

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		limitations, the Responsible Entity shall document compensating measure(s) applied to mitigate risk exposure.				disabled due to technical limitations, the Responsible Entity did not document compensating measure(s) applied to mitigate risk. ~~exposure or state an acceptance of risk.~~
CIP-007-4	R3.	Security Patch Management — The Responsible Entity, either separately or as a component of the documented configuration management process specified in CIP-003-4 Requirement R6, shall establish, document and implement a security patch management program for tracking, evaluating, testing, and installing applicable cyber security software patches for all Cyber Assets within the Electronic Security Perimeter(s).	N/A~~The Responsible Entity established (implemented) and documented, either separately or as a component of the documented configuration management process specified in CIP-003-3 Requirement R6, a security patch management program **but** did not include one or more of the following: tracking, evaluating, testing, and installing applicable cyber security software patches for all Cyber Assets within the Electronic Security Perimeter(s).~~	N/A~~The Responsible Entity **established (implemented) but did not document**, either separately or as a component of the documented configuration management process specified in CIP-003-3 Requirement R6, a security patch management program for tracking, evaluating, testing, and installing applicable cyber security software patches for all Cyber Assets within the Electronic Security Perimeter(s).~~	N/A~~The Responsible Entity **documented but did not establish (implement)**, either separately or as a component of the documented configuration management process specified in CIP-003-3 Requirement R6, a security patch management program for tracking, evaluating, testing, and installing applicable cyber security software patches for all Cyber Assets within the Electronic Security Perimeter(s).~~	The Responsible Entity **did not establish (implement) ~~n~~or did not document**, either separately or as a component of the documented configuration management process specified in CIP-003-~~3~~4 Requirement R6, a security patch management program for tracking, evaluating, testing, and installing applicable cyber security software patches for all Cyber Assets within the Electronic Security Perimeter(s).

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
CIP-007-4	R3.1.	The Responsible Entity shall document the assessment of security patches and security upgrades for applicability within thirty calendar days of availability of the patches or upgrades.	N/A	N/A	N/A	The Responsible Entity did not document the assessment of security patches and security upgrades for applicability as required in Requirement R3 within 30 calendar days after the availability of the patches and upgrades.
CIP-007-4	R3.2.	The Responsible Entity shall document the implementation of security patches. In any case where the patch is not installed, the Responsible Entity shall document compensating measure(s) applied to mitigate risk exposure.	N/A	N/A	N/A	The Responsible Entity did not document the implementation of applicable security patches as required in R3. OR Where an applicable patch was not installed, the Responsible Entity did not document the compensating measure(s) applied to mitigate risk. ~~exposure or an acceptance of risk.~~
CIP-007-4	R4.	Malicious Software Prevention — The Responsible Entity shall use anti-virus software and other malicious software (“malware”) prevention	N/A	N/A	N/A	The Responsible Entity, where technically feasible,

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		tools, where technically feasible, to detect, prevent, deter, and mitigate the introduction, exposure, and propagation of malware on all Cyber Assets within the Electronic Security Perimeter(s).				did not use anti-virus software or other malicious software ("malware") prevention tools, on one or more Cyber Assets within the Electronic Security Perimeter(s).
CIP-007-4	R4.1.	The Responsible Entity shall document and implement anti-virus and malware prevention tools. In the case where anti-virus software and malware prevention tools are not installed, the Responsible Entity shall document compensating measure(s) applied to mitigate risk exposure.	N/A	N/A	N/A	The Responsible Entity did not document the implementation of antivirus and malware prevention tools for cyber assets within the electronic security perimeter. OR The Responsible Entity did not document the implementation of compensating measure(s) applied to mitigate risk exposure where antivirus and malware prevention tools are not installed.

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
CIP-007-4	R4.2.	The Responsible Entity shall document and implement a process for the update of anti-virus and malware prevention "signatures." The process must address testing and installing the signatures.	N/A	N/A	N/A	The Responsible Entity **did not document or did not implement** a process including addressing testing and installing the signatures for the update of anti-virus and malware prevention "signatures."
CIP-007-4	R5.	Account Management — The Responsible Entity shall establish, implement, and document technical and procedural controls that enforce access authentication of, and accountability for, all user activity, and that minimize the risk of unauthorized system access.	N/A	N/A	N/A	The Responsible Entity did not document or did not implement technical and procedural controls that enforce access authentication of, and accountability for, all user activity.
CIP-007-4	R5.1.	The Responsible Entity shall ensure that individual and shared system accounts and authorized access permissions are consistent with the concept of "need to know" with respect to work functions performed.	N/A	N/A	N/A	The Responsible Entity did not ensure that individual and shared system accounts and authorized access permissions are consistent with the concept of "need to know" with respect to work functions performed.
CIP-007-4	R5.1.1.	The Responsible Entity shall ensure that user accounts are implemented	N/A	N/A	N/A	One or more user

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		as approved by designated personnel. Refer to Standard CIP-003-4 Requirement R5.				accounts implemented by the Responsible Entity were not implemented as approved by designated personnel.
CIP-007-4	R5.1.2.	The Responsible Entity shall establish methods, processes, and procedures that generate logs of sufficient detail to create historical audit trails of individual user account access activity for a minimum of ninety days.	N/A	The Responsible Entity generated logs with sufficient detail to create historical audit trails of individual user account access activity, however the logs do not contain activity for a minimum of 90 days.	The Responsible Entity generated logs with insufficient detail to create historical audit trails of individual user account access activity.	The Responsible Entity did not generate logs of individual user account access activity.
CIP-007-4	R5.1.3.	The Responsible Entity shall review, at least annually, user accounts to verify access privileges are in accordance with Standard CIP-003-4 Requirement R5 and Standard CIP-004-4 Requirement R4.	N/A	N/A	N/A	The Responsible Entity did not review, at least annually, user accounts to verify access privileges are in accordance with Standard CIP-003-~~4~~3 Requirement R5 and Standard CIP-004-~~3~~4 Requirement R4.
CIP-007-4	R5.2.	The Responsible Entity shall implement a policy to minimize and manage the scope and acceptable use of administrator, shared, and	N/A	N/A	N/A	The Responsible Entity did not implement a policy to minimize and

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		other generic account privileges including factory default accounts.				manage the scope and acceptable use of administrator, shared, and other generic account privileges including factory default accounts.
CIP-007-4	R5.2.1.	The policy shall include the removal, disabling, or renaming of such accounts where possible. For such accounts that must remain enabled, passwords shall be changed prior to putting any system into service.	N/A	N/A	The Responsible Entity's policy did not include the removal, disabling, or renaming of such accounts where possible, however for accounts that must remain enabled, passwords were changed prior to putting any system into service.	For accounts that must remain enabled, the Responsible Entity did not change passwords prior to putting any system into service.
CIP-007-4	R5.2.2.	The Responsible Entity shall identify those individuals with access to shared accounts.	N/A	N/A	N/A	The Responsible Entity did not identify all individuals with access to shared accounts.
CIP-007-4	R5.2.3.	Where such accounts must be shared, the Responsible Entity shall have a policy for managing the use of such accounts that limits access to only those with authorization, an audit trail of the account use (automated or manual), and steps for securing the account in the event of personnel changes (for example,	N/A	N/A	N/A	Where such accounts must be shared, the Responsible Entity has not implemented (one or more components of) a policy for managing

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		change in assignment or termination).				the use of such accounts that limits access to only those with authorization, an audit trail of the account use (automated or manual), and steps for securing the account in the event of personnel changes (for example, change in assignment or termination).
CIP-007-4	R5.3.	At a minimum, the Responsible Entity shall require and use passwords, subject to the following, as technically feasible:	N/A	N/A	N/A	The Responsible Entity **does not require passwords** subject to R5.3.1, R5.3.2, R5.3.3. OR **Does not use passwords** subject to R5.3.1, R5.3.2, R5.3.3.
CIP-007-4	R5.3.1.	Each password shall be a minimum of six characters.	N/A	N/A	N/A	N/A
CIP-007-4	R5.3.2.	Each password shall consist of a combination of alpha, numeric, and “special” characters.	N/A	N/A	N/A	N/A
CIP-007-4	R5.3.3.	Each password shall be changed at least annually, or more frequently based on risk.	N/A	N/A	N/A	N/A
CIP-007-4	R6.	Security Status Monitoring — The Responsible Entity shall ensure that	N/A	N/A	N/A	The Responsible Entity as technically

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		all Cyber Assets within the Electronic Security Perimeter, as technically feasible, implement automated tools or organizational process controls to monitor system events that are related to cyber security.				feasible, did not implement automated tools or organizational process controls, to monitor system events that are related to cyber security on one or more of Cyber Assets inside the Electronic Security Perimeter(s).
CIP-007-4	R6.1.	The Responsible Entity shall implement and document the organizational processes and technical and procedural mechanisms for monitoring for security events on all Cyber Assets within the Electronic Security Perimeter.	N/A	N/A	N/A	The Responsible Entity **did not implement or did not document** the organizational processes and technical and procedural mechanisms for monitoring for security events on all Cyber Assets within the Electronic Security Perimeter.
CIP-007-4	R6.2.	The security monitoring controls shall issue automated or manual alerts for detected Cyber Security Incidents.	N/A	N/A	N/A	The Responsible entity's security monitoring controls do not issue automated or manual alerts for detected Cyber Security Incidents.

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
CIP-007-4	R6.3.	The Responsible Entity shall maintain logs of system events related to cyber security, where technically feasible, to support incident response as required in Standard CIP-008-4.	N/A	N/A	N/A	The Responsible Entity did not maintain logs of system events related to cyber security, where technically feasible, to support incident response as required in Standard CIP-008.
CIP-007-4	R6.4.	The Responsible Entity shall retain all logs specified in Requirement R6 for ninety calendar days.	N/A	N/A	N/A	The Responsible Entity did not retain one or more of the logs specified in Requirement R6 for at least 90 calendar days.
CIP-007-4	R6.5.	The Responsible Entity shall review logs of system events related to cyber security and maintain records documenting review of logs.	N/A	N/A	N/A	The Responsible Entity did not review logs of system events related to cyber security nor maintain records documenting review of logs.
CIP-007-4	R7.	Disposal or Redeployment — The Responsible Entity shall establish and implement formal methods, processes, and procedures for disposal or redeployment of Cyber Assets within the Electronic Security Perimeter(s) as identified and documented in Standard CIP-005-4.	N/A~~The Responsible Entity established and implemented formal methods, processes, and procedures for disposal and redeployment of Cyber Assets within the Electronic~~	N/A~~The Responsible Entity established and implemented formal methods, processes, and procedures for disposal of Cyber Assets within the Electronic Security~~	The Responsible Entity established and implemented formal methods, processes, and procedures for redeployment of Cyber Assets within the Electronic Security	The Responsible Entity did not establish or implement formal methods, processes, and procedures for disposal or redeployment of Cyber Assets within the Electronic

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
			~~Security Perimeter(s) as identified and documented in Standard CIP-005-3 **but** did not maintain records as specified in R7.3.~~	~~Perimeter(s) as identified and documented in Standard CIP-005-3 **but** did not address redeployment as specified in R7.2.~~	Perimeter(s) as identified and documented in Standard CIP-005-~~4~~3 **but** did not address ~~disposal~~ redeployment as specified in R7.~~2~~1.	Security Perimeter(s) as identified and documented in Standard CIP-005-~~4~~3. OR The Responsible Entity established formal methods, processes, and procedures for redeployment of Cyber Assets within the Electronic Security Perimeter(s) as identified and documented in Standard CIP-005-4 but did not address disposal as specified in R7.1. OR The Responsible Entity did not maintain records pertaining to disposal or[3]

[3] Please note that FERC's January 20, 2011 Order on Version 2 And Version 3 Violation Risk Factors And Violation Severity Levels For Critical Infrastructure Protection Reliability Standards dictated that this should read "…records pertaining to disposal **of** redeployment as specified in R7.3." (Emphasis added) It has come to NERC's attention that it should read "…records pertaining to disposal **or** redeployment as specified in R7.3." (emphasis added) and NERC has made this change accordingly. NERC proposes to remove this footnote from the final approved list of VSLs.

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						redeployment as specified in R7.3.
CIP-007-4	R7.1.	Prior to the disposal of such assets, the Responsible Entity shall destroy or erase the data storage media to prevent unauthorized retrieval of sensitive cyber security or reliability data.	N/A	N/A	N/A	N/A
CIP-007-4	R7.2.	Prior to redeployment of such assets, the Responsible Entity shall, at a minimum, erase the data storage media to prevent unauthorized retrieval of sensitive cyber security or reliability data.	N/A	N/A	N/A	N/A
CIP-007-4	R7.3.	The Responsible Entity shall maintain records that such assets were disposed of or redeployed in accordance with documented procedures.	N/A	N/A	N/A	N/A
CIP-007-4	R8	Cyber Vulnerability Assessment — The Responsible Entity shall perform a cyber vulnerability assessment of all Cyber Assets within the Electronic Security Perimeter at least annually. The vulnerability assessment shall include, at a minimum, the following:	N/A	N/A	N/A	The Responsible Entity did not perform a Vulnerability Assessment on one or more Cyber Assets within the Electronic Security Perimeter at least annually. OR The vulnerability assessment did not include one (1) or more of the subrequirements 8.1, 8.2, 8.3, 8.4.

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
CIP-007-4	R8.1.	A document identifying the vulnerability assessment process;	N/A	N/A	N/A	N/A
CIP-007-4	R8.2.	A review to verify that only ports and services required for operation of the Cyber Assets within the Electronic Security Perimeter are enabled;	N/A	N/A	N/A	N/A
CIP-007-4	R8.3.	A review of controls for default accounts; and,	N/A	N/A	N/A	N/A
CIP-007-4	R8.4.	Documentation of the results of the assessment, the action plan to remediate or mitigate vulnerabilities identified in the assessment, and the execution status of that action plan.	N/A	N/A	N/A	N/A
CIP-007-4	R9	Documentation Review and Maintenance — The Responsible Entity shall review and update the documentation specified in Standard CIP-007-4 at least annually. Changes resulting from modifications to the systems or controls shall be documented within thirty calendar days of the change being completed.	N/A	N/A	The Responsible Entity did not review and update the documentation specified in Standard CIP-007-43 at least annually. OR The Responsible Entity did not document changes resulting from modifications to the systems or controls within thirty calendar days of the change being completed.	The Responsible Entity did not review and update the documentation specified in Standard CIP-007-43 at least annually ~~nor~~ and ~~were~~ changes resulting from modifications to the systems or controls were not documented within thirty calendar days of the change being completed.
CIP-008-4	R1.	Cyber Security Incident Response Plan — The Responsible Entity shall	N/A	N/A~~The Responsible Entity has developed~~	The Responsible Entity has developed	The Responsible Entity has not

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		develop and maintain a Cyber Security Incident response plan and implement the plan in response to Cyber Security Incidents. The Cyber Security Incident response plan shall address, at a minimum, the following:		~~but not maintained a Cyber Security Incident response plan.~~	a Cyber Security Incident response plan ~~but the plan~~that addresses all of the components required by R1.1 through R1.6 but has not maintained the plan in accordance with those components. ~~does not address one or more of the subrequirements R1.1 through R1.6.~~	developed a Cyber Security Incident response plan that addresses all of the components required by R1.1 through R1.6, or has not implemented the plan in response to a Cyber Security Incident.
CIP-008-4	R1.1.	Procedures to characterize and classify events as reportable Cyber Security Incidents.	N/A	N/A	N/A	N/A
CIP-008-4	R1.2.	Response actions, including roles and responsibilities of Cyber Security Incident response teams, Cyber Security Incident handling procedures, and communication plans.	N/A	N/A	N/A	N/A
CIP-008-4	R1.3.	Process for reporting Cyber Security Incidents to the Electricity Sector Information Sharing and Analysis Center (ES-ISAC). The Responsible Entity must ensure that all reportable Cyber Security Incidents are reported to the ES-ISAC either directly or through an intermediary.	N/A	N/A	N/A	N/A
CIP-008-4	R1.4.	Process for updating the Cyber Security Incident response plan within thirty calendar days of any	N/A	N/A	N/A	N/A

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
		changes.				
CIP-008-4	R1.5.	Process for ensuring that the Cyber Security Incident response plan is reviewed at least annually.	N/A	N/A	N/A	N/A
CIP-008-4	R1.6.	Process for ensuring the Cyber Security Incident response plan is tested at least annually. A test of the Cyber Security Incident response plan can range from a paper drill, to a full operational exercise, to the response to an actual incident.	N/A	N/A	N/A	N/A
CIP-008-4	R2	Cyber Security Incident Documentation — The Responsible Entity shall keep relevant documentation related to Cyber Security Incidents reportable per Requirement R1.1 for three calendar years.	N/A	N/A	N/A	The Responsible Entity has not kept relevant documentation related to Cyber Security Incidents reportable per Requirement R1.1 for at least three calendar years.
CIP-009-4	R1	Recovery Plans — The Responsible Entity shall create and annually review recovery plan(s) for Critical Cyber Assets. The recovery plan(s) shall address at a minimum the following:	N/A	N/A	N/A	The Responsible Entity has not created or has not annually reviewed their recovery plan(s) for Critical Cyber Assets OR has created a plan but did not address one or more of the requirements CIP-009-~~4~~3 R1.1 **and** R1.2.

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
CIP-009-4	R1.1.	Specify the required actions in response to events or conditions of varying duration and severity that would activate the recovery plan(s).	N/A	N/A	N/A	N/A
CIP-009-4	R1.2.	Define the roles and responsibilities of responders.	N/A	N/A	N/A	N/A
CIP-009-4	R2	Exercises — The recovery plan(s) shall be exercised at least annually. An exercise of the recovery plan(s) can range from a paper drill, to a full operational exercise, to recovery from an actual incident.	N/A	N/A	N/A	The Responsible Entity's recovery plan(s) have not been exercised at least annually.
CIP-009-4	R3	Change Control — Recovery plan(s) shall be updated to reflect any changes or lessons learned as a result of an exercise or the recovery from an actual incident. Updates shall be communicated to personnel responsible for the activation and implementation of the recovery plan(s) within thirty calendar days of the change being completed.	N/A~~The Responsible Entity's recovery plan(s) have been updated to reflect any changes or lessons learned as a result of an exercise or the recovery from an actual incident but the updates were communicated to personnel responsible for the activation and implementation of the recovery plan(s) in more than30 but less than or equal to 120 calendar days of the change.~~	N/A~~The Responsible Entity's recovery plan(s) have been updated to reflect any changes or lessons learned as a result of an exercise or the recovery from an actual incident but the updates were communicated to personnel responsible for the activation and implementation of the recovery plan(s) in more than 120 but less than or equal to 150 calendar days of the change.~~	N/A~~The Responsible Entity's recovery plan(s) have been updated to reflect any changes or lessons learned as a result of an exercise or the recovery from an actual incident but the updates were communicated to personnel responsible for the activation and implementation of the recovery plan(s) in more than 150 but less than or equal to 180 calendar days of the change.~~	The Responsible Entity's recovery plan(s) have not been updated to reflect any changes or lessons learned as a result of an exercise or the recovery from an actual incident. OR The Responsible Entity's recovery plan(s) have been updated to reflect any changes or lessons learned as a result of an exercise or the recovery from an actual incident but the updates

Standard Number	Requirement Number	Text of Requirement	Lower VSL	Moderate VSL	High VSL	Severe VSL
						were not communicated to personnel responsible for the activation and implementation of the recovery plan(s) within in thirty ~~more than 180~~ calendar days of the change.
CIP-009-4	R4	Backup and Restore — The recovery plan(s) shall include processes and procedures for the backup and storage of information required to successfully restore Critical Cyber Assets. For example, backups may include spare electronic components or equipment, written documentation of configuration settings, tape backup, etc.	N/A	N/A	N/A	The Responsible Entity's recovery plan(s) do not include processes and procedures for the backup and storage of information required to successfully restore Critical Cyber Assets.
CIP-009-4	R5	Testing Backup Media — Information essential to recovery that is stored on backup media shall be tested at least annually to ensure that the information is available. Testing can be completed off site.	N/A	N/A	N/A	The Responsible Entity's information essential to recovery that is stored on backup media has not been tested at least annually to ensure that the information is available.

Standard Number	Requirement Number	Text of Requirement	VRF
CIP-002-4	R1.	Critical Asset Identification — The Responsible Entity shall develop a list of its identified Critical Assets determined through an annual application of the criteria contained in *CIP-002-4 Attachment 1 – Critical Asset Criteria*. The Responsible Entity shall update this list as necessary, and review it at least annually.	HIGH
CIP-002-4	R2.	Critical Cyber Asset Identification— Using the list of Critical Assets developed pursuant to Requirement R1, the Responsible Entity shall develop a list of associated Critical Cyber Assets essential to the operation of the Critical Asset. The Responsible Entity shall update this list as necessary, and review it at least annually. For each group of generating units (including nuclear generation) at a single plant location identified in Attachment 1, criterion 1.1, the only Cyber Assets that must be considered are those shared Cyber Assets that could, within 15 minutes, adversely impact the reliable operation of any combination of units that in aggregate equal or exceed Attachment 1, criterion For the purpose of Standard CIP 002-4, Critical Cyber Assets are further qualified to be those having at least one of the following characteristics: • The Cyber Asset uses a routable protocol to communicate outside the Electronic Security Perimeter; or, • The Cyber Asset uses a routable protocol within a control center; or, • The Cyber Asset is dial-up accessible.	HIGH
CIP-002-4	R3.	Annual Approval —The senior manager or delegate(s) shall approve annually the list of Critical Assets and the list of Critical Cyber Assets. Based on Requirements R1 and R2 the Responsible Entity may determine that it has no Critical Assets or Critical Cyber Assets. The Responsible Entity shall keep a signed and dated record of the senior manager or delegate(s)'s	LOWER

Standard Number	Requirement Number	Text of Requirement	VRF
		approval of the list of Critical Assets and the list of Critical Cyber Assets (even if such lists are null.)	
CIP-003-4	R1.	Cyber Security Policy — The Responsible Entity shall document and implement a cyber security policy that represents management's commitment and ability to secure its Critical Cyber Assets. The Responsible Entity shall, at minimum, ensure the following:	MEDIUM
CIP-003-4	R1.1.	The cyber security policy addresses the requirements in Standards CIP-002-4 through CIP-009-4, including provision for emergency situations.	LOWER
CIP-003-4	R1.2.	The cyber security policy is readily available to all personnel who have access to, or are responsible for, Critical Cyber Assets.	LOWER
CIP-003-4	R1.3	Annual review and approval of the cyber security policy by the senior manager assigned pursuant to R2.	LOWER
CIP-003-4	R2.	Leadership — The Responsible Entity shall assign a senior manager with overall responsibility for leading and managing the entity's implementation of, and adherence to, Standards CIP-002-4 through CIP-009-4.	~~LOWER~~MEDIUM
CIP-003-4	R2.1.	The senior manager shall be identified by name, title, and date of designation.	LOWER
CIP-003-4	R2.2.	Changes to the senior manager must be documented within thirty calendar days of the effective date.	LOWER
CIP-003-4	R2.3.	Where allowed by Standards CIP-002-4 through CIP-009-4, the senior manager may delegate authority for specific actions to a named delegate or delegates. These delegations shall be documented in the same manner as R2.1 and R2.2, and approved by the senior manager.	LOWER
CIP-003-4	R2.4	The senior manager or delegate(s), shall authorize and document any exception from the requirements of the cyber security policy.	LOWER
CIP-003-4	R3.	Exceptions — Instances where the Responsible Entity cannot conform to its cyber security policy must be documented as exceptions and authorized by the senior manager or delegate(s).	LOWER
CIP-003-4	R3.1.	Exceptions to the Responsible Entity's cyber security policy must be documented within thirty days of being approved by the senior manager or delegate(s).	LOWER
CIP-003-4	R3.2.	Documented exceptions to the cyber security policy must include an explanation as to why the exception is necessary and any compensating measures.	LOWER
CIP-003-4	R3.3.	Authorized exceptions to the cyber security policy must be reviewed and approved annually by the senior manager or delegate(s) to ensure the exceptions are still required and valid. Such review and approval shall be documented.	LOWER

Standard Number	Requirement Number	Text of Requirement	VRF
CIP-003-4	R4.	Information Protection — The Responsible Entity shall implement and document a program to identify, classify, and protect information associated with Critical Cyber Assets.	MEDIUM
CIP-003-4	R4.1.	The Critical Cyber Asset information to be protected shall include, at a minimum and regardless of media type, operational procedures, lists as required in Standard CIP-002-4, network topology or similar diagrams, floor plans of computing centers that contain Critical Cyber Assets, equipment layouts of Critical Cyber Assets, disaster recovery plans, incident response plans, and security configuration information.	MEDIUM
CIP-003-4	R4.2.	The Responsible Entity shall classify information to be protected under this program based on the sensitivity of the Critical Cyber Asset information.	LOWER
CIP-003-4	R4.3.	The Responsible Entity shall, at least annually, assess adherence to its Critical Cyber Asset information protection program, document the assessment results, and implement an action plan to remediate deficiencies identified during the assessment.	LOWER
CIP-003-4	R5.	Access Control — The Responsible Entity shall document and implement a program for managing access to protected Critical Cyber Asset information.	LOWER
CIP-003-4	R5.1.	The Responsible Entity shall maintain a list of designated personnel who are responsible for authorizing logical or physical access to protected information.	LOWER
CIP-003-4	R5.1.1.	Personnel shall be identified by name, title, and the information for which they are responsible for authorizing access.	LOWER
CIP-003-4	R5.1.2.	The list of personnel responsible for authorizing access to protected information shall be verified at least annually.	LOWER
CIP-003-4	R5.2.	The Responsible Entity shall review at least annually the access privileges to protected information to confirm that access privileges are correct and that they correspond with the Responsible Entity's needs and appropriate personnel roles and responsibilities.	LOWER
CIP-003-4	R5.3.	The Responsible Entity shall assess and document at least annually the processes for controlling access privileges to protected information.	LOWER
CIP-003-4	R6.	Change Control and Configuration Management — The Responsible Entity shall establish and document a process of change control and configuration management for adding, modifying, replacing, or removing Critical Cyber Asset hardware or software, and implement supporting configuration management activities to identify, control and document all entity or vendor related changes to hardware and software components of Critical Cyber Assets pursuant to the change control process.	LOWER
CIP-004-4	R1.	Awareness — The Responsible Entity shall establish, document, implement, and maintain a security awareness program to ensure personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets receive on-going reinforcement in sound security practices. The program shall include security awareness reinforcement on at least a quarterly basis using mechanisms such as:	LOWER

Standard Number	Requirement Number	Text of Requirement	VRF
		• Direct communications (e.g. emails, memos, computer based training, etc.); • Indirect communications (e.g. posters, intranet, brochures, etc.); • Management support and reinforcement (e.g., presentations, meetings, etc.).	
CIP-004-4	R2.	Training — The Responsible Entity shall establish, document, implement, and maintain an annual cyber security training program for personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets. The cyber security training program shall be reviewed annually, at a minimum, and shall be updated whenever necessary.	LOWER
CIP-004-4	R2.1.	This program will ensure that all personnel having such access to Critical Cyber Assets, including contractors and service vendors, are trained prior to their being granted such access except in specified circumstances such as an emergency.	MEDIUM
CIP-004-4	R2.2.	Training shall cover the policies, access controls, and procedures as developed for the Critical Cyber Assets covered by CIP-004-4, and include, at a minimum, the following required items appropriate to personnel roles and responsibilities:	MEDIUM
CIP-004-4	R2.2.1.	The proper use of Critical Cyber Assets;	LOWER
CIP-004-4	R2.2.2.	Physical and electronic access controls to Critical Cyber Assets;	LOWER
CIP-004-4	R2.2.3.	The proper handling of Critical Cyber Asset information; and,	LOWER
CIP-004-4	R2.2.4.	Action plans and procedures to recover or re-establish Critical Cyber Assets and access thereto following a Cyber Security Incident.	MEDIUM
CIP-004-4	R2.3.	The Responsible Entity shall maintain documentation that training is conducted at least annually, including the date the training was completed and attendance records.	LOWER
CIP-004-4	R3.	Personnel Risk Assessment —The Responsible Entity shall have a documented personnel risk assessment program, in accordance with federal, state, provincial, and local laws, and subject to existing collective bargaining unit agreements, for personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets. A personnel risk assessment shall be conducted pursuant to that program prior to such personnel being granted such access except in specified circumstances such as an emergency. The personnel risk assessment program shall at a minimum include:	MEDIUM
CIP-004-4	R3.1.	The Responsible Entity shall ensure that each assessment conducted include, at least, identity verification (e.g., Social Security Number verification in the U.S.) and seven year criminal check. The Responsible Entity may conduct more detailed reviews, as permitted by law and subject to existing collective bargaining unit agreements, depending upon the criticality of the position.	LOWER

Standard Number	Requirement Number	Text of Requirement	VRF
CIP-004-4	R3.2.	The Responsible Entity shall update each personnel risk assessment at least every seven years after the initial personnel risk assessment or for cause.	LOWER
CIP-004-4	R3.3.	The Responsible Entity shall document the results of personnel risk assessments of its personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets, and that personnel risk assessments of contractor and service vendor personnel with such access are conducted pursuant to Standard CIP-004-4.	LOWER
CIP-004-4	R4.	Access — The Responsible Entity shall maintain list(s) of personnel with authorized cyber or authorized unescorted physical access to Critical Cyber Assets, including their specific electronic and physical access rights to Critical Cyber Assets.	LOWER
CIP-004-4	R4.1.	The Responsible Entity shall review the list(s) of its personnel who have such access to Critical Cyber Assets quarterly, and update the list(s) within seven calendar days of any change of personnel with such access to Critical Cyber Assets, or any change in the access rights of such personnel. The Responsible Entity shall ensure access list(s) for contractors and service vendors are properly maintained.	LOWER
CIP-004-4	R4.2.	The Responsible Entity shall revoke such access to Critical Cyber Assets within 24 hours for personnel terminated for cause and within seven calendar days for personnel who no longer require such access to Critical Cyber Assets.	LOWER
CIP-005-4	R1.	Electronic Security Perimeter — The Responsible Entity shall ensure that every Critical Cyber Asset resides within an Electronic Security Perimeter. The Responsible Entity shall identify and document the Electronic Security Perimeter(s) and all access points to the perimeter(s).	MEDIUM
CIP-005-4	R1.1.	Access points to the Electronic Security Perimeter(s) shall include any externally connected communication end point (for example, dial-up modems) terminating at any device within the Electronic Security Perimeter(s).	MEDIUM
CIP-005-4	R1.2.	For a dial-up accessible Critical Cyber Asset that uses a non-routable protocol, the Responsible Entity shall define an Electronic Security Perimeter for that single access point at the dial-up device.	MEDIUM
CIP-005-4	R1.3.	Communication links connecting discrete Electronic Security Perimeters shall not be considered part of the Electronic Security Perimeter. However, end points of these communication links within the Electronic Security Perimeter(s) shall be considered access points to the Electronic Security Perimeter(s).	MEDIUM
CIP-005-4	R1.4.	Any non-critical Cyber Asset within a defined Electronic Security Perimeter shall be identified and protected pursuant to the requirements of Standard CIP-005-4.	MEDIUM
CIP-005-4	R1.5.	Cyber Assets used in the access control and/or monitoring of the Electronic Security Perimeter(s) shall be afforded the protective measures as a specified in Standard CIP-003-4; Standard CIP-004-4 Requirement R3; Standard CIP-005-4 Requirements R2 and R3; Standard CIP-006-4 Requirement R3; Standard CIP-007-4 Requirements R1 and R3	MEDIUM

Standard Number	Requirement Number	Text of Requirement	VRF
		through R9; Standard CIP-008-4; and Standard CIP-009-4.	
CIP-005-4	R1.6.	The Responsible Entity shall maintain documentation of Electronic Security Perimeter(s), all interconnected Critical and non-critical Cyber Assets within the Electronic Security Perimeter(s), all electronic access points to the Electronic Security Perimeter(s) and the Cyber Assets deployed for the access control and monitoring of these access points.	LOWER
CIP-005-4	R2.	Electronic Access Controls — The Responsible Entity shall implement and document the organizational processes and technical and procedural mechanisms for control of electronic access at all electronic access points to the Electronic Security Perimeter(s).	MEDIUM
CIP-005-4	R2.1.	These processes and mechanisms shall use an access control model that denies access by default, such that explicit access permissions must be specified.	MEDIUM
CIP-005-4	R2.2.	At all access points to the Electronic Security Perimeter(s), the Responsible Entity shall enable only ports and services required for operations and for monitoring Cyber Assets within the Electronic Security Perimeter, and shall document, individually or by specified grouping, the configuration of those ports and services.	MEDIUM
CIP-005-4	R2.3.	The Responsible Entity shall implement and maintain a procedure for securing dial-up access to the Electronic Security Perimeter(s).	MEDIUM
CIP-005-4	R2.4.	Where external interactive access into the Electronic Security Perimeter has been enabled, the Responsible Entity shall implement strong procedural or technical controls at the access points to ensure authenticity of the accessing party, where technically feasible.	MEDIUM
CIP-005-4	R2.5.	The required documentation shall, at least, identify and describe:	LOWER
CIP-005-4	R2.5.1.	The processes for access request and authorization.	LOWER
CIP-005-4	R2.5.2.	The authentication methods.	LOWER
CIP-005-4	R2.5.3.	The review process for authorization rights, in accordance with Standard CIP-004-4 Requirement R4.	LOWER
CIP-005-4	R2.5.4.	The controls used to secure dial-up accessible connections.	LOWER
CIP-005-4	R2.6.	Appropriate Use Banner — Where technically feasible, electronic access control devices shall display an appropriate use banner on the user screen upon all interactive access attempts. The Responsible Entity shall maintain a document identifying the content of the banner.	LOWER
CIP-005-4	R3.	Monitoring Electronic Access — The Responsible Entity shall implement and document an electronic or manual process(es) for monitoring and logging access at access points to the Electronic Security Perimeter(s) twenty-four hours a day, seven days a week.	MEDIUM

Standard Number	Requirement Number	Text of Requirement	VRF
CIP-005-4	R3.1.	For dial-up accessible Critical Cyber Assets that use non-routable protocols, the Responsible Entity shall implement and document monitoring process(es) at each access point to the dial-up device, where technically feasible.	MEDIUM
CIP-005-4	R3.2.	Where technically feasible, the security monitoring process(es) shall detect and alert for attempts at or actual unauthorized accesses. These alerts shall provide for appropriate notification to designated response personnel. Where alerting is not technically feasible, the Responsible Entity shall review or otherwise assess access logs for attempts at or actual unauthorized accesses at least every ninety calendar days.	MEDIUM
CIP-005-4	R4.	Cyber Vulnerability Assessment — The Responsible Entity shall perform a cyber vulnerability assessment of the electronic access points to the Electronic Security Perimeter(s) at least annually. The vulnerability assessment shall include, at a minimum, the following:	MEDIUM
CIP-005-4	R4.1.	A document identifying the vulnerability assessment process;	LOWER
CIP-005-4	R4.2.	A review to verify that only ports and services required for operations at these access points are enabled;	MEDIUM
CIP-005-4	R4.3.	The discovery of all access points to the Electronic Security Perimeter;	MEDIUM
CIP-005-4	R4.4.	A review of controls for default accounts, passwords, and network management community strings;	MEDIUM
CIP-005-4	R4.5.	Documentation of the results of the assessment, the action plan to remediate or mitigate vulnerabilities identified in the assessment, and the execution status of that action plan.	MEDIUM
CIP-005-4	R5.	Documentation Review and Maintenance — The Responsible Entity shall review, update, and maintain all documentation to support compliance with the requirements of Standard CIP-005-4.	LOWER
CIP-005-4	R5.1.	The Responsible Entity shall ensure that all documentation required by Standard CIP-005-4 reflect current configurations and processes and shall review the documents and procedures referenced in Standard CIP-005-4 at least annually.	LOWER
CIP-005-4	R5.2.	The Responsible Entity shall update the documentation to reflect the modification of the network or controls within ninety calendar days of the change.	LOWER
CIP-005-4	R5.3.	The Responsible Entity shall retain electronic access logs for at least ninety calendar days. Logs related to reportable incidents shall be kept in accordance with the requirements of Standard CIP-008-4.	LOWER
CIP-006-4c	R1.	Physical Security Plan — The Responsible Entity shall document, implement, and maintain a physical security plan, approved by the senior manager or delegate(s) that shall address, at a minimum, the following:	MEDIUM

Standard Number	Requirement Number	Text of Requirement	VRF
CIP-006-4c	R1.1.	All Cyber Assets within an Electronic Security Perimeter shall reside within an identified Physical Security Perimeter. Where a completely enclosed ("six-wall") border cannot be established, the Responsible Entity shall deploy and document alternative measures to control physical access to such Cyber Assets.	MEDIUM
CIP-006-4c	R1.2.	Identification of all physical access points through each Physical Security Perimeter and measures to control entry at those access points.	MEDIUM
CIP-006-4c	R1.3	Processes, tools, and procedures to monitor physical access to the perimeter(s).	MEDIUM
CIP-006-4c	R1.4	Appropriate use of physical access controls as described in Requirement R4 including visitor pass management, response to loss, and prohibition of inappropriate use of physical access controls.	MEDIUM
CIP-006-4c	R1.5	Review of access authorization requests and revocation of access authorization, in accordance with CIP-004-4 Requirement R4.	MEDIUM
CIP-006-4c	R1.6	A visitor control program for visitors (personnel without authorized unescorted access to a Physical Security Perimeter), containing at a minimum the following:	MEDIUM
CIP-006-4c	R1.6.1	Logs (manual or automated) to document the entry and exit of visitors, including the date and time, to and from Physical Security Perimeters.	MEDIUM
CIP-006-4c	R1.6.2	Continuous escorted access of visitors within the Physical Security Perimeter	MEDIUM
CIP-006-4c	R1.7	Update of the physical security plan within thirty calendar days of the completion of any physical security system redesign or reconfiguration, including, but not limited to, addition or removal of access points through the Physical Security Perimeter, physical access controls, monitoring controls, or logging controls.	LOWER
CIP-006-4c	R1.8	Annual review of the physical security plan.	LOWER
CIP-006-4c	R2	Protection of Physical Access Control Systems — Cyber Assets that authorize and/or log access to the Physical Security Perimeter(s), exclusive of hardware at the Physical Security Perimeter access point such as electronic lock control mechanisms and badge readers, shall:	MEDIUM
CIP-006-4c	R2.1.	Be protected from unauthorized physical access.	MEDIUM
CIP-006-4c	R2.2.	Be afforded the protective measures specified in Standard CIP-003-4; Standard CIP-004-4 Requirement R3; Standard CIP-005-4 Requirements R2 and R3; Standard CIP-006-4a Requirements R4 and R5; Standard CIP-007-4; Standard CIP-008-4; and Standard CIP-009-4.	MEDIUM
CIP-006-4c	R3	Protection of Electronic Access Control Systems — Cyber Assets used in the access control and/or monitoring of the Electronic Security Perimeter(s) shall reside within an	MEDIUM

Standard Number	Requirement Number	Text of Requirement	VRF
		identified Physical Security Perimeter.	
CIP-006-4c	R4	Physical Access Controls — The Responsible Entity shall document and implement the operational and procedural controls to manage physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week. The Responsible Entity shall implement one or more of the following physical access methods: • Card Key: A means of electronic access where the access rights of the card holder are predefined in a computer database. Access rights may differ from one perimeter to another. • Special Locks: These include, but are not limited to, locks with "restricted key" systems, magnetic locks that can be operated remotely, and "man-trap" systems. • Security Personnel: Personnel responsible for controlling physical access who may reside on-site or at a monitoring station. • Other Authentication Devices: Biometric, keypad, token, or other equivalent devices that control physical access to the Critical Cyber Assets	MEDIUM
CIP-006-4c	R5	Monitoring Physical Access — The Responsible Entity shall document and implement the technical and procedural controls for monitoring physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week. Unauthorized access attempts shall be reviewed immediately and handled in accordance with the procedures specified in Requirement CIP-008-4. One or more of the following monitoring methods shall be used: • Alarm Systems: Systems that alarm to indicate a door, gate or window has been opened without authorization. These alarms must provide for immediate notification to personnel responsible for response. • Human Observation of Access Points: Monitoring of physical access points by authorized personnel as specified in Requirement R4.	MEDIUM
CIP-006-4c	R6	Logging Physical Access — Logging shall record sufficient information to uniquely identify individuals and the time of access twenty-four hours a day, seven days a week. The Responsible Entity shall implement and document the technical and procedural mechanisms for logging physical entry at all access points to the Physical Security Perimeter(s) using one or more of the following logging methods or their equivalent: • Computerized Logging: Electronic logs produced by the Responsible Entity's	LOWER

Standard Number	Requirement Number	Text of Requirement	VRF
		selected access control and monitoring method. • Video Recording: Electronic capture of video images of sufficient quality to determine identity. • Manual Logging: A log book or sign-in sheet, or other record of physical access maintained by security or other personnel authorized to control and monitor physical access as specified in Requirement R4	
CIP-006-4c	R7	Access Log Retention — The responsible entity shall retain physical access logs for at least ninety calendar days. Logs related to reportable incidents shall be kept in accordance with the requirements of Standard CIP-008-4.	LOWER
CIP-006-4c	R8	Maintenance and Testing — The Responsible Entity shall implement a maintenance and testing program to ensure that all physical security systems under Requirements R4, R5, and R6 function properly. The program must include, at a minimum, the following:	MEDIUM
CIP-006-4c	R8.1	Testing and maintenance of all physical security mechanisms on a cycle no longer than three years.	MEDIUM
CIP-006-4c	R8.2	Retention of testing and maintenance records for the cycle determined by the Responsible Entity in Requirement R8.1.	LOWER
CIP-006-4c	R8.3	Retention of outage records regarding access controls, logging, and monitoring for a minimum of one calendar year.	LOWER
CIP-007-4	R1.	Test Procedures — The Responsible Entity shall ensure that new Cyber Assets and significant changes to existing Cyber Assets within the Electronic Security Perimeter do not adversely affect existing cyber security controls. For purposes of Standard CIP-007-4, a significant change shall, at a minimum, include implementation of security patches, cumulative service packs, vendor releases, and version upgrades of operating systems, applications, database platforms, or other third-party software or firmware.	MEDIUM
CIP-007-4	R1.1.	The Responsible Entity shall create, implement, and maintain cyber security test procedures in a manner that minimizes adverse effects on the production system or its operation.	LOWER
CIP-007-4	R1.2.	The Responsible Entity shall document that testing is performed in a manner that reflects the production environment.	LOWER
CIP-007-4	R1.3.	The Responsible Entity shall document test results.	LOWER
CIP-007-4	R2.	Ports and Services — The Responsible Entity shall establish, document and implement a process to ensure that only those ports and services required for normal and emergency operations are enabled.	MEDIUM
CIP-007-4	R2.1.	The Responsible Entity shall enable only those ports and services required for normal	MEDIUM

Standard Number	Requirement Number	Text of Requirement	VRF
		and emergency operations.	
CIP-007-4	R2.2.	The Responsible Entity shall disable other ports and services, including those used for testing purposes, prior to production use of all Cyber Assets inside the Electronic Security Perimeter(s).	MEDIUM
CIP-007-4	R2.3.	In the case where unused ports and services cannot be disabled due to technical limitations, the Responsible Entity shall document compensating measure(s) applied to mitigate risk exposure.	MEDIUM
CIP-007-4	R3.	Security Patch Management — The Responsible Entity, either separately or as a component of the documented configuration management process specified in CIP-003-4 Requirement R6, shall establish, document and implement a security patch management program for tracking, evaluating, testing, and installing applicable cyber security software patches for all Cyber Assets within the Electronic Security Perimeter(s).	LOWER
CIP-007-4	R3.1.	The Responsible Entity shall document the assessment of security patches and security upgrades for applicability within thirty calendar days of availability of the patches or upgrades.	LOWER
CIP-007-4	R3.2.	The Responsible Entity shall document the implementation of security patches. In any case where the patch is not installed, the Responsible Entity shall document compensating measure(s) applied to mitigate risk exposure.	LOWER
CIP-007-4	R4.	Malicious Software Prevention — The Responsible Entity shall use anti-virus software and other malicious software ("malware") prevention tools, where technically feasible, to detect, prevent, deter, and mitigate the introduction, exposure, and propagation of malware on all Cyber Assets within the Electronic Security Perimeter(s).	MEDIUM
CIP-007-4	R4.1.	The Responsible Entity shall document and implement anti-virus and malware prevention tools. In the case where anti-virus software and malware prevention tools are not installed, the Responsible Entity shall document compensating measure(s) applied to mitigate risk exposure.	MEDIUM
CIP-007-4	R4.2.	The Responsible Entity shall document and implement a process for the update of anti-virus and malware prevention "signatures." The process must address testing and installing the signatures.	MEDIUM
CIP-007-4	R5.	Account Management — The Responsible Entity shall establish, implement, and document technical and procedural controls that enforce access authentication of, and accountability for, all user activity, and that minimize the risk of unauthorized system access.	LOWER
CIP-007-4	R5.1.	The Responsible Entity shall ensure that individual and shared system accounts and authorized access permissions are consistent with the concept of "need to know" with respect to work functions performed.	MEDIUM
CIP-007-4	R5.1.1.	The Responsible Entity shall ensure that user accounts are implemented as approved by	LOWER

Standard Number	Requirement Number	Text of Requirement	VRF
		designated personnel. Refer to Standard CIP-003-4 Requirement R5.	
CIP-007-4	R5.1.2.	The Responsible Entity shall establish methods, processes, and procedures that generate logs of sufficient detail to create historical audit trails of individual user account access activity for a minimum of ninety days.	LOWER
CIP-007-4	R5.1.3.	The Responsible Entity shall review, at least annually, user accounts to verify access privileges are in accordance with Standard CIP-003-4 Requirement R5 and Standard CIP-004-4 Requirement R4.	MEDIUM
CIP-007-4	R5.2.	The Responsible Entity shall implement a policy to minimize and manage the scope and acceptable use of administrator, shared, and other generic account privileges including factory default accounts.	LOWER
CIP-007-4	R5.2.1.	The policy shall include the removal, disabling, or renaming of such accounts where possible. For such accounts that must remain enabled, passwords shall be changed prior to putting any system into service.	MEDIUM
CIP-007-4	R5.2.2.	The Responsible Entity shall identify those individuals with access to shared accounts.	LOWER
CIP-007-4	R5.2.3.	Where such accounts must be shared, the Responsible Entity shall have a policy for managing the use of such accounts that limits access to only those with authorization, an audit trail of the account use (automated or manual), and steps for securing the account in the event of personnel changes (for example, change in assignment or termination).	MEDIUM
CIP-007-4	R5.3.	At a minimum, the Responsible Entity shall require and use passwords, subject to the following, as technically feasible:	LOWER
CIP-007-4	R5.3.1.	Each password shall be a minimum of six characters.	LOWER
CIP-007-4	R5.3.2.	Each password shall consist of a combination of alpha, numeric, and “special” characters.	LOWER
CIP-007-4	R5.3.3.	Each password shall be changed at least annually, or more frequently based on risk.	MEDIUM
CIP-007-4	R6.	Security Status Monitoring — The Responsible Entity shall ensure that all Cyber Assets within the Electronic Security Perimeter, as technically feasible, implement automated tools or organizational process controls to monitor system events that are related to cyber security.	LOWER
CIP-007-4	R6.1.	The Responsible Entity shall implement and document the organizational processes and technical and procedural mechanisms for monitoring for security events on all Cyber Assets within the Electronic Security Perimeter.	MEDIUM
CIP-007-4	R6.2.	The security monitoring controls shall issue automated or manual alerts for detected Cyber Security Incidents.	MEDIUM
CIP-007-4	R6.3.	The Responsible Entity shall maintain logs of system events related to cyber security, where technically feasible, to support incident response as required in Standard CIP-008-4.	MEDIUM

Standard Number	Requirement Number	Text of Requirement	VRF
CIP-007-4	R6.4.	The Responsible Entity shall retain all logs specified in Requirement R6 for ninety calendar days.	LOWER
CIP-007-4	R6.5.	The Responsible Entity shall review logs of system events related to cyber security and maintain records documenting review of logs.	LOWER
CIP-007-4	R7.	Disposal or Redeployment — The Responsible Entity shall establish and implement formal methods, processes, and procedures for disposal or redeployment of Cyber Assets within the Electronic Security Perimeter(s) as identified and documented in Standard CIP-005-4.	LOWER
CIP-007-4	R7.1.	Prior to the disposal of such assets, the Responsible Entity shall destroy or erase the data storage media to prevent unauthorized retrieval of sensitive cyber security or reliability data.	LOWER
CIP-007-4	R7.2.	Prior to redeployment of such assets, the Responsible Entity shall, at a minimum, erase the data storage media to prevent unauthorized retrieval of sensitive cyber security or reliability data.	LOWER
CIP-007-4	R7.3.	The Responsible Entity shall maintain records that such assets were disposed of or redeployed in accordance with documented procedures.	LOWER
CIP-007-4	R8	Cyber Vulnerability Assessment — The Responsible Entity shall perform a cyber vulnerability assessment of all Cyber Assets within the Electronic Security Perimeter at least annually. The vulnerability assessment shall include, at a minimum, the following:	LOWER
CIP-007-4	R8.1.	A document identifying the vulnerability assessment process;	LOWER
CIP-007-4	R8.2.	A review to verify that only ports and services required for operation of the Cyber Assets within the Electronic Security Perimeter are enabled;	MEDIUM
CIP-007-4	R8.3.	A review of controls for default accounts; and,	MEDIUM
CIP-007-4	R8.4.	Documentation of the results of the assessment, the action plan to remediate or mitigate vulnerabilities identified in the assessment, and the execution status of that action plan.	MEDIUM
CIP-007-4	R9	Documentation Review and Maintenance — The Responsible Entity shall review and update the documentation specified in Standard CIP-007-4 at least annually. Changes resulting from modifications to the systems or controls shall be documented within thirty calendar days of the change being completed.	LOWER
CIP-008-4	R1.	Cyber Security Incident Response Plan — The Responsible Entity shall develop and maintain a Cyber Security Incident response plan and implement the plan in response to Cyber Security Incidents. The Cyber Security Incident response plan shall address, at a minimum, the following:	LOWER
CIP-008-4	R1.1.	Procedures to characterize and classify events as reportable Cyber Security Incidents.	LOWER

Standard Number	Requirement Number	Text of Requirement	VRF
CIP-008-4	R1.2.	Response actions, including roles and responsibilities of Cyber Security Incident response teams, Cyber Security Incident handling procedures, and communication plans.	LOWER
CIP-008-4	R1.3.	Process for reporting Cyber Security Incidents to the Electricity Sector Information Sharing and Analysis Center (ES-ISAC). The Responsible Entity must ensure that all reportable Cyber Security Incidents are reported to the ES-ISAC either directly or through an intermediary.	LOWER
CIP-008-4	R1.4.	Process for updating the Cyber Security Incident response plan within thirty calendar days of any changes.	LOWER
CIP-008-4	R1.5.	Process for ensuring that the Cyber Security Incident response plan is reviewed at least annually.	LOWER
CIP-008-4	R1.6.	Process for ensuring the Cyber Security Incident response plan is tested at least annually. A test of the Cyber Security Incident response plan can range from a paper drill, to a full operational exercise, to the response to an actual incident.	LOWER
CIP-008-4	R2	Cyber Security Incident Documentation — The Responsible Entity shall keep relevant documentation related to Cyber Security Incidents reportable per Requirement R1.1 for three calendar years.	LOWER
CIP-009-4	R1	Recovery Plans — The Responsible Entity shall create and annually review recovery plan(s) for Critical Cyber Assets. The recovery plan(s) shall address at a minimum the following:	MEDIUM
CIP-009-4	R1.1.	Specify the required actions in response to events or conditions of varying duration and severity that would activate the recovery plan(s).	MEDIUM
CIP-009-4	R1.2.	Define the roles and responsibilities of responders.	MEDIUM
CIP-009-4	R2	Exercises — The recovery plan(s) shall be exercised at least annually. An exercise of the recovery plan(s) can range from a paper drill, to a full operational exercise, to recovery from an actual incident.	LOWER
CIP-009-4	R3	Change Control — Recovery plan(s) shall be updated to reflect any changes or lessons learned as a result of an exercise or the recovery from an actual incident. Updates shall be communicated to personnel responsible for the activation and implementation of the recovery plan(s) within thirty calendar days of the change being completed.	LOWER
CIP-009-4	R4	Backup and Restore — The recovery plan(s) shall include processes and procedures for the backup and storage of information required to successfully restore Critical Cyber Assets. For example, backups may include spare electronic components or equipment, written documentation of configuration settings, tape backup, etc.	LOWER
CIP-009-4	R5	Testing Backup Media — Information essential to recovery that is stored on backup media shall be tested at least annually to ensure that the information is available. Testing can be completed off site.	LOWER

NEW Exhibit G

Standard Drafting Team Meeting Minutes

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Cyber Security Order 706 Standard Drafting Team

DRAFT ORGANIZATIONAL MEETING SUMMARY

October 6, 2008 | 1 p.m. – 5 p.m.
October 7, 2008 | 8 a.m. – 5 p.m.
October 8, 2008 | 8 a.m. – 12 p.m.
National Institute of Standards and Technology, Gaithersburg, MD

MEETING SUMMARY CONTENTS

Meeting Facilitation and Draft Report By: Robert Jones, Stuart Langton & Hal Beardall
FCRC Consensus Solutions- Florida Conflict Resolution Consortium**, Florida State University**

Thanks to Team members Sharon Edwards, Kevin Perry and Tom Hofstetter for sharing their meeting notes.

http://www.nerc.com/filez/standards/Project_2008-06_Cyber_Security.html

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Cyber Security Order 706 Standard Drafting Team

DRAFT ORGANIZATIONAL MEETING SUMMARY

EXECUTIVE SUMMARY

The Chair and Vice Chair welcomed the members and reviewed with the Standard Development Team (SDT) and participants the proposed meeting agenda. Team Members introduced themselves highlighting a broad spectrum of expertise and industry and governmental perspectives and a shared expectation that they would keep the needs of the industry in mind, but do the right thing. Several noted the importance of engaging and involving Canada in the standards development process. Others pointed to the fact the industry must successfully respond to the cyber security challenges facing the bulk electric system or risk a regulatory response and imposed "solution."

Following the Team and staff introductions, Michael Assante, NERC's Chief Security Officer, offered welcoming remarks and opening comments for the Team's consideration. He noted that this was an unusual standards development process surrounded by an increased level of attention and some sense of urgency. He urged the Team to focus on their standards development task and to take the time necessary to build consensus and answer the critical challenge of coming up with practical solutions that address the directives of FERC and the concerns of the industry. NERC is providing its staff expertise and facilitation assistance to do everything it can to make this effort a success. Mr. Assante also noted the context of President Rick Sergel's recent industry stakeholder letter and congressional testimony highlighting the industry's commitment to making a priority of enhancing security leadership and situational awareness of the urgency of the threat while improving the industry response to cyber security and critical infrastructure protection concerns for the bulk power system in North America.

David Taylor, NERC Manager of Standards Development, reviewed with the Team the need to comply with NERC's Antitrust Guidelines. He then provided an overview of the Cyber Security Order 706 SDT scope, process and roles. Mr. Taylor noted that the 24-member Drafting Team will be responsible for: producing technically sound and complete standard(s) that meets stakeholder and regulatory approval; developing a realistic implementation plan; and preserving the open ANSI process. The Team discussed general comments on the scope, communication networks, serial communications, what should be included in critical assets, comparing NIST and CIP Standards, glossary definitions, bulk power system vs. bulk electric system, responsibility for standards and NERC Standards Development.

Mr. Taylor noted the 24 members of the Team appointed by the Standards Committee will be led by the Chair, Jeri Domingo-Brewer and the Vice Chair, Kevin Perry, who were appointed by the Standards Committee. NERC is committed to providing considerable NERC staff support and expertise as represented by those attending this organizational meeting and by neutral facilitation being provided by a team from Florida State University's FCRC-Consensus Solutions Center.

Bob Jones, with the FCRC Consensus Solutions facilitation team, provided an overview of how consensus could be defined and used by the drafting team as well as meeting ground-rules. He suggested that the Team

agree to the ground-rules and review the consensus process again at the next meeting with an eye towards adopting a procedure going forward.

David Taylor and Gerry Adamski noted that NERC will be developing, in consultation with the Team, a communications effort to the industry to explain what is going on in standards development process so that the industry has a heads up and does not have to digest the entire standards revision in a short period just prior to balloting. NERC would like to see the SDT complete its work within an 18 to 24 month time frame. An FAQ document may be developed by the SDT.

Members discussed who they are serving, i.e. who is the beneficiary, not who does the standards apply to in this process? Is the Congress, the FERC, the auditor, and/or the asset owner? One member suggested the SDT is serving North American society as a whole in working to protect critical infrastructure. The facilitator suggested bringing this back at the next meeting as the SDT reviews, refines and adopts a purpose statement.

The Chair noted that the FERC Order 706 directs NERC to consider the NIST framework. Keith Stouffer, team member and NIST employee, presented an introduction of the NIST approach to standards development to the Team. Stuart Katzke presented on the NIST framework and approach. Marshall Abrams presented a comparison of the NIST and NERC CIP Standards.

Prior to the meeting Scott Mix, Manager of Situation Awareness & Infrastructure Security at NERC, reviewed the FERC Order 706 and created and presented a straw man red-lined version of the CIP standards as an Approach to Phase I issues at the meeting. The facilitator then suggested the Team use the acceptability ranking tool to both test support and focus discussion on a threshold question of whether to proceed with a single phase or more than one phase. The Team ranked and agreed on the following project roadmap proposition: The SDT should proceed with an approach with two or more phases and products for ballot body consideration.

The SDT reviewed and agreed to apply the following draft criteria for consideration of issues to address in Phase-1:

- It represents an "Editorial" item
- It is a must-do item per Order 706 to meet the July 1, 2009 time frame
- It will not preclude the Team changing standards language in Phase 2

The Chair and Vice Chair suggested that the Team review and offer suggestions and concerns with the "straw man" phase 1 proposal that Scott Mix had put together as a "redline" draft of the CIP 002-009 standards in response to FERC Order 706. During the course of the Team's Tuesday afternoon's review of the redline, changes were made to the redline draft. The revised redline draft from Tuesday was then reviewed by the Team and ranked for acceptability and further refined on Wednesday morning. Below is the final draft of the changes in CIP-002-009:

CIP 002 – CRITICAL CYBER ASSET IDENTIFICATION

CIP-002 DRAFT REDLINE LANGUAGE AS OF END OF MEETING, 10-8-08

A1. Title: Cyber Security — Critical Cyber Asset Identification
A2. Number: CIP-002-~~1~~2
A3. Purpose *(2nd paragraph)*
These standards recognize the differing roles of each entity in the operation of the Bulk Electric System, the criticality and vulnerability of the assets needed to manage Bulk Electric System reliability, and the risks to which they are exposed. ~~Responsible Entities should interpret and apply Standards CIP-002 through CIP-009 using reasonable business judgment.~~
A4. Applicability:
Add: 4.1.12 Regional Entities.
A5. Effective Date: ~~June 1, 2006~~

B. Requirements
R4. Annual Approval — A senior manager or delegate(s) shall approve annually the risk-based assessment methodology, the list of Critical Assets and the list of Critical Cyber Assets. Based on Requirements R1, R2, and R3 the Responsible Entity may determine that it has no Critical Assets or Critical Cyber Assets. The Responsible Entity shall keep a signed and dated record of the senior manager or delegate(s)'s approval of the the risk-based assessment methodology, the list of Critical Assets and the list of Critical Cyber Assets (even if such lists are null.)

CIP 003 — CYBER SECURITY — SECURITY MANAGEMENT CONTROLS

CIP-003 DRAFT REDLINE LANGUAGE AS OF END OF MEETING, 10-8-08

A1. Title: Cyber Security — Security Management Controls
A2. Number: CIP-003-~~1~~2
A3. Purpose *(2nd paragraph)*
Standard CIP-003 requires that Responsible Entities have minimum security management controls in place to protect Critical Cyber Assets. Standard CIP-003 should be read as part of a group of standards numbered Standards CIP-002 through CIP-009. ~~Responsible Entities should interpret and apply Standards CIP-002 through CIP-009 using reasonable business judgment.~~
A4. Applicability:
Add: 4.1.12 Regional Entities.
A5. Effective Date: ~~June 1, 2006~~

B. Requirements
R2. Leadership — The Responsible Entity shall assign a senior manager with overall responsibility and authority for leading and managing the entity's implementation of, and adherence to, Standards CIP-002 through CIP-009.
R2. 3Where allowed by Standards CIP-002 through CIP-009, the senior manager may delegate authority for specific actions to a named delegate. These delegations must be documented in the same manner as R2.1 and R2.2, and approved by the senior manager.

R2.~~3~~ 4. The senior manager or delegate(s), shall authorize and document any exception from the requirements of the cyber security policy.

CIP 004 – CYBER SECURITY — PERSONNEL & TRAINING

CIP-004 DRAFT REDLINE LANGUAGE AS OF END OF MEETING, 10-8-08

A1. Title: Cyber Security — Cyber Security — Personnel & Training
A2. Number: CIP-004-~~1~~2
A3. Purpose:
Standard CIP-004 requires that personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets, including contractors and service vendors, have an appropriate level of personnel risk assessment, training, and security awareness. Standard CIP-004 should be read as part of a group of standards numbered Standards CIP-002 through CIP-009. ~~Responsible Entities should interpret and apply Standards CIP-002 through CIP-009 using reasonable business judgment~~.
A4. Applicability:
Add: 4.1.12 Regional Entities.
A5. Effective Date: ~~June 1, 2006~~

B. Requirements
R1. Awareness — The Responsible Entity shall establish, maintain, and document and implement a security awareness program to ensure personnel having authorized cyber or authorized unescorted physical access to critical cyber security assets receive on-going reinforcement in sound security practices…
R2. Training — The Responsible Entity shall establish, maintain, and document and implement an annual cyber security training program for personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets, and review the program annually and update as necessary.
R2.1. This program will ensure that all personnel having such access to Critical Cyber Assets, including contractors and service vendors, are trained prior to their being granted such access. ~~within ninety calendar days of such authorization.~~
R3. Personnel Risk Assessment —The Responsible Entity shall have a documented personnel risk assessment program, in accordance with federal, state, provincial, and local laws, and subject to existing collective bargaining unit agreements, for personnel having authorized cyber or authorized unescorted physical access. A personnel risk assessment shall be conducted pursuant to that program prior to ~~within thirty days of~~ such personnel being granted such access.

CIP 005 – ELECTRONIC SECURITY PERIMETER(S)

CIP-005 DRAFT REDLINE LANGUAGE AS OF END OF MEETING, 10-8-08

A1. Title: Cyber Security — Electronic Security Perimeter(s)
A2. Number: CIP-005-~~1~~2
A3. Purpose:
Standard CIP-005 requires the identification and protection of the Electronic Security Perimeter(s) inside which all Critical Cyber Assets reside, as well as all access points on the perimeter. Standard CIP-005 should be read as part of a group of standards numbered Standards CIP-002 through CIP-009.~~Responsible Entities should interpret and apply Standards CIP-002 through CIP-009 using reasonable business judgment~~.
A4. Applicability:
Add: 4.1.12 Regional Entities.

A5. Effective Date: ~~June 1, 2006~~

B. Requirements

R1.5. Cyber Assets used in the access control and monitoring of the Electronic Security Perimeter(s) shall be afforded the protective measures as a specified in Standard CIP- 003, Standard CIP-004 Requirement R3, Standard CIP-005 Requirements R2 and R3, Standard CIP-006 Requirements R2 and R3, Standard CIP-007, Requirements R1 and R3 through R9, Standard CIP-008, and Standard CIP-009. *(Staff will correct the citations)*

R2.3. The Responsible Entity shall maintain and implement a procedure for securing dial-up access to the Electronic Security Perimeter(s).

CIP 006 – PHYSICAL SECURITY OF CRITICAL CYBER ASSETS

CIP-006 DRAFT REDLINE LANGUAGE AS OF END OF MEETING, 10-8-08

A1. Title: Cyber Security — Physical Security of Critical Cyber Assets
A2. Number: CIP-006-~~1~~2
A3. Purpose:
Standard CIP-006 is intended to ensure the implementation of a physical security program for the protection of Critical Cyber Assets. Standard CIP-006 should be read as part of a group of standards numbered Standards CIP-002 through CIP-009. ~~Responsible Entities should apply Standards CIP-002 through CIP-009 using reasonable business judgment.~~
A4. Applicability:
Add: 4.1.12 Regional Entities.
A5. Effective Date: ~~June 1, 2006~~

B. Requirements

R1. Physical Security Plan — The Responsible Entity shall create ~~and~~ maintain and implement a physical security plan, approved by the ~~a~~ senior manager or delegate(s) that shall address, at a minimum, the following:
R1.2. Processes to identify all access points through each Physical Security Perimeter and implement measures to control entry at those access points.
R1.4. Procedures for and the implementation of the appropriate use of physical access controls as described in Requirement R3 including visitor pass management, response to loss, and prohibition of inappropriate use of physical access controls.
R1.6. Procedures for and implementation of escorted access within the physical security perimeter of personnel not authorized for unescorted access.
R1.7. Process for updating the physical security plan within ~~ninety~~ thirty calendar days of implementation of any physical security system redesign or reconfiguration, including, but not limited to, addition or removal of access points through the physical security perimeter, physical access controls, monitoring controls, or logging controls.
R1.8. Cyber Assets used in the access control and monitoring of the Physical Security Perimeter(s) shall be afforded the protective measures specified in Standard CIP-003, Standard CIP-004 Requirement R3, Standard CIP-005 Requirements R2 and R3, Standard CIP-006 Requirement Standard CIP-009. *(Staff will correct the citations)*

CIP 007 SYSTEMS SECURITY MANAGEMENT

CIP-007 DRAFT REDLINE LANGUAGE AS OF END OF MEETING, 10-8-08

A1. Title: Cyber Security — Systems Security Management
A2. Number: CIP-007-~~1~~2
A3. Purpose:
Standard CIP-007 requires Responsible Entities to define methods, processes, and procedures for securing those systems determined to be Critical Cyber Assets, as well as the non-critical Cyber Assets within the Electronic Security Perimeter(s). Standard CIP-007 should be read as part of a group of standards numbered Standards CIP-002 through CIP-009. ~~Responsible Entities should apply Standards CIP-002 through CIP-009 using reasonable business judgment.~~
A4. Applicability:
Add: 4.1.12 Regional Entities.
A5. Effective Date: ~~June 1, 2006~~

B. Requirements
R2. Ports and Services — The Responsible Entity shall establish and document and implement a process to ensure that only those ports and services required for normal and emergency operations are enabled.
R3. Security Patch Management — The Responsible Entity, either separately or as a component of the documented configuration management process specified in CIP-003 Requirement R6, shall establish, ~~and~~ document and implement a security patch management program for tracking, evaluating, testing, and installing applicable cyber security software patches…
R4.1. The Responsible Entity shall document and implement anti-virus and malware prevention tools. In the case where anti-virus software and malware prevention tools are not installed, the Responsible Entity shall document compensating measure(s) applied to mitigate risk exposure. ~~or an acceptance of risk~~.
R7. Disposal or Redeployment — The Responsible Entity shall establish and implement formal methods, processes, and procedures for disposal or redeployment of Cyber Assets within the Electronic Security Perimeter(s) as identified and documented in Standard CIP-005.
R9. Documentation Review and Maintenance — The Responsible Entity shall review and update the documentation specified in Standard CIP-007 at least annually. Changes resulting from modifications to the systems or controls shall be documented within ~~ninety~~ thirty calendar days of the change being completed.

CIP 008 INCIDENT RESPONSE & REPORTING

CIP-008 DRAFT REDLINE LANGUAGE AS OF END OF MEETING, 10-8-08

A1. Title: Cyber Security — Incident Reporting and Response Planning
A2. Number: CIP-008-~~1~~2
A3. Purpose:
Standard CIP-008 ensures the identification, classification, response, and reporting of Cyber Security Incidents related to Critical Cyber Assets. Standard CIP-008 should be read as part of a group of standards numbered Standards CIP-002 through CIP-009. ~~Responsible Entities should apply Standards CIP-002 through CIP-009 using reasonable business judgment~~
A4. Applicability:
Add: 4.1.12 Regional Entities.
A5. Effective Date: ~~June 1, 2006~~

B. Requirements
R1. Cyber Security Incident Response Plan — The Responsible Entity shall develop and maintain a Cyber Security Incident response plan and implement the plan in response to Cyber Security Incidents. The Cyber Security Incident Response plan shall address, at a minimum…
R1.4. Process for updating the Cyber Security Incident response plan within ~~ninety~~ thirty calendar days of any changes.
R1.6. Process for ensuring the Cyber Security Incident response plan is tested at least annually. A test of the incident response plan can range from a paper drill, to a full operational exercise, to the response to an actual incident. Testing the Cyber Security Incident response plan does not require removing a component or system from service during the test.

CIP 009 RECOVERY PLANS FOR CRITICAL CYBER ASSETS

CIP-009 DRAFT REDLINE LANGUAGE AS OF END OF MEETING, 10-8-08

A1. Title: Cyber Security — Recovery Plans for Critical Cyber Assets
A2. Number: CIP-009-~~1~~2
A3. Purpose:
Standard CIP-009 ensures that recovery plan(s) are put in place for Critical Cyber Assets and that these plans follow established business continuity and disaster recovery techniques and practices. Standard CIP-009 should be read as part of a group of standards numbered Standards CIP-002 through CIP-009. ~~Responsible Entities should apply Standards CIP-002 through CIP-009 using reasonable business judgment~~.
A4. Applicability:
Add: 4.1.12 Regional Entities.
A5. Effective Date: ~~June 1, 2006~~

B. Requirements
R3. Change Control — Recovery plan(s) shall be updated to reflect any changes or lessons learned as a result of an exercise or the recovery from an actual incident. Updates shall be communicated to personnel responsible for the activation and implementation of the recovery plan(s) within ~~ninety~~ thirty calendar days of the change being completed.

On Wednesday morning, the Team engaged in a brief exercise to highlight the members' individual preferences for problem solving and decision making. Finally the Team reviewed and agreed to the Phase 1 meeting schedule (both in-person and Webex conference call drafting meetings) and drafting assignments. At the conclusion of the meeting, the Team offered an evaluation of the process including what worked and what could be improved. *The meeting adjourned at Noon on Wednesday October 8, 2008*.

Cyber Security Order 706 Standard Drafting Team

DRAFT ORGANIZATIONAL MEETING SUMMARY

A. INTRODUCTIONS, AGENDA REVIEW AND WELCOMING REMARKS

The Chair, and Vice Chair welcomed the members and asked NERC staff Harry Tom to conduct a roll call of members and participants in the room and on the conference call *(See appendix #3*). They then reviewed with the Team and participants the proposed meeting agenda *(See appendix #1*).

Team Members introduced themselves highlighting a broad spectrum of expertise and industry and governmental perspectives and a shared expectation that they would keep the needs of the industry in mind, but do the right thing. Several noted the importance of engaging and involving Canada in the standards development process. Others pointed to the fact the industry must successfully respond to the cyber security challenges facing the bulk electric system or risk a regulatory response and imposed "solution." In addition, several Team members noted their participation on the first CIP drafting team.

Following the Team and staff introductions, Michael Assante, NERC's Chief Security Officer, offered welcoming remarks and opening comments for the Team's consideration. He noted that he joined NERC as the new Chief Security Officer in September, 2008, moving from Idaho and the Department of Energy's Idaho National Labs (INL) in the fields of security and infrastructure protection to Princeton. He noted prior to his work with INL he served as Chief Security Officer at American Electric Power. Overseeing NERC's plan, at the Electric Reliability Organization, to improve response to cyber and critical infrastructure protection, he noted he will lead the effort in establishing a new core Critical Infrastructure Program at NERC including the critical task of related standards development and compliance.

He noted that this was an unusual standards development process surrounded by an increased level of attention and some sense of urgency. He urged the Team to focus on their standards development task and to take the time necessary to build consensus and answer the critical challenge of coming up with practical solutions that address the directives of FERC and the concerns of the industry. He noted that the Team will not be following someone's model, since no sector has taken this standards issue on. The Team needs to focus on producing just and reasonable standards that are not unduly discriminatory or preferential and that are in the public interest. NERC is providing its staff expertise and facilitation assistance to do everything it can to make this effort a success.

Mr. Assante also noted the context of President Rick Sergel's recent industry stakeholder letter and congressional testimony highlighting the industry's commitment to making a priority of enhancing security leadership and situational awareness of the urgency of the threat while improving the industry response to cyber security and critical infrastructure protection concerns for the bulk power system in North America. The leaders in the sector believe we have a great "culture of compliance" and that the ERO is about achieving real security. He noted that cyber security is a fast evolving area in terms of tools and approaches where there needs to be a balancing of the security value with establishing good measurable standards in a dynamic system. The experience with the Maritime

Security Act of 2002 highlights what lack of flexibility can produce. NERC's hope is to strengthen the regime to protect assets and demonstrate a confidence and willingness to do this right.

Mr. Assante suggested the Team should consider as part of its scope:

- The merits of blackout report recommendations;
- "Must do's" in the short term;
- Eliminate reasonable business judgment in the standards
- How to address acceptance of risk exceptions and accountability.
- Develop specific conditions that a reasonable entity must satisfy to invoke the "technical feasibility" exception;
- Data as a critical cyber asset and help to defining critical assets- and what external review and procedures may be involved and who should be involved in that process;
- Application of a measurable "defense in depth" to create an electronic security perimeter. Different definitions by different world- network view of the world vs. operations.
- What strong controls are needed and how much change triggers an "active vulnerability assessment" (change controls).
- What is a representative system that will allow you to say the testing is enough.
- Security standards and operations realities different, E.g. "resilience," efficiency is the evil to resilience? Philosophically how to protect assets and how to best operate to get to reliability.
- Timetable- One hard date in FERC Order 706 is to remove "using reasonable business judgment" before the compliance audits commence in July, 2009.
- Satisfy what needs to be done in the short term while taking the longer view in the standards development. Are there approaches that might allow addressing important issues sooner?

Finally, Mr. Assante noted that everything the Team will do will be part of an open process guided by the ANSI framework and procedures and, "If we get this right, we can provide a model for the industry and that others can utilize."

B. REVIEW OF ANTITRUST GUIDELINES

David Taylor, NERC Manager of Standards Development, reviewed with the Team the need to comply with NERC's Antitrust Guidelines (See, Appendix #3). He urged the Team and other participants in the process to carefully review these as they would cover all participants and observers. He urged all to avoid behaviors or appearance that would be anti-competitive in nature.

C. SDT PROJECT PROCESS, SCOPE, ROLES AND CONSENSUS GUIDELINES

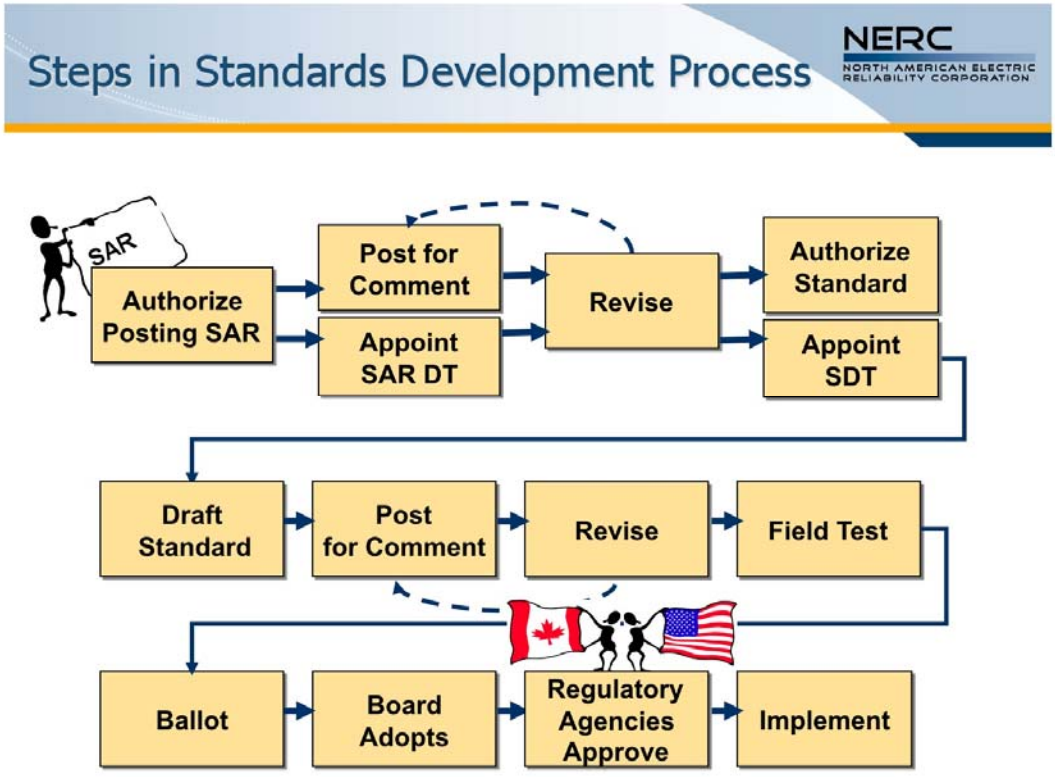
David Taylor, Manager of Standards Development at NERC, provided an overview of the SDT Project scope, process and roles. (See, power point presentation at: http://www.nerc.com/filez/standards/Project_2008-06_Cyber_Security.html

1. Standards Development Process and SAR Scope

Mr. Taylor reviewed with the Team the development and adoption of the Standard Authorization Request (SAR), Revisions to Critical Infrastructure Protection Standards (revisions to CIP-002 through CIP-009, June 9, 2008) (See, http://www.nerc.com/docs/standards/sar/SAR_Modify_CIP_Stds_D2_clean_07Jul08.pdf . He noted that the Standards Committee appointed the Standards Drafting Team with an eye towards member expertise and representation of both geographic and industry segment perspectives. The 24-member Drafting Team will be responsible for:

- Producing technically sound and complete standard(s) that meets stakeholder and regulatory approval;
- Producing a realistic implementation plan; and
- Preserving the open ANSI process.

He described the potential phases of a standards development process featured in the graphic below:



Mr. Taylor noted that if there is anything that needs to be changed in the standard, the group should raise the issue. Historically SARs have been narrowly focused. He noted that Volume #1 of Standards Development Plan outlines that the scope of the standards

development process and directs teams to effectively deal with standards overall to produce an effective standard. Taylor expects the majority of the time to be spent on Requirements and on accompanying Measures. In the past the requirements may not have been written to provide clarity. David Taylor and Maureen Long of NERC will review the Team's products for completeness and clarity prior to posting. If the requirements are not clear, modification will be required. All requirements must be measurable. If the requirement cannot be clearly measured, then the drafting team will be asked to re-write the requirement and measure. The measures must be precise and understandable by both the entities and the auditors.

The drafting team should address all the issues identified in the Issues Database prior to posting and the standard should meet NERC benchmarks for reliability standards. The expectation is that each of the existing requirements and modifications and an implementation plan should be addressed and the drafting team will be expected to respond to all comments. He noted that the Team will need to decide fairly early on if they are going to address something with a revision to the standard or address a FERC directive via external guidance documents.

Mr. Taylor addressed the following SDT Scope items:

Balloting and Implementation
- What is directed in Order 706
- There is a spreadsheet that lists the items in Order 706 to be addressed by the drafting team.
- Determine the optimal implementation plan

Clarify Existing Requirements
- Consider the need for different requirements for different environments, i.e., control centers, substations, generation, etc.

Other items including interpretations.
- The team may believe it should consider clarifying interpretations, etc.
- E.g., Within an ESP, the wiring over which data flows should be protected.
- E.g., Application of CIP to Nuclear

Industry education
- FAQ document revision/replacement
- Development of guideline documents such as those for extended LAN's over multiple geographically dispersed locations

Finally, he noted the following products that must accompany a standard change and are used by the NERC compliance staff:

- A standards requirements document (saying what the entity shall do but not how they do it).
- An SDT Implementation Plan for the Standard(s)
- A Comment Form which presents an opportunity for the Team to tell the "story" behind the proposed standard and asks some very pointed questions for industry to respond to in providing input.

- A document describing Violation Risk Factors –focusing on Severity of impact and are used by auditors to determine, along with other mitigating factors, the initial sanction "price point."
- A document describing the Violation Severity Level — i.e. how badly off from the compliance mark was the entity being audited? This will expand on the measure. Note that VSLs were not a part of the original CIP standard development, instead there was a separate team working on initial VSL. This team will revise VSLs as part of its process.

Finally, Mr. Taylor noted the following reference documents that had been sent in advance to the Team:

- Reliability Standards Development Plan — Volume I
- Reliability Standards Development Procedure
- Standard Drafting Team Guidelines — the SDT bible
- Pages 7–11 of the SAR gives a lot of really good information.

Team Member Comments and Questions on SAR Scope

- **General Comments on Scope**

- Extended WAN — consider Ethernet Over SONET.
- Consider the impact of Smart Grid (AMI, etc.).
- Try to stand back and look at the bigger picture.
- The word "etc." in the requirement to consider other information sources is believed to give the SDT the latitude to go wherever it needs to.
- Need to be more explicit where the ESP begins and ends.
- Need to be cognizant of the use of high speed communication and cost models.
- Need to look at CIP-002, including the RAWG guideline and the NIST framework. Does not mean we throw out the CIP standards and wholesale replace them with the NIST standards.
- Perhaps there is a minimum set of requirements that apply to all cyber assets and an elevated set of requirements that apply to critical cyber assets. The NIST/FISMA risk framework gives you this latitude.
- The fear is the threat of financial sanctions. That is the big roadblock against moving away from the existing cherry-pick approach.
- The RAWG guideline looks at the problem from a functional perspective (generation, transmission, systems, and special controls). The CIP-002 as it exists today does not organize the same way.
- Verizon data breach study — victims are not taking upstream/downstream connections seriously. No longer a predominately internal threat.
- Is everything fair game as far as the SAR is concerned? Answer: There is an item in the SAR that provides freedom to include other related items as appropriate.

- Are **Communication networks** today out of scope in terms of the SAR? Answer: If the communications are disrupted via the end points, such as the meters, the

question of who is responsible is not clear under today's standards. The communications provider is not responsible. Issues similar to this should be within the scope under "other items". However, the standards drafting team will probably not have authority to decide this issue.

- **Serial Communications**: a strategy of moving IP based systems away from IP communications and back to serial communications by some industry participants may not be a good idea. FERC intends to address this issue in the future.
- **What should be included in Critical Asset?** Could the definition of Critical Asset be expanded to cover a broader set of reliability standards? The answer is yes, it is within scope of the SDT. RAWG is leading the process of developing a guideline for Critical Asset identification in support of the existing CIP standard. Jay Cribb, chair of the RAWG and member of this Team can be a conduit between this drafting team and the work of the RAWG.
- **NIST and CIP Standards.** Federal strategy is to try to adapt existing NIST standards to new environments. For example, applicability of SP 800-53 to control systems. Very difficult to apply. Added additional information to a good number of 800-53 requirements to specifically apply to control systems (Became SP 800-53, Rev 2). We can learn from the NIST experience. NIST will provide as little or as much detail and assistance as the SDT wants. NIST 800-39 provides some directives. NIST 800-39 should be looked at very closely because we have been directed to do so and because it makes sense when studied. We may not be able to provide cyber security protection of the systems that support the electric grid using the Critical Asset directives contained in CIP 002. The drafting team should be free to replace CIP 002 with the NIST framework if they determine this is the right course of action. NIST 800-39 may provide a framework that can be used over time. Based on risk, there are different levels of security that may be applied to different assets at different levels of risk.
- **Glossary Definitions.** Definitions that are global to NERC, how does the drafting team work with them? Answer: NERC Glossary terms used in standards are capitalized. All glossary terms must be universal and not specific only to the cyber security context. Changing the way a word is defined in the NERC glossary could have a ripple effect throughout other standards where the word is referenced. If it is in the NERC glossary, that is the definition the drafting team should use or propose a change to the glossary. The drafting team may want to propose that new definitions are added to the glossary.
- **Bulk power system vs. bulk electric system.** The terms "bulk power system" and "bulk electric system" may be contingent upon the regional definitions. What term will the Team use? Answer: BES will be used until further direction is provided by FERC. BPS is more expansive than BES, but FERC did not probably expect imminent compliance across industry. FERC expects eventually that all the NERC standards will apply to the BPS and not just to the BES.
- **Responsibility for Standards.** Who is responsible for published standards? Answer: NERC is responsible in conjunction with the industry for ERO standards. NIST is responsible for publishing their standards.

- **NERC Standard Development**. Will or can we limit the number of revisions? Answer: Based on experiences to date, the Team should expect 2 or 3 drafts in responding to comments. The plan is have a good idea of what the industry wants prior to submitting the standards for ballot. Can the standards be separated or do they need to be balloted as a group? Answer: This is part of the road map for development. This question will be decided over the next couple of days. The ballot body is not typically expert in cyber security matters and companies will turn to their experts for guidance. Is this process of 18 to 24 months soon enough to satisfy the regulators? Answer: NERC's responsibility is to assist the group. There is urgency but CSO's role is to assure reasonable expectations. The Team should have time to 'get it right.'

2. Roles in the SDT Process

Mr. Taylor noted the 24 members of the Team appointed by the Standards Committee will be led by the Chair, Jeri Domingo-Brewer and the Vice Chair, Kevin Perry, who were appointed by the Standards Committee. NERC is committed to providing considerable NERC staff support and expertise as represented by those attending this organizational meeting and by neutral facilitation being provided by a team from Florida State University's FCRC-Consensus Solutions Center.

3. Proposed SDT Consensus Guidelines and Meeting Ground Rules

Bob Jones, with the FCRC Consensus Solutions facilitation team, provided an overview of how consensus could be defined and used by the drafting team *(See Appendix #6)*. He noted that consensus can be understood as having three meanings in a group process: it is an attitude of each of the team members, it is an outcome or decision rule for the team, and it is a structured problem solving process. He suggested that the Team has some flexibility to define what a 'consensus' decision should mean for the Team's process. He noted that among the ballot body, a standard requires at least a 2/3 majority of all of the industry segments to be adopted. The Team may want to establish a higher supermajority for agreement (perhaps +75%) to assure 2/3 acceptance of the ballot body. He suggested that this could serve as a default standard and that the process would be designed to seek 100% acceptance of the Team. He suggested that the Team review this again at the next meeting with an eye towards adopting a procedure going forward.

Mr. Jones proposed a set of ground rules for the meeting. *(See, Appendix #6)*.

Team Comments on Ground rules

- Perhaps some additional phone protocols
- Say your name at the start if you are on the phone — "comment on the phone" with name to get in the queue to speak on an issue
- Check with team members on the phone to include their acceptability ranking as needed
- In past group this large need to clearly state what we are trying to get consensus on to aid in staying on issue and avoid drift

4. Expectations of Drafting Team

David Taylor and Gerry Adamski noted that NERC will be developing, in consultation with the Team, a communications effort to the industry to explain what is going on in standards development process so that the industry has a heads up and does not have to digest the entire standards revision in a short period just prior to balloting. NERC would like to see the SDT complete its work within an 18 to 24 month time frame. An FAQ document may be developed by the SDT.

Members discussed who they are serving, i.e. who is the beneficiary, not who do the standards apply to in this process? Is the Congress, the FERC, the auditor, and/or the asset owner? One member suggested the SDT is serving North American society as a whole in working to protect critical infrastructure. The facilitator suggested bringing this back at the next meeting as the SDT reviews, refines and adopts a purpose statement.

D. REVIEWING THE NIST FRAMEWORK AND COMPARISON WITH THE NERC CIP STANDARDS (002-009)

The Chair noted that the FERC Order 706 directs NERC to consider the NIST framework.

1. NIST Framework

Keith Stouffer, team member and NIST employee, presented an introduction of the NIST approach to standards development to the Team. He noted that he does not believe a wholesale swap out of NIST for the CIP is prudent, but he believes there is quite a bit to be gained for the SDT in reviewing the NIST approach. He noted that the NIST strategy has been to look to see if they can add additional guidance to their framework to support applications such as control systems environment. The first thing they looked at was 800-53 requirements by bringing stakeholders together to determine what concerns exist. They determined 800-53 as written would not apply well to control systems so they created a Revision #2 to 800-53 for entities which operate control systems and must comply with NIST requirements. Keith noted that NIST is ready to help as much or as little as the drafting team wants. NIST provides an alternative way of looking at the standards.

Keith Stouffer then reviewed a presentation that he gave to the NERC Standards Committee. His power point presentation is available for review at: http://www.nerc.com/filez/standards/Project_2008-06_Cyber_Security.html. Key points in Keith's presentation included:

- NIST keeps measurement standards, but they also create principle-based standards.
- 800 series contains information systems guidelines. Auditing done by GAO. There are about 115 of the 800 series documents.
- FIPS — standards approved by the Secretary of Commerce.

- NIST 800 documents go through a 3 stage public vetting process, but do not require Secretary of Commerce's approval.
- Connection between FIPS and 800 documents includes a reference in FIPS to the 800 series documents. Therefore a change in a reference in FIPS to an 800 series document does not require Secretary of Commerce's approval.
- NIST approach to Standards Development in order of priority
- Seek commercial sector involvement and attempt to adapt an existing document.
- Review other existing standards to see if one of those can be adopted.
- Create a new document.
- 800-53 is the document used for securing Federal information systems.
- Over 800 comments received on the initial public draft
- In response NIST streamlined the controls
- Revised in 2006 and again to revise for control systems in late 2007.
- NIST brought in industry companies covered by 800-53 and determined why implementing the controls created problems for the companies covered by the document.
- There are 3 levels assessed for each control. For example, for a system categorized as low the particular control may not apply or only parts of the control may apply.
- 800-53 cannot be used for both general information systems and control systems.
- The following framework allows the organization to tailor the controls to their systems:
  - Low Impact: Selection of a subset of security controls – Non hazardous materials
  - Moderate builds a low baseline. Selection of subset of control from the master catalog – Some hazardous material & some proprietary information
  - High Impact: Highest level - Protect human life
- Federal Government approach
- Use the existing NIST risk framework
- Make modifications
- Apply to control systems
- 800-82 provides guidance on how to implement 800-53.
- Final public draft released in September of 2008 with 60 days for comments
- Used in the private sector for control systems

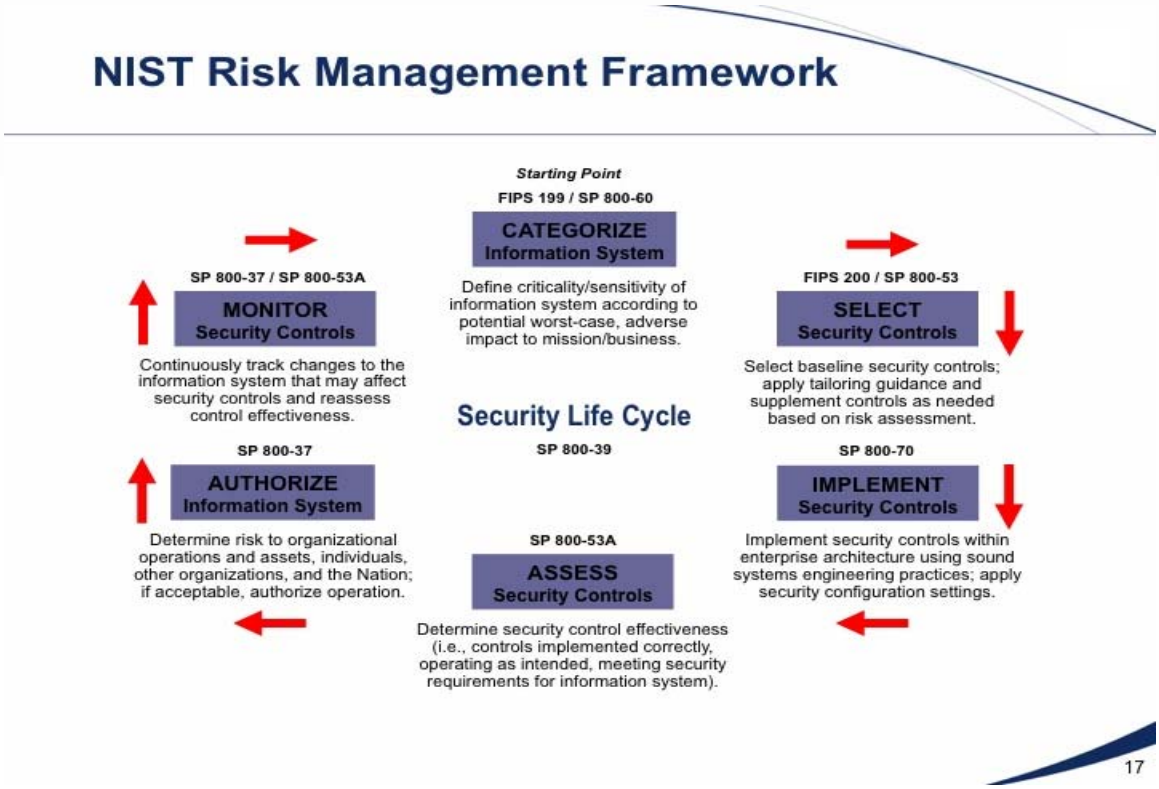
Stuart Katzke presented on the NIST framework and approach, (see, http://www.nerc.com/filez/standards/Project_2008-06_Cyber_Security.html) including the following key points:

- Control mapping was the easy part. Harder part was looking at model and the underlying model for CIPs.
- NIST is a "Plug and play" framework-
- FIPS and 800 documents — are security standards and guidelines.
- Tasked under FISMA to do 3 things:
  - Categorization scheme for info and info systems;
  - Guidelines for categorization;
  - Create minimum standards for categories.
- 3 buckets- low, mod, high based on worst case impacts and decide which bucket.
- Minimums imply more is required. Not a good 1 size fits all solution.

- Put flexibility in standard by fixing the standard and have the guideline allow you to tailor it.
- Look for ways to compensate.
- Minimum control smacks of a compliance/regulatory view. Inclined toward understand and accept risks.
- When system is ready to go- controls will be in place and operating. This goes into authorization to operate (accreditation) decision.
- Certification- assessment of security controls
- Problem- evolved into a paper work exercise — boon for consultants.
- Accreditation/certification woven into the process vs. an end checkpoint.

Team and Participant Comments on the Presentations

- NIST approach includes understanding risks under assessment and the intent of the controls. If the controls cannot be implemented, the users must understand the intent of what the control is trying to accomplish and implement controls which compensate for the intent of the control which will not be implemented.
- NIST approach includes continually assessing level of security. Therefore, following the NIST model correctly will result in being in compliance.
- The framework of NIST occurs within the information system development lifecycle. Today's CIP standards apply to Critical Assets, which may include control centers, generation plants, and substations.
- 800-39 presents a broader view for inter-connected information systems and external entities.
- 800-53 sets standards but doesn't tell how.
- Reviewed all controls. Provide guidance re problems in applying controls to this environment.
- 17 control families; 171 controls (requirements).
- Control enhancement to original control. Low/Mod/High. Based on level of impacts if system is compromised. Additional rigor as you go up to high.
- 800-53 took about 1 year to develop draft.



- NIST Risk Management Framework/Security Lifecycle
  - FIPS 199/800-60 — Categorize information Systems (low, medium, high)
  - Level of rigor is based on the categorization
  - FIPS 200/800-53 — Select Security controls
  - SP 800-70 — Implement Security controls
  - SP 800-53A — Assess Security Controls
  - Security Assessment plan is required & independent assessor is required for moderate and high impact systems
  - SP 800-37 — Authorize Information System
  - SP 800-37/SP 800-53A — Monitor Security State
- NIST does not perform the assessments or audits. NIST gets feedback from the GAO surrounding changes that may be required to NIST standards.
  Merging systems together- depends on circumstances.
- Assess controls when a security event occurs.
- How does system hold up to scrutiny — NIST relatively new.
- Look at control sets following events —
- Would the BES need an organization to manage family of controls, to assess etc.?
- GAO reports on incidents.
- Consider Total cost of ownership — with a life cycle framework approach. Need to think through the care and feeding.

- Assessment based upon what the org decided are its goals in an area. Measurable and $$. Tendency to shoot low. What are they assessed against for standards. How to encourage how to set their goals high.
- Assessment against controls vs. goals? Assess security controls- audit focusing on $$. Adopt lower level of controls.
- Adequately secure vs. meeting controls.

Team and Participant Comments on the NIST Framework

- For control system how are federal agencies categorizing systems- which baselines using? FIPS 199.
- Assignment clause — organization defined list of inappropriate or unusual activities that are to result in alerts? The organization determines within the framework of control.
- "regularly reviews" -organization determines the frequency.
- CIP standards — for not keeping 1 document up to date is a potential violation that is not consequential to security. Evaluating the level of control vs. small pieces = violation.
- NOPR in 706- might provide too much angst.
- Compliance elements- onerous.
- "If it ain't written down, it didn't happen."- This captures the old view.
- If we go down more prescriptive route- have to clarify the costs of putting this in place. Intensive to implement controls.
- Tell me exactly what I have to do. Flexibility factor is providing
- Control and enhancements. Low mod high — lots of variation.
- Changes- didn't change any of the controls in 800-53. Instead provided additional guidance to 645 of 171 controls to address ICS (industrial control systems)
- Control systems- not all in BES context.
- DOD interested in this approach — now they use their own.
- 882 supplemental- security process controls — 800-53 revision 2 is requirement
- Security baselines- low, mod, high.
- 800-53- tailoring baseline security controls to fit needs.
- Industrial control systems security guide
- 800-82- Sept 08 final public draft. Out by end of the year.
- 90% of ICS are industry.
- ISA 99- Bryan Singer. ANSI — Industrial Automation and Control Equipment
- IEC 62443- Tom Phinney.
- Not just compliant – compliance with baseline does not equal security.
- Must define minimums.
- Life cycle management? Not a maturity element. Degrees of rigor come in depending on impact level.
- One large interconnected system- what is the system? Each separate or one?
- What is the info system (accreditation boundary- what you have control over)
- NIST Protecting info systems. CIP speaks to critical cyber assets and non-critical not necessarily systems. Apply all the CIPs.

- Framework- differences- NIST- system level approach requires high degree of system/state awareness of context of components. CIP – make judgment about critical assets and apply approach.
- Accreditation boundary — are we Industrial control systems or not?
- Draw boundary around set of components and consider as a holistic system.
- Evolved to enterprise wide view of activities. (mission, role, impacts on organizations and other depending on organization.
- Information system: accreditation boundary- components within- people, processes and technical- management operational and technical controls.
- "Common controls"-training, physical security) provided to system from external sources.
- NERC standards- cyber security not factored into overall trainers as a common control. Should be doing this going forward. Operators are first line of defense.
- Assignment of responsibility- asset/system owner. Where does responsibility lie that everyone getting access to critical asset is properly trained?
- Flexibility to flavor requirements specific to each environment within organization.
- CIP- accountable executive- responsibility assigned. It is there? Yes but not as prescriptive as NIST standards. Needs to be open enough, not too prescriptive. Split into different number because ANSI. Not being read as one standard.
- ESP boundary in CIPS vs. the NIST boundary and everything within.

2. Comparison of NIST and NERC Cyber Standards

Marshall Abrams presented a comparison of the NIST and NERC CIP Standards. (See, his PowerPoint presentation at: http://www.nerc.com/filez/standards/Project_2008-06_Cyber_Security.html

He noted both the similarities between CIP vs. NIST (e.g. concepts of internal/exterior boundaries, etc.) and the differences between CIP vs. NIST (e.g. NIST uses information system view rather than NERC Critical Asset/CCA view, NIST allows holistic defense in depth approach through system design, etc.) Other points included:

- Under CIP security requirements are applied to all components whether the components are capable of supporting the security requirements or not (i.e., legacy substation devices);
- Under CIP Treating boundary and contents separately (CIP 005 and 007) creates problems;
- Wireless is addressed in NIST but not in CIP.

Mr. Abrams handed out a NIST augmented CIP and NIST Example of Augmentation of CIP 005. See, http://www.nerc.com/filez/standards/Project_2008-06_Cyber_Security.html

Team Discussion of NIST compared with the NERC CIP:

- NIST staff performed the mapping of the CIP vs. the NIST standards to assist Federal entities which had to comply with both NIST and CIP.

- CIP 002-009 standards should be taken as a whole and that many of the concerns which have been raised can be answered in either one of the other CIP standards or in the CIP FAQ.
- The Chair and Vice Chair reminded the Team that they have an obligation to set aside partisan opinions of whether members support NIST or CIP but to do the right thing for enhancement of cyber security standards.
- A mapping of what is? Indicates controls or part of controls added CIP requirements.
- Gap assessment- e.g. Least Privilege- mapped to 007?
- Identification and authentication- not adequately address to CIP.
- Configuration management- adequate records/documentation, who can make change.
- Auditing and accountability- e.g. time stamps missing?
- Risk Assessment- R4 renamed- vulnerability assessment and testing.
- System and Communication protection
- Certification, accreditation.- CIP examining controls, managing as intended.
- Security assessment suggestions: security assessment requirement- Responsible entity
- This is not easy. It is on 007.
- Forced by ANSI process. All 1300 were one standard. Read as one standard 2-9.
- Are ANSI rules being cited correctly?
- Technical feasibility with an exception process.
- Suggest level of review- exception plan. Annual audit compliance.
- Physical security?
- CIP Standards- 002-009 should be read as one. It is stated in each in the purpose statement.
- What value might this add- square peg through round hole?
- Let's not spend our time defending the CIP standards.
- Size and risk aren't correlated in CIP?
- Restrict access- assess risk posture of business partners.
- Not try to defend but point out where it was taken care of in the standard.
- Lots of things we need to fix. Gives options to fix few things.
- Procedures written by each company is where NIST and CIP standards come together.
- E.g. "reference we are meeting NIST standard to meet CIP requirements."
- Look at comparison paper on NIST website- Marshall et al.
- Red guide- restricted distribution. Undergoing future review and modification.
- NIST standard has more specificity in all areas. What has to be done not how to do it.
- Team has an opportunity to do what is right. Re-write, incorporate as much or little of 800 framework. Set aside love of one or other. What do we need to do to achieve the goal. This should not be about pleasing auditor or pleasing FERC, but about improving security of the BES for benefit for North America.

E. REVIEW OF HOW TO STRUCTURE THE SDT PROJECT ROADMAP

1. Initial Overview of "Straw Man" Multi-Phased Approach

Prior to the meeting Scott Mix, Manager of Situation Awareness & Infrastructure Security at NERC, reviewed the FERC Order 706 and created and presented a straw man red-lined version of the CIP standards as an Approach to Phase I issues at the meeting. The facilitator then suggested the Team

use the acceptability ranking tool to both test support and focus discussion on a threshold question of whether to proceed with a single phase or more than one phase. The Team ranked and agreed on the following project roadmap proposition: The SDT should proceed with an approach with two or more phases and products for ballot body consideration. (*See, power point, "Cyber Security Standards: Development Proposal at)*. His key points included:

- Violation Severity Level process is beginning for all requirements
- The only date-certain in FERC Order 706 is for the required change is removal of " using reasonable business judgment" by end of June 2009.
- NERC is developing training for NERC regional compliance auditor staff on CIP
- Meeting frequency for the Team- may have to meet face to face every other week for 2 to 3 days
- Proposing 3 phases with doing the "easier" and "must do" work first:

  1. Low hanging fruit — high priority — Reasonable business judgment needs to be removed
  - Complete & to Commission in 6 months (March of 2009)
  - Mostly non-contentious issues
  - NER staff has a proposal of these items

  2. Moderate/Majority of issues
  - Complete and to the Commission 18 months following #1 (October of 2010)

  3. Large challenging, complex, controversial issues — Take a long time to get through
  - Following #2 above – exact timing depends on how many and how long
  - Extremely large and challenging issues.

- Guidelines need to be addressed. Guidelines are NOT standards and are NOT requirements. Cannot be sanctioned for not following a guideline. This drafting teams needs to determine whether a topic needs to be addressed in the standard or in a guideline. CIPC is ready to write guidelines. The Team needs to identify what needs to be done and whether or not CIPC needs to be the writer. About 25 guideline topics have been identified in the FERC Order 706. What can be started now because the subject requirement is not expected to change?
- Develop modification to standards language
- Develop Violation Risk Factor/Violation Severity Level
- Develop implementation timeline and effective date — Less complicated
- Industry review and comment
- Industry ballot
- BOT Approval
- Submit to FERC prior to spring of 2009 and prior to the beginning of CIP audits.

Scott then reviewed a red-lined straw man draft for the Team's consideration that included:

CIP 002 – CRITICAL CYBER ASSET IDENTIFICATION
Proposed language changes include:

- Language to address 706 concerns to remove 'reasonable business judgment."
- Add RE in addition to RRO.
- Newly identified Critical Assets was put into the parking lot.
- Annual approval by Sr. Manager of the Risk Based Assessment in addition to the CA list

CIP 003 – CYBER SECURITY — SECURITY MANAGEMENT CONTROLS

Proposed language changes include:

- Language to address 706 concerns to remove 'reasonable business judgment."
- Add RE in addition to RRO.
- Slight modification to the specifics requested for the designated senior manager

CIP 004 – CYBER SECURITY — PERSONNEL & TRAINING

Proposed language changes include:

- Language to address 706 concerns to remove 'reasonable business judgment."
- Add RE in addition to RRO.
- The individuals shall be trained prior to being granted access rather than within 90 days of access
- Individuals shall be background screened prior to being granted access rather than within 30 days of access

CIP 005 – ELECTRONIC SECURITY PERIMETER(S)

Proposed language changes include:

- Language to address 706 concerns to remove 'reasonable business judgment."
- Add RE in addition to RRO.
- Minor editorial changes only

CIP 006 – PHYSICAL SECURITY OF CRITICAL CYBER ASSETS

Proposed language changes include:

- Language to address 706 concerns to remove 'reasonable business judgment."
- Add RE in addition to RRO.
- Several items where the word 'implement' was added to clarify that requirements must be both documented and implemented
- Item concerning the fact that dial up accessible CCA's using dial up only do not require physical security was put onto parking lot

CIP 007- SYSTEMS SECURITY MANAGEMENT

Proposed language changes include:

- Language to address 706 concerns to remove 'reasonable business judgment."
- Add RE in addition to RRO.
- Removed acceptance of risk from Malicious Software Prevention (R4.1).
- Added implement under R7 Asset disposal or Redeployment.
- Editing to cite revision number
- Document maintenance was changed from review in 90 days to review documents within 30 of changes

CIP 008- INCIDENT RESPONSE & REPORTING

Proposed language changes include:

- Language to address 706 concerns to remove 'reasonable business judgment."
- Add RE in addition to RRO.
- Added implement when necessary to R1
- Added that testing the Cyber Security Plan does not require taking the component out of service.

CIP 009- RECOVERY PLANS FOR CRITICAL CYBER ASSETS

Proposed language changes include

- Language to address 706 concerns to remove 'reasonable business judgment."
- Add RE in addition to RRO.

- Changes must be incorporated into the plan within 30 days of the change

2. Discussion of More than One Phase

The facilitator suggested the Team use the acceptability ranking tool to test support and identify issues on a threshold question of whether to proceed with a single phase or more than one phase.

Team Clarifying Questions:

- Need to see what is "low-hanging" to see if time frame works or not
- Why the spring deadline? See, Letter of Response from NERC President Rick Sergel.
- Do we have to wait for the beginning of a phase to begin addressing the issue identified for that phase? No, can work on some key issues for phase two during the first phase while waiting on balloting for example
- CIP2 — concept of critical asset based assessment (NIST) versus security approach (NERC – CIP)? If tackle that then could look at current standards. The low-hanging could improve some of the current standards. If change course then earlier the better. Address some of the issues and standards before then. An incremental change over what we have now.
- If something is put up for ballot, does that preclude changes that impact it later? Identify and address first phase then address additional issues. Do not want to readdress issues a second time in phase two. Creates confusion and doubt in the industry.
- Concern is with phase two — put off more complex issue to third phase there the danger increases for addressing issues twice
- What happens in first ballot and someone votes no but it is not anything we thought about changing, is irrelevant to modifications in the ballot? There are no provisions against that happening. ANSI offers opportunities to address but upfront. Other bodies have provision saying you cannot object to something not in the proposed revision.
- Clarifying that phase one is low contention and easy and everything else is pushed to future phase(s)
- If it is in phase one does it impact the audits starting next July? Could establish a tiered approach to implementation of items in Phase One to address this.
- Only alternative is one monolithic approach rather than this proposal to break it up.
- Yes, but the "reasonable business" standard would still need to be removed by next July no matter which approach

***Roadmap Strawman Proposition*:**
"The SDT should proceed with an approach with two or more phases and products for ballot body consideration."
(This proposition does not identify what might be in each phase, just that there can be multiple phases. If a multi-phased approach is not adopted, then the approach would be that all standards changes are made within a single phase.)

First Poll on	*4 — Acceptable*	*3 — Minor Issues*	*2 — Only Acceptable*	*1 — Not acceptab*

More than 1 phase			*if major issues are addressed*	
Avg.=3.4	**11**	**8**	**2**	**0**

Team Comments following the First Ranking

- *2 ranking*-at least two items proposed for first phase concern me — first phase include easy ones but reasonable business standard needs to be deleted and then addressed in the next phase
- *2 ranking*. It is intuitive that low hanging fruit like the reasonable business exceptions language should be separated from this group while this we tackles tougher issues. However dealing with "low hanging fruit" in first phase may signal to the industry that the current standards are generally fine and we may encounter resistance when we come back to address the phase 2 tough standards issues.
- Would it be possible to address the FERC "reasonable business exception" issue and low hanging separately outside this group? Could NERC address the reasonable business standard separately? Alternates to this committee? Not given the approved SAR assigns this to the Team.
- *3 ranking*. Timetable for phase one is a concern — need more time, can we ask for an April, 2009 vs. March, 2009 deadline?
- *3 ranking*. Support a two phase but not four phase effort.
- FERC said "you must remove" and then President Rick Sergel committed getting something done quickly to be responsive to those with oversight.
- Can you just send out an advisory note saying the reasonable business judgment is no longer valid? Not appropriate to make such a statement outside the drafting process – some immediacy emergency alert exceptions to close gaps in a short order and it is not an action order, not super-ceding an existing standard as indicated here
- Another way to deal with? Issue a separate SAR and standard with red-line striping it out for comment

Following the comments and discussions regarding concerns revealed in the first poll, the Team ranked the same proposition with the following result.

Second Poll on More than 1 phase	*4 — Acceptable*	*3 — Minor Issues*	*2 — Only Acceptable if major issues are addressed*	*1 — Not acceptab*
Avg.=3.5	**14**	**5**	**3**	**0**

The Chair suggested that SDT should review and seek to agree on identifying "low hanging fruit" and must do propositions for early comments and ballot testing. The Vice Chair suggested that the question is not how many phases should there be, rather how to separate out those issues which can be quickly resolved from those items which require a longer time for resolution.

3. Draft Criteria for Inclusion of Issues in Phase-1 Product(s)

The Facilitator proposed draft criteria for inclusion of issues in Phase 1 for the Team's consideration and refinement:

- **It represents an "Editorial" item**

- **It is a must-do item per Order 706 to meet the July 1, 2009 time frame**
- **It will not preclude the Team changing standards language in Phase 2**

==========

- ~~Clarification item to design and implementation~~
- ~~Little known industry resistance~~
- ~~Limited complexity~~
- ~~Builds confidence~~
- ~~Correct known or obvious deficiencies~~

Team Comments on Draft Criteria

- "Clarification item"? I may not be able to live with this – too broad. May turn an FAQ into a guideline.
- Drop the "builds confidence" — I would say correct known or obvious deficiencies
- Correct known or obvious deficiencies (**I cannot live with this — too broad**)
- Builds confidence (** How measured? ** — just a reason for doing)
- I would add after third bullet "per 706" — that handles efficiency, drop the rest of the list as political optics — first three enough
- "Clarification" could still be very contentious
- "Building confidence"? do not know which those are?
- Okay with simple edit and per 706 must do removal of reasonable business standard
- The more we put in then the tougher it is to do it quickly
- Editing and must do should be included
- "Clarification" is just change 'design and implementation'? The "that is what we meant last time" items
- Removal of Reasonable Business Judgment, coupled with leaving some other things in that FERC wants addressed, will give the entities some latitude.
- Will FERC reject the phase 1 revisions because not everything else has been addressed? FERC staff will be attending the meetings and reporting back to the Commission on the progress, with a recommendation for approval or not, notwithstanding the fact that there are other changes pending.
- Issue of new CA/CCA does not need to be in the standard. Could possibly be handled via new Implementation plan table.
- Difficulty with the level of this discussion, it feels down in the weeds — expressing what could be in or not in phase one —
- Industry on the whole sees these issues as moving targets. The danger is if we have to go back and readdress an issue it will cause confusion in the industry.

F. PHASE I STRAWMAN REVIEW AND CONSENSUS TESTING- CIP 002-009

The Chair and Vice Chair suggested that the Team review and offer suggestions and concerns with the "strawman" phase 1 proposal that Scott Mix had put together as a "redline" draft of the CIP 002-009 standards in response to FERC Order 706. During the course of Tuesday afternoon's review of the redline draft, changes were made to the redline draft. On Wednesday morning the Team reflected on Tuesday's work and offered the following comments:

- I heard we want to get first piece out and into the process, then take some time with remaining issues — deal with time directive, then take time to look at meat of the problem.
- Is there a risk that we are toothless tiger if there is not enough progress in the first phase — will industry look up and say is that all?
- Extremely short time for change with a time certain — in communication plan must clearly let industry know there is a lot more work to come and just dealing with an immediate issue — do not put a show stopper in that keeps us from getting immediate need done.
- Higher risk to putting too much in than too little — will cause dissension and make us look like we do not know what we are doing.
- Communication plan important — get message out that we will be dealing with tougher issues.
- Two edge sword — hardest part of implementation comes in June — too much in and the industry will ask what are we doing to them — need to address FERC's request
- We say more by saying less in Phase 1.
- Implementation plan for new assets — consider addressing that and it will let industry know we are being responsive
- Go through redlines and test comfort level with what we did yesterday – some can be dealt with as implementation — create a new table 5 for implementation with groups permission and later review and approval.
- Industry may want to make comments on the requirements, measures and implementation plan – if there are controversial issues with the draft, the Team has the option of removing them before balloting.

The revised redline draft from Tuesday was then reviewed by the Team and ranked for acceptability and further refined on Wednesday morning.

OVERALL

Removing Reasonable Business Judgment Language discussion:

- If we remove the references to reasonable business judgment in CIP, what does the drafting team tell the industry they will replace for the phrases that are being removed?
- NERC staff noted there will need to be a communication plan so that the industry understands the changes that are being balloted and why the changes are being made.
- This same type of communication will need to occur at FERC so that FERC does not review the language with the elimination of reasonable business judgment but not approve the new version because it fails to address the bulk of other required changes.

CIP 002 – CRITICAL CYBER ASSET IDENTIFICATION

Proposed language changes include:

- Language to address 706 concerns to remove 'reasonable business judgment."
- Add RE in addition to RRO.
- Newly identified Critical Assets was put into the parking lot.

- Annual approval by Sr. Manager of the Risk Based Assessment in addition to the CA list

Tuesday Comments on 1st Review of the Redline

- "Reasonable business judgment" – just eliminating the end of the sentence or the whole sentence?
- Confusion if leave in the first part of that sentence — eliminate the whole sentence
- Eliminate whole sentence and avoid confusion
- Have to remove it — but must convince ballot body that it has been replaced by something somewhere
- Need supporting discussion as to why — eliminate because FERC asked us to and continuing to address the issue — acknowledge it is a small step in the right direction but only the first step
- Two main issues: based on finance not reliability — better ways to go dealing with risk management in other places in the document — kept "technical feasibility to retain flexibility but explain why
- Rather than just strike and assume dealt with below — struck for legal interpretation – should we still have the flexibility in managing to give industry flexibility without this statement
- We are meeting deadline and continuing to deal with the issue carefully - assurances we are dealing with it
- Application of exceptions must have a plan to address mitigation of the exception
- Suggest keeping both RRO and RE — later as .12

R3 – Critical Asset Identification Review?

- Don't list all the entities
- Take out the word "submit" – shall review
- Thus bump it off and address later
- Put in periodicity

R4 Newly identified critical asset

- Bump it
- Need to address when in compliance once merger takes affect — asset piece is on line — newly identified or acquired asset
- For nuclear folks they will balk at one year — evolving issue of applicability — understanding or grace period for those late to the game —
- This does not address a brand new asset — can be handled through table 5
- Requires more discussion — move it to later
- Handle through additional to implementation table — not the standard
- Cover acquisition as a separate issue?
- Add "acquired"?
- Important to address the issue — impacts when and how to bid on a system — when do I have to bring it into compliance — base line issue
- Put into early phase — phase one — but not today
- Put into phase two — but early in that phase both R4 and R5

Old R4: okay

CIP- 002 Wednesday Morning Rank, Review and Refinement

Poll on CIP 002	*4 — Acceptable*	*3 — Minor Issues*	*2 — Only Acceptable if major issues are addressed*	*1 — Not acceptab.*
Avg.=3.5	**22**	**0**	**1**	**2**

Team and Participant Comments after the Ranking

- Version updates and excise reasonable business issues (for all sections)
- Senior managers approval the only change
- Measures okay but will make change to table at the bottom
- Risk assessments changing next year — need newly identified assets here or somewhere else — comfortable with this going forward if reassured about the proposed implementation table 5 — if abandon from requirements then need somewhere
- Newly identified assets — new definition in glossary? No, put language at top of table
- Newly constructed assets? Can handle within the table but is a different issue

CIP 002 – CRITICAL CYBER ASSET IDENTIFICATION

CIP-002 DRAFT REDLINE LANGUAGE AS OF END OF MEETING, 10-8-08

A1. Title: Cyber Security — Critical Cyber Asset Identification
A2. Number: CIP-002-~~1~~2
A3. Purpose *(2nd paragraph)*
These standards recognize the differing roles of each entity in the operation of the Bulk Electric System, the criticality and vulnerability of the assets needed to manage Bulk Electric System reliability, and the risks to which they are exposed. ~~Responsible Entities should interpret and apply Standards CIP-002 through CIP-009 using reasonable business judgment.~~
A4. Applicability:
Add: 4.1.12 Regional Entities.
A5. Effective Date: ~~June 1, 2006~~

B. Requirements
R4. Annual Approval — A senior manager or delegate(s) shall approve annually the risk-based assessment methodology, the list of Critical Assets and the list of Critical Cyber Assets. Based on Requirements R1, R2, and R3 the Responsible Entity may determine that it has no Critical Assets or Critical Cyber Assets. The Responsible Entity shall keep a signed and dated record of the senior manager or delegate(s)'s approval of the the risk-based assessment methodology, the list of Critical Assets and the list of Critical Cyber Assets (even if such lists are null.)

CIP 003 – CYBER SECURITY — SECURITY MANAGEMENT CONTROLS

Proposed language changes include:

- Language to address 706 concerns to remove 'reasonable business judgment."
- Add RE in addition to RRO.
- Slight modification to the specifics requested for the designated senior manager

Tuesday Comments on 1st Review of the Redline

- Same issue of "reasonable"

- Same issue of RRO and RE's

R2.1 senior manager clarification

- Use the word fiduciary responsibility
- Can't sue the federal govt.
- Clarifying response to comments received
- "a manager" is just one, not a set of?
- In some cases it is the senior manager of each business unit within the organization
- Defining a single person for compliance when there is a second person responsible for implementation — and the two are not responsible to each other
- Intent is to establish a clear line of authority to give cyber security a higher level of importance — a person with clear line of authority who can delegate authority
- Delegation language down in R2.4
- Any thought given to how it applies in and organization with nuclear and non-nuclear facilities — depends on whether or not each is held out as a separate legal entity — how is the entity registered?
- "Senior manager accountable for"? Language here is quoted from the FERC order
- no opposition to including
- R2.4 establishes the paper trail for delegation — the form for R2.1 should include requirement to list delegation — "documented in the same manner as R2.2 and R2.3"
- Promulgating more and more documentation that creates little value — phone number changes and you are not in compliance
- Strike business phone and address
- Senior delegation — add a line regarding what a senior manager cannot sign off on? More definition to what can be by saying what can not.
- Must say "or delegate" or it cannot be delegated
- But that implies confusion — must clarify that can only be delegated where specified
- R2.1 – single manager per entity?
- Instead add "single" up in R2 and can strike R2.1? But retain the language from the directive by moving up into R2 itself
- Replace "in adherence with" with "ongoing compliance with"
- Change to make previous changes in compliance with striking R2.1 — scriveners correction

R5.3

- Punt this one for now
- Also need to add definition for "escort"

CIP- 003 Wednesday Morning Rank, Review and Refinement

Poll on CIP 003	*4 — Acceptable*	*3 — Minor Issues*	*2 — Only Acceptable if major issues are addressed*	*1 — Not acceptabl*
Avg.=	**19**	**3**	**1**	**0**

Team and Participant Comments after the first Ranking

R2 changes

- R2.3 - provides audit trail for delegation by senior manager

- In this document might take out quotes to "senior" manager — universal edit
- This is set to deal with typical response of policy — not response to requirements
- Will deal with when take up the whole body
- Auditor can only look at and audit the policy
- Why have measures?
- Instructor training for auditors to audit to the standard, not to the policy unless the standard says to audit to the policy
- Discussion in 706 about where policy says something beyond the standard — an entry in the SAR
- Quotes around "senior" have a purpose? Put in glossary? If not capitalized then glossary does not apply
- Issue beyond standard should be in policy but does not trigger a penalty
- Look at wording single senior manager — separate responsibility between compliance and operation manager — must find single senior manager above both, who can delegate specific responsibility on particular issues
- "2"- Enough question about senior and delegation of responsibility not to put it in the first phase – difficult for large company to comply with it — prefer to pull from phase one box
- One individual signs off on certification to NERC — wrinkle is when nuclear involved and not under the same umbrella — can manage but potentially problematic
- Painting CEO into being the senior manager – but that may not be the best person
- Between a 3 and 2 — are we designing the organization? Cojoining implementation and compliance which are separate in large organizations, percolates this responsibility to the top — take direct and comprehensive language out
- Part of problem is how is the organization registered versus functional model for purposes of the standards — we have three separate entities with fiduciary vice presidents at the head of each — each entity has two separate functional entities — does that mean six filings?
- Anything commensurate with this in other sections? No
- Need to resolve issue with FERC on registered entity — suspend this and clarify then revisit
- Clarify language of legislative intent
- For many entities this will be moot at the end of the calendar year — intent of FERC is whoever is signing is prominent level and influence the positive allocation of resources to improve security of the power system
- FERC focused on "single" to be sure responsibility
- Issue is the authority to correct non-compliance and that enough resources are available to comply — person who certifies needs to be the one who can direct the resources needed to address non-compliance — that is the intent, need someone with authority to correct, not just manage
- Suggest R2 changes be removed but keep change in R2.3 and 2.1 — re-poll issue
- This assignment has to be made now
- But are we making it worse with the language in R2? Compliance has a specific meaning in the industry

- We want the guy responsible for making implementation possible — in longer term revisit the "one single" person responsible
- Minor comment — "responsibility" — we delegate authority but responsibility belongs to senior manager — replace with "authority"
- Diluting the changes despite original vote — are we letting the minority rule and water down proposals? This is not a voting tool but a way to focus discussion. Grateful that points of contention are raised — this is a good thing and is a way of strengthening the language.
- This sets up the auditability of the delegation — without the paper trail, unclear whether lower levels have authority.

2nd Poll on CIP 003 As revised	*4 — Acceptable*	*3 — Minor Issues*	*2 — Only Acceptable if major issues are addressed*	*1 — Not acceptabl*
Avg.=	**22**	**0**	**0**	**1**

Comments following 2nd Rank

- 1 Rank. The problem is that you can assign responsibility but without authority to make changes — need both words in the language
- Works for everyone else
- Check with NERC General Counsel as to the meaning of the two words and the difference between the two? Suggest members check with their counsels
- We do not have accountability assigned in this
- Heads of agencies may not be allowed to delegate accountability if it is in the law – means need to add to R2.

CIP 003 – CYBER SECURITY — SECURITY MANAGEMENT CONTROLS

CIP-003 DRAFT REDLINE LANGUAGE AS OF END OF MEETING, 10-8-08

A1. Title: Cyber Security — Security Management Controls
A2. Number: CIP-003-~~1~~2
A3. Purpose *(2nd paragraph)*
Standard CIP-003 requires that Responsible Entities have minimum security management controls in place to protect Critical Cyber Assets. Standard CIP-003 should be read as part of a group of standards numbered Standards CIP-002 through CIP-009. ~~Responsible Entities should interpret and apply Standards CIP-002 through CIP-009 using reasonable business judgment.~~
A4. Applicability:
Add: 4.1.12 Regional Entities.
A5. Effective Date: ~~June 1, 2006~~

B. Requirements
R2. Leadership — The Responsible Entity shall assign a senior manager with overall responsibility and authority for leading and managing the entity's implementation of, and adherence to, Standards CIP-002 through CIP-009.
R2. 3Where allowed by Standards CIP-002 through CIP-009, the senior manager may delegate authority for specific actions to a named delegate. These delegations must be documented in the same manner as R2.1 and R2.2, and approved by the senior manager.

R2.~~3~~ 4. The senior manager or delegate(s), shall authorize and document any exception from the

requirements of the cyber security policy.

CIP 004 – Cyber Security — Personnel & Training

Proposed language changes include:

- Language to address 706 concerns to remove 'reasonable business judgment."
- Add RE in addition to RRO.
- The individuals shall be trained prior to being granted access rather than within 90 days of access
- Individuals shall be background screened prior to being granted access rather than within 30 days of access

Tuesday Comments on 1st Review of the Redline

CIP 004

- Same notes for first two

R1

- "and implement"

R2

- Lots of "ensure"s
- "carelessness"?
- some one on windows platform goes on the web for job related search — training needed to ensure they do not make mistakes
- "accidental" "unauthorized" "inadvertent" rather than "carelessness"
- more appropriate for a guidance document
- training cannot ensure but can encourage
- proper use of cyber assets includes not web surfing — already included in standards
- established who the training is for
- what was the comment that the sentence responds to?
- Move to phase two if debatable and not immediate
- Do we need to transplant everything from the FERC order into the standards?
- Depends on the wording offered by FERC — use words whenever possible, paraphrase or rephrase only as needed
- Second half of paragraph is removed and punted to next phase

R2.1.1 Emergencies

- Standard post storm procedure — puts it into the standard
- Tough on a substation but works in a center?
- Might belong in a different section , not training
- Might get questions on what constitutes and emergency
- Everything the temporary person did? That is a bit much for compliance — need alternate language — too much documentation
- Punt to phase two?
- Suggest leave in 2.1.1 and punt 2.1.2
- Change 2.1.2 to "defensive measures remain in effect"
- Move both to next phase?
- Now have no emergency provision
- Put in the parking lot the whole R2.1 section for review in phase two

R2.2

- R2.2.5-7 additional training
- Say "other security issues"
- This is where the escort training came from
- Clarification in 2.2.5 — in conflict with networking hardware?
- "security issues of electronic interconnectivity"? what does it mean?
- Three types of training — manager, real live and general awareness — maybe spell it out that simply
- 2.2.7 is a rehash and should be stricken
- But is a reply to a comment to clarify question
- Covered above
- 2.2.5 needs more work — punt to phase two — punt the whole section

R3

- Can only escort physical access not cyber access
- Okay

R3.4

- Punted under training. Moved here?
- Punt here to phase two along with R3.5 and 3.6
- What does limited escort mean? Strike "limited"

CIP- 004 Wednesday Morning Rank, Review and Refinement

1st Poll on CIP 004	*4 — Acceptable*	*3 — Minor Issues*	*2 — Only Acceptable if major issues are addressed*	*1 — Not acceptabl*
Avg.=3.5	**18**	**2**	**3**	**0**

R1

- Problem and comments about granting access electronically — not the physical escorted access — we will get lots of comments
- 2 ranking- requirement to train prior to granting access — no provision for emergency process or technical exception — will not fly with industry —
- 2 ranking — must tie to R2 above — Prior to granting access?
- R2 applies to the sub parts
- Add below in R2.1 to avoid confusion
- "Prior to" is the question — lack of emergency provision or even ongoing access to trainer before access to facilities could be a problem
- Question of physical versus electronic access — also what about the GE rep who comes in to work on equipment, cannot get him agency specific training or afford to have someone stand over his shoulder full time.
- Still required to train GE representative regardless — question is whether train before or after access; that is the correction here
- Only fix is to treat emergencies as a technical exception
- Did we put language in C3 to address this situation? Put security training in with the safety training
- We have to give access electronically to technicians in Japan
- "granted such access"?

- C3 — R1.1 deals with emergency of the storm and crews coming in to work — not the maintenance from Japan
- Contractors and vendors training? Must be equivalent to what you give employees
- C3 says write policy so that emergency storm situation would not violate the standard
- If contractor is called in for maintenance or warranty, then must be trained before being allowed access
- In an emergency situation cannot put into policy
- That is already dealt with in C3 – deals with emergency
- Good example of separating out substation, control centers, etc.

2nd Poll on CIP 004	*4 — Acceptable*	*3 — Minor Issues*	*2 — Only Acceptable if major issues are addressed*	*1 — Not acceptabl*
Avg.=3.5	**15**	**1**	**6**	**0**

Comments After 2nd Ranking

- Anything we can keep here and defer the controversy?
- The issue is timing of training and PRAs
- Propose a small team to try and redraft. Steve Vandenberg would like to be on the team

CIP 004 – CYBER SECURITY — PERSONNEL & TRAINING

CIP-004 DRAFT REDLINE LANGUAGE AS OF END OF MEETING, 10-8-08

A1. Title: Cyber Security — Cyber Security — Personnel & Training
A2. Number: CIP-004-~~1~~2
A3. Purpose:
Standard CIP-004 requires that personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets, including contractors and service vendors, have an appropriate level of personnel risk assessment, training, and security awareness. Standard CIP-004 should be read as part of a group of standards numbered Standards CIP-002 through CIP-009. ~~Responsible Entities should interpret and apply Standards CIP-002 through CIP-009 using reasonable business judgment~~.
A4. Applicability:
Add: 4.1.12 Regional Entities.
A5. Effective Date: ~~June 1, 2006~~

B. Requirements
R1. Awareness — The Responsible Entity shall establish, maintain, and document and implement a security awareness program to ensure personnel having authorized cyber or authorized unescorted physical access to critical cyber security assets receive on-going reinforcement in sound security practices…
R2. Training — The Responsible Entity shall establish, maintain, and document and implement an annual cyber security training program for personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets, and review the program annually and update as necessary.
R2.1. This program will ensure that all personnel having such access to Critical Cyber Assets, including contractors and service vendors, are trained prior to their being granted such access. ~~within ninety calendar~~

~~days of such authorization.~~
R3. Personnel Risk Assessment —The Responsible Entity shall have a documented personnel risk assessment program, in accordance with federal, state, provincial, and local laws, and subject to existing collective bargaining unit agreements, for personnel having authorized cyber or authorized unescorted physical access. A personnel risk assessment shall be conducted pursuant to that program prior to ~~within thirty days of~~ such personnel being granted such access.

CIP 005 – ELECTRONIC SECURITY PERIMETER(S)

Proposed language changes include:

- Language to address 706 concerns to remove 'reasonable business judgment."
- Add RE in addition to RRO.
- Minor editorial changes only

Tuesday Comments on 1st Review of the Redline

R1.5

- Editorial
- The rest are fine
- Address specific call outs in R1.5 as needed

CIP- 005 Wednesday Morning Rank, Review and Refinement

Poll on CIP 005	*4 — Acceptable*	*3 — Minor Issues*	*2 — Only Acceptable if major issues are addressed*	*1 — Not acceptabl*
Avg.=3.5	**22**	**0**	**0**	**0**

CIP 005 revisited

R1.5

- If used only for monitoring or control does it fall under this – put in "and/or" monitoring.
- Same issue under CIP 006

CIP 005 – ELECTRONIC SECURITY PERIMETER(S)

CIP-005 DRAFT REDLINE LANGUAGE AS OF END OF MEETING, 10-8-08

A1. Title: Cyber Security — Electronic Security Perimeter(s)
A2. Number: CIP-005-~~1~~2
A3. Purpose:
Standard CIP-005 requires the identification and protection of the Electronic Security Perimeter(s) inside which all Critical Cyber Assets reside, as well as all access points on the perimeter. Standard CIP-005 should be read as part of a group of standards numbered Standards CIP-002 through CIP-009.~~Responsible Entities should interpret and apply Standards CIP-002 through CIP-009 using reasonable business judgment~~.
A4. Applicability:
Add: 4.1.12 Regional Entities.
A5. Effective Date: ~~June 1, 2006~~

B. Requirements

R1.5. Cyber Assets used in the access control and monitoring of the Electronic Security Perimeter(s) shall be afforded the protective measures as a specified in Standard CIP- 003, Standard CIP-004 Requirement R3, Standard CIP-005 Requirements R2 and R3, Standard CIP-006 Requirements R2 and R3, Standard CIP-007, Requirements R1 and R3 through R9, Standard CIP-008, and Standard CIP-009. *(Staff will correct the citations)*

R2.3. The Responsible Entity shall maintain and implement a procedure for securing dial-up access to the Electronic Security Perimeter(s).

CIP 006 – PHYSICAL SECURITY OF CRITICAL CYBER ASSETS

Proposed language changes include:

- Language to address 706 concerns to remove 'reasonable business judgment."
- Change RRO to RRO and also include RE.
- Several items where the word 'implement' was added to clarify that requirements must be both documented and implemented
- Item concerning the fact that dial up accessible CCA's using dial up only do not require physical security was put onto parking lot

Tuesday Comments on 1st Review of the Redline

R.1

- "The" senior manager not "a" senior manager
- "implementing"
- R1.7 — back it down to thirty days from completion of any physical system
- Same specific call outs as in CIP005
- Interpretation sce&g RFI

CIP- 006 Wednesday Morning Rank, Review and Refinement

Poll on CIP 006	*4 - Acceptable*	*3 – Minor Issues*	*2 – Only Acceptable if major issues are addressed*	*1 – Not acceptable*
Avg.=3.5	**0**	**0**	**0**	**0**

Tabled, hand off to a drafting team

Comments after Ranking

- Request for R4 — physical access include individual leaving facility — for physical access include when individual leaves as written — what is the intent?
- Only time of access not time ended or duration
- This is contentious to industry — pull until later
- "Thirty" calendar days — make it from completion of implementation, to capture the spirit and intent
- 1.4 and 1.6 need "procedures for and implementation of"
- this applies to physical facility plans
- 1.8 — must change to right numbers to match version two for consistency
- 1.7 — bad English — remove "completion of"
- Punt to a scrivener team
- prefer the original language — confuses implementation and procedures

- wordsmith starting with R1 to clean up — hand off to a team
- Interpretation of R1.1 about non-routable protocols?
- Important but recommend deferring until after FERC renders initial judgment
- Agree, but defer
- But not filed with FERC yet — will never go to FERC to act on for procedural reasons. Then handle in phase two

CIP 006 – PHYSICAL SECURITY OF CRITICAL CYBER ASSETS

CIP-006 DRAFT REDLINE LANGUAGE AS OF END OF MEETING, 10-8-08

A1. Title: Cyber Security — Physical Security of Critical Cyber Assets
A2. Number: CIP-006-~~1~~2
A3. Purpose:
Standard CIP-006 is intended to ensure the implementation of a physical security program for the protection of Critical Cyber Assets. Standard CIP-006 should be read as part of a group of standards numbered Standards CIP-002 through CIP-009. ~~Responsible Entities should apply Standards CIP-002 through CIP-009 using reasonable business judgment.~~
A4. Applicability:
Add: 4.1.12 Regional Entities.
A5. Effective Date: ~~June 1, 2006~~

B. Requirements
R1. Physical Security Plan — The Responsible Entity shall create ~~and~~ maintain and implement a physical security plan, approved by the ~~a~~ senior manager or delegate(s) that shall address, at a minimum, the following:
R1.2. Processes to identify all access points through each Physical Security Perimeter and implement measures to control entry at those access points.
R1.4. Procedures for and the implementation of the appropriate use of physical access controls as described in Requirement R3 including visitor pass management, response to loss, and prohibition of inappropriate use of physical access controls.
R1.6. Procedures for and implementation of escorted access within the physical security perimeter of personnel not authorized for unescorted access.
R1.7. Process for updating the physical security plan within ~~ninety~~ thirty calendar days of implementation of any physical security system redesign or reconfiguration, including, but not limited to, addition or removal of access points through the physical security perimeter, physical access controls, monitoring controls, or logging controls.
R1.8. Cyber Assets used in the access control and monitoring of the Physical Security Perimeter(s) shall be afforded the protective measures specified in Standard CIP-003, Standard CIP-004 Requirement R3, Standard CIP-005 Requirements R2 and R3, Standard CIP-006 Requirement Standard CIP-009. *(Staff will correct the citations)*

CIP 007 SYSTEMS SECURITY MANAGEMENT

Proposed language changes include:

- Language to address 706 concerns to remove 'reasonable business judgment."
- Change RRO to RRO and also include RE.
- Removed acceptance of risk from Malicious Software Prevention (R4.1).
- Added implement under R7 Asset disposal or Redeployment.
- Editing to cite revision number
- Document maintenance was changed from review in 90 days to review documents within 30 of changes

Tuesday Comments on 1st Review of the Redline

CIP- 007

R2

- Implement

R4.1

- The use of anti-virus — document the use of and implement anti-virus
- Implement and document the use of
- Need more definition of "technical feasibility" not necessarily remove it
- What does 4.1 add that is not already in R4 — first sentence is redundant
- Return 4.1 to its original language — remove proposed edits
- Strike or an acceptance of risk from the end of the sentence

R5

- Editorial corrections

R7.1

- "sufficiently" is vague – why use it?
- Remove
- Clarify what you mean by unauthorized retrieval of data
- Punt it for now
- Look at NIST and DOD language
- Not changing approved language but parking the data storage requirements

R9

- Ninety to thirty days

CIP- 007 Wednesday Morning Rank, Review and Refinement

Poll on CIP 007	*4 — Acceptable*	*3 — Minor Issues*	*2 — Only Acceptable if major issues are addressed*	*1 — Not acceptabl*
Avg.=3.5	**21**	**1**	**0**	**0**

Team and Participant Comments Following the Ranking

- Clarifications?
- What do we gain by saying establish and implement rather than document – should we be consistent
- R4.1?
- Can not just accept risk

- Explain how technical feasibility exception applies for a virus? Must have mitigating measures.
- If you have a system that can not use anti-virus software such as a substation or that would be adverse impacts if installed – best option is a network filtering anti-virus
- Is it acceptable to say there are not mitigations available if cannot use anti-virus – un-hackability is acceptable but be documented
- Is there such a thing as unhackable software?
- Developing a formal cyber security plan discussion yesterday? C6 requires a physical security plan but nothing requires a cyber security plan

CIP 007 SYSTEMS SECURITY MANAGEMENT

CIP-007 DRAFT REDLINE LANGUAGE AS OF END OF MEETING, 10-8-08

A1. Title: Cyber Security — Systems Security Management
A2. Number: CIP-007-~~1~~2
A3. Purpose:
Standard CIP-007 requires Responsible Entities to define methods, processes, and procedures for securing those systems determined to be Critical Cyber Assets, as well as the non-critical Cyber Assets within the Electronic Security Perimeter(s). Standard CIP-007 should be read as part of a group of standards numbered Standards CIP-002 through CIP-009. ~~Responsible Entities should apply Standards CIP-002 through CIP-009 using reasonable business judgment.~~
A4. Applicability:
Add: 4.1.12 Regional Entities.
A5. Effective Date: ~~June 1, 2006~~

B. Requirements
R2. Ports and Services — The Responsible Entity shall establish and document and implement a process to ensure that only those ports and services required for normal and emergency operations are enabled.
R3. Security Patch Management — The Responsible Entity, either separately or as a component of the documented configuration management process specified in CIP-003 Requirement R6, shall establish, ~~and~~ document and implement a security patch management program for tracking, evaluating, testing, and installing applicable cyber security software patches…
R4.1. The Responsible Entity shall document and implement anti-virus and malware prevention tools. In the case where anti-virus software and malware prevention tools are not installed, the Responsible Entity shall document compensating measure(s) applied to mitigate risk exposure. ~~or an acceptance of risk~~.
R7. Disposal or Redeployment — The Responsible Entity shall establish and implement formal methods, processes, and procedures for disposal or redeployment of Cyber Assets within the Electronic Security Perimeter(s) as identified and documented in Standard CIP-005.
R9. Documentation Review and Maintenance — The Responsible Entity shall review and update the documentation specified in Standard CIP-007 at least annually. Changes resulting from modifications to the systems or controls shall be documented within ~~ninety~~ thirty calendar days of the change being completed.

CIP 008 INCIDENT RESPONSE & REPORTING

Proposed language changes include:

- Language to address 706 concerns to remove 'reasonable business judgment."
- Add RE in addition to RRO.
- Added implement when necessary to R1
- Added that testing the Cyber Security Plan does not require taking the component out of service.

Tuesday Comments on 1st Review of the Redline

CIP 008

R1

- Implement when you have an incident — when necessary
- When necessary applies grammatically to the "prepare and maintain" phrase too
- Move "implement when necessary" to the end of the sentence.

R1.4 & 1.5

- Why have requirement after action has occurred — getting approval for what you did after the fact
- You have an approved plan but realize it is not adequate and you take additional steps — now need to document that and ask if you can modify the plan
- The wording is implicit that plan has prescribed reaction to prescribe incident — depends on level of detail in a plan
- Detailed prescriptive plan that anyone after you can follow
- What are we adding here if we review plan every year?
- After action reports to revise plan for those plans that were inadequate for dealing with the plan —
- Tested your plan but cannot anticipate every possibility
- Lessons learned in 686 is different than words used here
- Punt and deal with in phase 2 for both items

R1.6

- Improving plan in response to lessons learned
- Keep "thirty days" — punt the "resulting from implementing the plan"

R1.8

- Change is good

CIP- 008 Wednesday Morning Rank, Review and Refinement

Poll on CIP 008	*4 — Acceptable*	*3 — Minor Issues*	*2 — Only Acceptable if major issues are addressed*	*1 — Not acceptabl*
Avg.=3.5	**20**	**2**	**0**	**0**

C8

- Need to explain R1 to industry
- Better to say implement when an incident occurs – refines the word "necessary"
- In response to a Cyber Security Incident – a defined term in the NERC glossary
- Need to say suspected incident – say "potential" instead
- That creates issues – we have potential incidents all the time and do not invoke the plan – if you don't know – should be a know incident with a measurable impact
- Need to anticipate suspected or potential to invoke and update the plan as needed
- Table this for now – problem with a one level plan – defined a process to address multiple levels of plans – needs more discussion in phase two
- Someone fat fingers their password – is that an incident? Must the plan be invoked?
- Important thing is that the plan has to be implemented in response to an event – type of event does not matter – if never implemented it is because you never had an event
- Adding "potential" confuses things
- Take out "potential" – adds confusion
- Consider changing cyber security incidents by removing "a"
- Needs to be some thought or wordsmithing on a few areas – need to review suggested changes
- Any drafting need to be done before next meeting or take up in two weeks?
- Still unsettled but not sure why
- Like to revisit the whole thing in next phase
- Also concerned as to why this statement is even there

- Probably not harmful to leave in but creating an opportunity for comments that we have to respond to
- Point to industry comment and FERC order to explain why it is being addressed
- Consider second sentence: plan will be implemented in response to an cyber security incident
- Put in "implement the plan in response"
- May need to address cyber security incident definition in the next phase
- No assignment needed to address language prior to next meeting

CIP 008 INCIDENT RESPONSE & REPORTING

CIP-008 DRAFT REDLINE LANGUAGE AS OF END OF MEETING, 10-8-08

A1. Title: Cyber Security — Incident Reporting and Response Planning
A2. Number: CIP-008-~~1~~2
A3. Purpose:
Standard CIP-008 ensures the identification, classification, response, and reporting of Cyber Security Incidents related to Critical Cyber Assets. Standard CIP-008 should be read as part of a group of standards numbered Standards CIP-002 through CIP-009. ~~Responsible Entities should apply Standards CIP-002 through CIP-009 using reasonable business judgment~~
A4. Applicability:
Add: 4.1.12 Regional Entities.
A5. Effective Date: ~~June 1, 2006~~

B. Requirements
R1. Cyber Security Incident Response Plan — The Responsible Entity shall develop and maintain a Cyber Security Incident response plan and implement the plan in response to Cyber Security Incidents. The Cyber Security Incident Response plan shall address, at a minimum…
R1.4. Process for updating the Cyber Security Incident response plan within ~~ninety~~ thirty calendar days of any changes.
R1.6. Process for ensuring the Cyber Security Incident response plan is tested at least annually. A test of the incident response plan can range from a paper drill, to a full operational exercise, to the response to an actual incident. Testing the Cyber Security Incident response plan does not require removing a component or system from service during the test.

CIP 009 RECOVERY PLANS FOR CRITICAL CYBER ASSETS

Proposed language changes include

- Language to address 706 concerns to remove 'reasonable business judgment."
- Add RE in addition to RRO.
- Changes must be incorporated into the plan within 30 days of the change

Tuesday Comments on 1st Review of the Redline
CIP- 009
R1.3 & 1.4

- Similar to CIP008 – but language from the order
- Imply the action must be approved by the senior manager?

- If the document was wrong and following it would have cause problems then you need to apply the lesson, revise the plan and get it approved
- Is 1.4 a restatement of 1.3? No, first is a justification and 1.4 is revise the plan
- This does not read right
- Punt this one for redraft

R3

- "Thirty days"

CIP-009 Wednesday Morning Rank, Review, and Refinement

Poll on CIP 009	*4 — Acceptable*	*3 — Minor Issues*	*2 — Only Acceptable if major issues are addressed*	*1 — Not acceptable*
Avg.=4.0	**22**	**0**	**0**	**0**

CIP-009 DRAFT REDLINE LANGUAGE AS OF END OF MEETING, 10-8-08

A1. Title: Cyber Security — Recovery Plans for Critical Cyber Assets
A2. Number: CIP-009-~~1~~2
A3. Purpose:
Standard CIP-009 ensures that recovery plan(s) are put in place for Critical Cyber Assets and that these plans follow established business continuity and disaster recovery techniques and practices. Standard CIP-009 should be read as part of a group of standards numbered Standards CIP-002 through CIP-009. ~~Responsible Entities should apply Standards CIP-002 through CIP-009 using reasonable business judgment~~.
A4. Applicability:
Add: 4.1.12 Regional Entities.
A5. Effective Date: ~~June 1, 2006~~

B. Requirements
R3. Change Control — Recovery plan(s) shall be updated to reflect any changes or lessons learned as a result of an exercise or the recovery from an actual incident. Updates shall be communicated to personnel responsible for the activation and implementation of the recovery plan(s) within ~~ninety~~ thirty calendar days of the change being completed.

G. TEAM BUILDING- GO LEFT- GO RIGHT PREFERENCES

The Team engaged in a brief exercise to highlight the members' individual preferences for problem solving and decision-making. *(See Appendix #7 for the results of the exercise)* Following the exercise the facilitator noted that a sign of a well balanced group includes a diversity of work styles. For example having some who prefer to pay attention to task and others who prefer to pay attention to people issues can be very helpful. These are not either/or preferences but signal for the Team how they individually and collectively come at the issues. Finally they can help group leaders and those assisting in process by, for example, noting a distinct preference for morning and trying not to take on the hardest issues late in the afternoon.

H. REVIEW OF PHASE I MEETING SCHEDULE AND DRAFTING ASSIGNMENTS

1. In Person Meetings and WebEx Schedule

Session Type	Dates	Agenda
Webex/Conf call session	Oct 15	Individual sub team Webex's to review their respective Phase I assignment deliverables in advance of full team review during October 21-22 meeting in Sacramento.
In person meeting at SMUD (Sacramento, Kevin Sherlin)	October 21-22 Full/Full	Review and comment upon sub team straw proposals.
Webex/Conf call session	Oct 29	Finalize the Phase I posting documents and submit to MEL
WebEx/conf call session	Nov 5 - NERC staff feedback	Review and conform drafts per feedback from MEL
In person meeting at Princeton, NJ (confirmed)	Nov 12-14 Half/Full/Half	Phase II
WebEx/conf call session	Nov 18 Webex/Conf call	Phase II
In person meeting at FERC offices or Charlotte	December 4-5 Full/Full	Phase II
In person meeting at APS (Phoenix, Bill Winters) or BPA (Portland WA, Jon Stanford)	January 7-9 Half/Full/Half	Consider Comments to Phase I posting

2. Assignments

	Task	Leader	Sub team	Due Date
1	CIP-004 R2 and R3	Jackie Collett	Chris Peters, John Varnell, Sharon Edwards	Straw Proposal due to sub team leader on October 14 in advance of sub team WebEx on October 15
2	CIP-006 R1	Kevin Perry	Joe Doetzl, Scott Fixmer, Thomas Hofstetter	Straw Proposal due to sub team leader on October 14 in advance of sub team WebEx on October 15
3	Review Measures	Jerry Freese	Keith Stouffer,	Straw Proposal due to

	associated with changes in CIP-002 to CIP-009		Roger Lampila, Todd Thompson	sub team leader on October 14 in advance of sub team WebEx on October 15
4	Implementation Plan – update to address newly identified CA	Scott Mix	Michael Winters, Dave Norton, Kevin Perry	Straw Proposal due to sub team leader on October 14 in advance of sub team WebEx on October 15
5	Implementation Plan update to address revised Requirements from Phase I and Mapping document – matrix that compares current version of standard with revised version with a comment that explains what changed.	Phil Huff	Kevin Sherlin, Scott Rosenberger, Jon Stanford, Scott Mix	Straw Proposal due to sub team leader on October 14 in advance of sub team WebEx on October 15
6	Comment Form – including an extensive write-up of the background, rationale for revisions, explanatory text.	Jeri Domingo-Brewer	Steve Vandenberg, Harry Tom, Sharon Edwards, John Lim	Straw Proposal due to sub team leader on October 14 in advance of sub team WebEx on October 15
7	Review VRFs associated with changes in CIP-002 to CIP-009	Todd Thompson	Roger Lampila	Straw Proposal due to sub team leader on October 14 in advance of sub team WebEx on October 15

I. AFTER-ACTION REVIEW AND EVALUATION

At the conclusion of the meeting, the Team offered an evaluation of the process including what worked and what could be improved. *(See Appendix # 4 for the Team's review and suggestions.)*

Adjourned at noon on Wednesday October 8, 2008.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Appendix # 1

SDT Cyber Security Order 706 1st Meeting Agenda

October 6, 2008 — 1 PM to 5 PM EST
October 7, 2008 — 8 AM to 5 PM EST
October 8, 2008 — 8 AM to 12 Noon EST

National Institute of Standards & Technology
100 Bureau Drive
Gaithersburg, MD

WebEx Password: standards	Conf Call dial-in number (732) 694-2061
WebEx Meeting numbers: Monday 711 925 616 Tuesday 713 677 232 Wednesday 712 239 082	Conference Codes: Monday 12081006082 Tuesday 12081007081 Wednesday 12081008082

Monday October 6, 2008

1. Opening remarks — Michael Assante, CSO, NERC
2. Review NERC Antitrust Compliance Guidelines — Harry Tom
3. Welcome and Introductions — Jeri Domingo-Brewer/Kevin Perry
4. Overview of NERC Standards Development Process — Gerry Adamski/Dave Taylor
5. Review of CSO706 SAR — Dave Norton

Tuesday October 7, 2008

6. Overview of NIST Risk Management Framework — Keith Stouffer
7. Comparison of NIST and NERC Cyber Standards — Keith Stouffer
8. Project Roadmap – Jeri Domingo-Brewer with facilitation assistance

Wednesday October 8, 2008

9. Project Roadmap Wrap-up (facilitated)
10. Next Steps
11. Plan future meetings schedule

Appendix # 2

Cyber Security for Order 706 Standard Drafting Team and Attendees List
Project 2008-06 — CSO 706 SDT

D. Jack Bernhardsen	President/Manager Pacific Northwest Security Coordinator, Inc.
Jeri Domingo Brewer, Chair	U.S. Bureau of Reclamation
Jackie Collett	Manitoba Hydro
Jay S. Cribb	Information Security Analyst, Principal, Southern Company Services, Inc.
Joe Doetzl	Manager, Information Security. Kansas City Power & Light Co
Sharon Edwards	Project Manager, Duke Energy
Scott Fixmer	Senior Security Analyst Exelon Corporate Security, Exelon Corporation
Gerald S. Freese	Director, Enterprise Information Security American Electric Power
Tom Hofstetter	Midwest ISO, Inc.
Philip Huff	Arkansas Electric Cooperative Corporation
John Lim,	CISSP, Department Manager, Consolidated Edison Co. of New York
David L. Norton	Policy Consultant - CIP Entergy Corporation
Kevin B. Perry, Vice Chair	Director, IT-Infrastructure, Southwest Power Pool
Christopher A. Peters	ICF International
David S. Revill	Georgia Transmission Corporation
Scott Rosenberger	Luminant Energy
Kevin Sherlin	Sacramento Municipal Utility District
Bryan Singer	Wurldtech Security Technologies
Jon Stanford	Bonneville Power Administration
Keith Stouffer	National Institute of Standards & Technology
Steve Vandenberg	BC Hydro Power Supply
John D. Varnell	Technology Director, Tenaska Power Services Co.
Michael Winters	Arizona Public Service Co.
William Winters	Hydro One Networks, Inc.
Roger Lampila	*NERC Regional Compliance Program Coordinator*
Scott Mix	*NERC Manager of Situation Awareness and Infrastructure Security,*
Todd Thompson	*NERC Regional Compliance Program Coordinator*
Harry Tom	*NERC Standards Development Coordinator*
Bob Jones, Stuart Langton, Hal Beardall	*Facilitators, FSU/ FCRC Consensus Solutions Center*

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

List of Attendees — Cyber Security Order 706

Standard Drafting Team Meeting
National Institute of Standards & Technology — Gaithersburg, MD
October 6–8, 2008

Attending in Person- Team Members

1. D. Jack Bernhardsen	President/Manager Pacific Northwest Security Coordinator, Inc.
2. Jeri Domingo Brewer, Chair	U.S. Bureau of Reclamation
3. Jackie Collett	Manitoba Hydro
4. Jay S. Cribb	Information Security Analyst, Principal, Southern Company Services, Inc.
5. Joe Doetzl	Manager, Information Security. Kansas City Power & Light Co
6. Sharon Edwards	Project Manager, Duke Energy
7. Scott Fixmer	Senior Security Analyst Exelon Corporate Security, Exelon Corporation
8. Gerald S. Freese	Director, Enterprise Information Security American Electric Power
9. Tom Hofstetter	Midwest ISO, Inc.
10. Philip Huff	Arkansas Electric Cooperative Corporation
11. John Lim,	CISSP, Department Manager, Consolidated Edison Co. of New York
12. David L. Norton	Policy Consultant - CIPEntergy Corporation
13. Kevin B. Perry, Vice Chair	Director, IT-Infrastructure, Southwest Power Pool
14. Christopher A. Peters	ICF International
15. David S. Revill	Georgia Transmission Corporation
16. Scott Rosenberger	Luminant Energy
17. Kevin Sherlin	Sacramento Municipal Utility District
18. Jon Stanford	Bonneville Power Administration
19. Keith Stouffer	National Institute of Standards & Technology
20. John D. Varnell	Technology Director, Tenaska Power Services Co.
21. Michael Winters	Arizona Public Service Co.
22. William Winters	Hydro One Networks, Inc.
1. David Taylor	*NERC*
2. Harry Tom	*NERC*
3. Michael Assante	*NERC*
4. Roger Lampila	*NERC*
5. Scott R Mix	*NERC*
6. Todd Thompson	*NERC*
7. Gerry Adamski	*NERC*
8. Robert Jones	*FSU/FCRC Consensus Solutions Center*
9. Stuart Langton	*FSU/FCRC Consensus Solutions Center*
10. Hal Beardall	*FSU/FCRC Consensus Solutions Center*

SDT Team Member Attending via Webex *(in order of roll call, October 6)*

1. Steve Vandenberg	BC Hydro

SDT Members Unable to Attend or Participate by Webex

1. Bryan L. Singer*	Kenexis

Attending in Person- Participants

	NAME	COMPANY
1	Marshall Abrams	MITRE
2	Markus Braendle	ABB
3	James Brenton	ERCOT

4	Jerome Farquharson	Burns & McDonnell Engineering
5	Roger Fradenburgh	Network & Security Technologies
6	Stu Katzke	NIST
7	John Joseph McGlynn IV	PJM
8	Steve McElwee	PJM Interconnection
9	Dan Mishra	Midwest ISO
10	Peter Nelson	Network & Security Technologies
11	Mike Peters	FERC *(October 6 & 7 in person, October 8 by phone)*
12	Mark Simon	Encari
13	Michael Toecker	Burns & McDonnell Engineering

Attending via Webex- Participants *(in order of roll call, October 6)*

2	Mike Mertz	Southern California Edison
4	Alex Tatistcheff	Idaho Power
5	Regis Binder	FERC
6	Mike Fischette	Lansing Board of Water and Light
7	Phil Sobol	Corporate Risk Solutions, Inc
8	David Dunn	IESO
9	Dan Thanos	GE
10	Vicki O'Leary	NGRID
11	Boyd Nation	Southern Company
12	Dave Batz	Alliant Energy
13	John Friday	Reliant Energy
14	Rodney O'Brian	Southern Company
15	Steve Brezina	WAPA
16	Matt Schnell	Nebraska Public Power District
17	Karen Yoder	First Energy
18	Mike Puscas	United Illuminating
19	Doug Johnson	Commonwealth Edison
20	Chip Lees	
21	Ameren — Hoang Ngo	Reliant
22	James Bassett	IPC

Appendix # 3
NERC Antitrust Compliance Guidelines

I. General

It is NERC's policy and practice to obey the antitrust laws and to avoid all conduct that unreasonably restrains competition. This policy requires the avoidance of any conduct that violates, or that might appear to violate, the antitrust laws. Among other things, the antitrust laws forbid any agreement between or among competitors regarding prices, availability of service, product design, terms of sale, division of markets, allocation of customers or any other activity that unreasonably restrains competition.

It is the responsibility of every NERC participant and employee who may in any way affect NERC's compliance with the antitrust laws to carry out this commitment.

Antitrust laws are complex and subject to court interpretation that can vary over time and from one court to another. The purpose of these guidelines is to alert NERC participants and employees to potential antitrust problems and to set forth policies to be followed with respect to activities that may involve antitrust considerations. In some instances, the NERC policy contained in these guidelines is stricter than the applicable antitrust laws. Any NERC participant or employee who is uncertain about the legal ramifications of a particular course of conduct or who has doubts or concerns about whether NERC's antitrust compliance policy is implicated in any situation should consult NERC's General Counsel immediately.

II. Prohibited Activities

Participants in NERC activities (including those of its committees and subgroups) should refrain from the following when acting in their capacity as participants in NERC activities (e.g., at NERC meetings, conference calls and in informal discussions):

- Discussions involving pricing information, especially margin (profit) and internal cost information and participants' expectations as to their future prices or internal costs.
- Discussions of a participants' marketing strategies.
- Discussions regarding how customers and geographical areas are to be divided among competitors.
- Discussions concerning the exclusion of competitors from markets.
- Discussions concerning boycotting or group refusals to deal with competitors, vendors or suppliers.

III. Activities That Are Permitted

From time to time decisions or actions of NERC (including those of its committees and subgroups) may have a negative impact on particular entities and thus in that sense adversely impact competition. Decisions and actions by NERC (including its committees and

subgroups) should only be undertaken for the purpose of promoting and maintaining the reliability and adequacy of the bulk power system. If you do not have a legitimate purpose consistent with this objective for discussing a matter, please refrain from discussing the matter during NERC meetings and in other NERC-related communications.

You should also ensure that NERC procedures, including those set forth in NERC's Certificate of Incorporation and Bylaws are followed in conducting NERC business. Other NERC procedures that may be applicable to a particular NERC activity include the following:

- Reliability Standards Process Manual
- Organization and Procedures Manual for the NERC Standing Committees
- System Operator Certification Program

In addition, all discussions in NERC meetings and other NERC-related communications should be within the scope of the mandate for or assignment to the particular NERC committee or subgroup, as well as within the scope of the published agenda for the meeting.

No decisions should be made nor any actions taken in NERC activities for the purpose of giving an industry participant or group of participants a competitive advantage over other participants. In particular, decisions with respect to setting, revising, or assessing compliance with NERC reliability standards should not be influenced by anti-competitive motivations.

Subject to the foregoing restrictions, participants in NERC activities may discuss:

- Reliability matters relating to the bulk power system, including operation and planning matters such as establishing or revising reliability standards, special operating procedures, operating transfer capabilities, and plans for new facilities.
- Matters relating to the impact of reliability standards for the bulk power system on electricity markets, and the impact of electricity market operations on the reliability of the bulk power system.
- Proposed filings or other communications with state or federal regulatory authorities or other governmental entities.
- Matters relating to the internal governance, management and operation of NERC, such as nominations for vacant committee positions, budgeting and assessments, and employment matters; and procedural matters such as planning and scheduling meetings.

Any other matters that do not clearly fall within these guidelines should be reviewed with NERC's General Counsel before being discussed.

Appendix # 4
After Action Review and Team Process Evaluation

What did you think was most effective about the meeting?

- This is a high performance group with experience and openness to listen and work together through disagreements — everyone participated
- Meeting preparation — Scott 's Phase 1"strawman" was something we could discuss and that was key. Information Harry sent in advance was very helpful
- Members and participants offered constructive solutions that we could rally around
- Helped to have someone else to push us through (i.e. facilitate) allowing the chair and vice chair to more fully participate without having to worry or focus on process
- First time with an outside facilitator for some members- very much helped
- Having senior NERC staff on hand (Gerry, David, Harry, Scott) saved lots of time and helped Team understand how this works.
- Sharon's note taking was well done, very helpful and will help the facilitators produce an accurate summary and record of the sessions
- Thank NIST for all their hard work — their review will benefit us as we move forward into Phase 2.
- Harry responding to everyone's requests was very helpful
- Thank you to the facilitators — positive experience to share with other drafting teams
- Thanks to Keith for hosting and all of his work behind the scenes to pulling this meeting off

Suggestions for next meeting – Should we do anything differently?

- Larger room would have helped
- Need more microphones for those on the phone to hear what those in the room are saying — need to assure quality of system too. This is an important investment in those participating beyond the team members.
- Internet access during the meeting to pull up documents as needed — and power strips for computers.
- Computer running projection should be separate from the WebEx computer — one running WebEx and a second to access research m whatever is running the projector should be separate from meeting host — allows you to use raise hand tool on WebEx

Other suggestions:

- Table purpose statement and any other organizational issues (consensus procedures, roles, etc.) until next full meeting

- Team meeting presentation materials will be posted on the NERC Team webpage. They will be referenced in the meeting summary as appendices and links. They will be clearly labeled as presentation and informational briefing materials for the Team's consideration, not Team products. This will also be made clear in the meeting summary.

Appendix #5
Standard Authorization Request (SAR)
Revisions to Critical Infrastructure Protection Standards (revisions to CIP-002 through CIP-009, June 9, 2008))

http://www.nerc.com/filez/standards/Project_2008-06_Cyber_Security.html

Appendix #5
CIP 002-009 Redline Straw Man Draft, October 8, 2008
CIP 002-009 Clean Straw Man Draft, October 8, 2008

Click on the following link for the document:

http://www.nerc.com/filez/standards/Project_2008-06_Cyber_Security.html

Appendix # 6 SDT Draft Consensus Guidelines

DRAFT CONSENSUS GUIDELINES

CONSENSUS DEFINED

Consensus is a **process**, **an attitude and an outcome**. Consensus processes can produce better quality more informed products.

A. Consensus is a problem solving process in which all members:

1. Jointly distinguish their concerns
2. Educate each other
3. Jointly develop alternatives and then
4. Adopt recommendations everyone can embrace or at least live with.

In a consensus process, members can honestly say:

- I believe that other members understand my point of view
- I believe I understand other members' points of view
- Whether or not I prefer this decision, I support it because it was arrived at openly and fairly and because it is the best solution for us at this time

B. Consensus as an attitude provides that each member commits to work toward agreements that meet their own and other member needs and that all can support the outcome.

C. Consensus as an outcome means that agreement is reached by all members or by a significant majority of members. The level of enthusiasm for the agreement may not be the same among all members on any issue, but on balance all should be able to live with the overall package. **Levels of consensus** can include:

- Participants strongly support the solution
- Participants can "live with" the solution
- Some participants do not support the solution but agree not to veto it.

DRAFT CONSENSUS GUIDELINES

The Cyber Security for Order 706 Standard Drafting Team (Team) will seek consensus on its recommendations for any revisions to the CIP standards including assessment of the reliability and market interface impacts.

General consensus is a participatory process whereby, on matters of substance, the members strive for agreements which all of the members can accept, support, live with or agree not to oppose. In instances where, after vigorously exploring possible ways to enhance the members' support for the final package of recommended revisions, and the Team finds that 100% acceptance or support is not achievable, final consensus recommendations will require at least 75% favorable vote of all members present and voting. This super majority decision rule underscores the importance of actively developing consensus throughout the process on substantive issues with the participation of all members. In instances where the Team finds that even 80% acceptance or support is not achievable, the Team's report will include documentation of any differences as well as the options that were considered for which there was greater than 50% support from the Team.

The Team will develop its recommendations using consensus-building techniques with the leadership of the Chair and Vice Chair and the assistance of the facilitators. Techniques such as brainstorming, ranking and prioritizing approaches will be utilized. The Team's consensus process will be conducted as a facilitated consensus-building process. Team members, NERC staff and facilitators will be the only participants seated at the table. Only Team members may participate in discussions and vote on proposals and recommendations. The Chair and Vice Chair may request specific clarification from observers in order to assist the Team in understanding an issue. Observers/members of the public are welcome to speak during a public comment period that will be provided at each meeting, and all written comments submitted on the comment forms will be included in the Team and facilitators' summary reports.

To enhance the possibility of constructive discussions as members educate themselves on the issues and engage in consensus-building, members agree to refrain from public statements that may prejudge the outcome of the Team's consensus process. In discussing the Team process with the media, members agree to be careful to present only their own views and not the views or statements of other participants and/or may direct such inquiries to the Team Chair and Vice Chair. In addition, in order to provide balance to the Team process, members agree to represent and consult with their stakeholder interest group.

MEETING GUIDELINES FOR PARTICIPANTS

Participants' role in meetings:

- Explore possibilities
- Listen to understand (Respect) (limit sidebar conversations)
- Be focused and concise. (Avoid repetition. No need to offer comments in "strong agreement.")

- Focus on issues, not personalities.
- Offer options to address others' concerns.
- No sidebars.

Facilitators/Staff role in meetings:

- Assist the Chair and Vice Chair in helping the Team stay on task
- Help the group follow agreed upon ground rules
- Design the meeting and problem solving process in consultation with the Chair and Vice Chair
- Facilitate discussion participation of the Team and other participants
- Prepare agenda packets and reports

CONSENSUS BUILDING TECHNIQUES

- **Brainstorming.** (green light thinking — not judgmental) At certain points, the facilitator may ask the group to suspend judgment and get ideas onto the table before debating.

- **Name Stacking in Team Discussions.** This helps the facilitator determine the speaking order. Team and participants will raise name tent to speak. Facilitator(s) will call on participants in turn. The Facilitator(s) may interrupt the stack (change the speaking order) in order to promote discussion on a specific issue or, to balance participation and allow those who have not spoken on a issue an opportunity to do so before others on the list who have already spoken on the issue.

- **"Parking Lot" —** a list of issues that are raised but set aside to be addressed at a later time in the meeting or subsequent meeting.

- **Acceptability Consensus Ranking Scale**
  - Use a consensus acceptability scale to help focus discussion and test support in reviewing substantive issues.
  - Use to guide and focus discussion, not used as a voting mechanism. Rather it is a poll to see where folks are.
  - Must be prepared to offer refinements and suggestions to address serious concerns.

  4 = Proposal is acceptable as it is
  3 = Proposal is acceptable; I can live with it but there are minor concerns to address
  2 = Proposal is not acceptable. Proposal may be acceptable if the major concerns are addressed
  1 = Proposal is not acceptable

Appendix #7
Team Building- Go-Left/Go Right Exercise Results

"Go Left/Go Right"
Work Style Preferences

Team Members absent: Jay S. Cribb, Bryan Singer and William Winters

Detail Oriented	Big Picture Oriented
Jackie Collett, Tom Hofstetter, Kevin B. Perry, Scott Rosenberger, Kevin Sherlin, Keith Stouffer	Jack Bernhardsen, Jeri Domingo Brewer, Joe Doetzl, Sharon Edwards, Scott Fixmer, Gerald S. Freese, Philip Huff, John Lim, David L. Norton, David S. Revill, Jon Stanford, Steve Vandenberg, John D. Varnell, Michael Winters

People Focus	Task Focus
Jack Bernhardsen, Jackie Collett, Joe Doetzl, Sharon Edwards, Tom Hofstetter, Christopher A. Peters, Jon Stanford, Steve Vandenberg	Scott Fixmer, Gerald S. Freese, Philip Huff, John Lim, David L. Norton, Kevin B. Perry, David S. Revill, Scott Rosenberger, Keith Stouffer, Michael Winters

Middle: John D. Varnell,

Facts and Information	Intuition, Gut Feelings
Jack Bernhardsen, Jackie Collett Jeri Domingo Brewer, Jackie Collett, Joe Doetzl, Scott Fixmer, Tom Hofstetter, David Norton, Scott Rosenberger, Keith Stouffer, Jon Stanford, Steve Vandenberg	Sharon Edwards, Gerald S. Freese, Christopher A. Peters, Jon Stanford, Michael Winters

Middle: John D. Varnell,

Spontaneous, Flexible	Structured, Organized
Jack Bernhardsen, Gerald S. Freese, Philip Huff, John Lim, David L. Norton, Christopher A. Peters, John D. Varnell	Jeri Domingo Brewer, Jackie Collett, Joe Doetzl, Sharon Edwards, Scott Fixmer, Tom Hofstetter, Kevin B. Perry, David S. Revill, Scott Rosenberger, Kevin Sherlin, Keith Stouffer, Jon Stanford, Steve Vandenberg, Michael Winters

Outgoing, Talkative	Reserved, Reflective
Jackie Collett, Gerald S. Freese, David Norton, Kevin B. Perry, Kevin Sherlin, John D. Varnell	Jeri Domingo Brewer, Joe Doetzl, Sharon Edwards, Scott Fixmer, Tom Hofstetter, Philip Huff, Christopher A. Peters, David S. Revill, Keith Stouffer, Jon Stanford, Steve Vandenberg, Michael Winters

Middle: Scott Rosenberger

Tactical, Short Term	Strategic, Long Range
	Jack Bernhardsen, Jeri Domingo Brewer, , Joe Doetzl, Sharon Edwards, Scott Fixmer, Tom Hofstetter, Philip Huff, John Lim, David Norton, Kevin B. Perry, Christopher A. Peters, David S. Revill, Kevin Sherlin, Keith Stouffer, Jon Stanford, Steve Vandenberg, Michael Winters

Middle: Gerald S. Freese

Rule with Head	Rule with Heart
All	None

Afternoon Person	Morning Person
Jack Bernhardsen, David Norton, Christopher A. Peters, Kevin Sherlin, David S. Revill	Jeri Domingo Brewer, Jackie Collett, Joe Doetzl, Sharon Edwards, Scott Fixmer, Gerald S. Freese, Tom Hofstetter, Philip Huff, John Lim, David Norton, Kevin B. Perry, Scott Rosenberger, Keith Stouffer, Jon Stanford, Steve Vandenberg, John D. Varnell, Michael Winters

Sprit of the Law	Letter of the Law
Jack Bernhardsen, Jeri Domingo Brewer, Jackie Collett, Joe Doetzl, Sharon Edwards, Scott Fixmer, Gerald S. Freese Tom Hofstetter, Philip Huff, John Lim, David Norton, Kevin B. Perry, Scott Rosenberger, Keith Stouffer, Jon Stanford, Steve Vandenberg, Michael Winters	Jackie Collett, Scott Rosenberger, Kevin Sherlin, David S. Revill

Middle: John D. Varnell

Team Player	Individual Achiever
Jack Bernhardsen, Jeri Domingo Brewer, Joe Doetzl, Sharon Edwards, Scott Fixmer Tom Hofstetter, Philip Huff, David Norton, Kevin B. Perry, Scott Rosenberger, Keith Stouffer, Kevin Sherlin Jon Stanford, Steve Vandenberg, John D. Varnell, Michael Winters	Jackie Collett, Gerald S. Freese, John Lim, Scott Rosenberger

Focus on Results	Focus on Process
Jeri Domingo Brewer, Jackie Collett, Joe Doetzl, Sharon Edwards, Scott Fixmer, Gerald S. Freese, Tom Hofstetter, Philip Huff, David Norton, Keith Stouffer, Kevin Sherlin, Jon Stanford, Steve Vandenberg, John D. Varnell, Michael Winters	Jack Bernhardsen, John Lim, Kevin B. Perry, Scott Rosenberger,

Doer	Planner
Jack Bernhardsen, Jackie Collett, Sharon Edwards, Gerald S. Freese, John Lim, Kevin B. Perry, Scott Rosenberger, Keith Stouffer, Kevin Sherlin John D. Varnell, Michael Winters	Jeri Domingo Brewer, Joe Doetzl, Scott Fixmer, Tom Hofstetter, Philip Huff, David Norton, Jon Stanford, Steve Vandenberg

Confront Issues Directly	Handle Issues Indirectly
Jack Bernhardsen, Jackie Collett, Sharon Edwards, Scott Fixmer, Gerald S. Freese, Philip Huff, John Lim, David Norton, Kevin B. Perry, Scott Rosenberger, Jon Stanford, Steve Vandenberg, John D. Varnell, Michael Winters	Jeri Domingo Brewer, Joe Doetzl, Tom Hofstetter Keith Stouffer

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Meeting Agenda – Project 2008-06
Cyber Security Order 706 Standard Drafting Team

October 6, 2008 | 1–5 p.m. EST
October 7, 2008 | 8 a.m.–5 p.m. EST
October 8, 2008 | 8 a.m.–noon EST
National Institute of Standards & Technology
100 Bureau Drive
Gaithersburg, MD
Note: The conference call and WebEx information is provided in the table on page two.

Monday, October 6, 2008

1. **Opening Remarks — Michael Assante, CSO, NERC**
2. **Review NERC Antitrust Compliance Guidelines — Harry Tom**
3. **Welcome and Introductions — Jeri Domingo-Brewer and Kevin Perry**
4. **Overview of NERC Standards Development Process — Gerry Adamski and Dave Taylor**
5. **Review of CSO706 SAR — Dave Norton**

Tuesday, October 7, 2008

6. **Overview of NIST Risk Management Framework — Keith Stouffer**
7. **Comparison of NIST and NERC Cyber Standards — Keith Stouffer**
8. **Project Roadmap — Jeri Domingo-Brewer**

Wednesday, October 8, 2008

9. **Project Roadmap Wrap-up**
10. **Next Steps**
11. **Plan future meetings schedule**

Date	Conference Call Information	WebEx Information
Monday October 6, 2008 at 1:00 p.m. EST	Conf Call dial-in number (732) 694-2061 Conference Code: 12081006082	Topic: Cyber Security SDT Kickoff Meeting Meeting Number: 711 925 616 Meeting Password: standards
Tuesday, October 7, 2008 at 8:00 a.m. EST	Conf Call dial-in number (732) 694-2061 Conference Code: 12081007081	Topic: Cyber Security SDT Kickoff Meeting Meeting Number: 713 677 232 Meeting Password: standards
Wednesday, October 8, 2008 at 8:00 a.m. EST	Conf Call dial-in number (732) 694-2061 Conference Code: 12081008082	Topic: Cyber Security SDT Kickoff Meeting Meeting Number: 712 239 082 Meeting Password: standards

Selected Standard Drafting Team Resources:

FERC Order 706:
http://www.ferc.gov/whats-new/comm-meet/2008/011708/E-2.pdf

MITRE Technical Report: Addressing Industrial Control Systems in NIST Special Publication 800-53:
http://csrc.nist.gov/groups/SMA/fisma/ics/documents/papers/ICS-in-SP800-53_final_21Mar07.pdf

Applying NIST SP 800-53 to Industrial Control Systems:
http://csrc.nist.gov/groups/SMA/fisma/ics/documents/papers/Apply-SP-800-53-ICS-final-22Aug06.pdf

Managing Enterprise Risk in Today's World of Sophisticated Threats:
http://csrc.nist.gov/groups/SMA/fisma/documents/rmf-sz.pdf

NIST Framework Overview Presentation:
http://csrc.nist.gov/groups/SMA/fisma/documents/risk-framework-2007.pdf

NIST SP800 Series Document Home Page:
http://csrc.nist.gov/publications/PubsSPs.html

Guide to NIST Information Security Documents:
http://csrc.nist.gov/publications/CSD_DocsGuide.pdf

NIST FISMA Implementation Project Home Page:
http://csrc.nist.gov/groups/SMA/fisma/index.html

Other NIST Presentations and Papers (including some of these):

http://csrc.nist.gov/groups/SMA/fisma/ics/related_pubs.html

DHS Catalog of Control System Security: Recommendations for Standards Developers:
http://www.us-cert.gov/control_systems/pdf/Catalog_of_Control_Systems_Security_Recommendations.pdf

GAO Report on TVA FISMA Audit:
http://www.gao.gov/new.items/d08526.pdf

INL: A Comparison of Electrical Sector Cyber Security Standards and Guidelines:
http://www.us-cert.gov/control_systems/pdf/electrical_comp1004.pdf

INL: Recommended Practice: Creating Cyber Forensics Plans for Control Systems:
http://csrp.inl.gov/Documents/Forensics_RP.pdf

US-CERT Control System CERT Home Page:
http://www.us-cert.gov/control_systems/index.html

NERC

NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Project 2008-06
Cyber Security Order 706
Standard Drafting Team Kick-off Meeting

David Taylor

Manager of Standards Development

to ensure the reliability of the bulk power system

Meeting Agenda

- Steps in the Standards Development Process
- Expectations of the Standard Drafting Team
- Drafting a Standard
- References

Steps in Standards Development Process

Authorize Posting SAR

Post for Comment

Appoint SAR DT

Revise

Authorize Standard

Appoint SDT

Draft Standard

Post for Comment

Revise

Field Test

Ballot

Board Adopts

Regulatory Agencies Approve

Implement

Roles

- NERC Staff
  - Harry Tom
  - Scott Mix
  - Maureen Long
  - Others
- Chair (Jeri Domingo-Brewer)
- Vice-chair (Kevin Perry)
- Florida State University Conflict Resolution Consortium

Expectations of Standards Drafting Team

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

- Produce a technically sound, complete standard that meets stakeholder and regulatory authorities approval
- Produce a realistic implementation plan
- Preserve ‘open’ process

Drafting a Standard

- **Applicability** — functional entities required to comply and any facility limits
- **Requirements** — who must do what under what conditions for what outcome
- **Measures** — what will be reviewed to determine if entity is compliant
- **Violation Risk Factors** — impact to reliability of violating the requirement
- **Violation Severity Levels** — how badly an entity ‘missed’ being fully compliant with a requirement

Applicability

SDT must decide — do requirements apply to:

- All Transmission Owners?
- All Generator Owners?
- All Distribution Providers?
- Others?

Requirements

Tells — **Who** shall do **what** under what **conditions** for what **outcome**

R1. Within 10 calendar days of a notice from NERC that a BES Disturbance is under investigation, the TO shall submit the disturbance data recorded by its DMEs to NERC for disturbance analysis.

Requirements

- Written in ‘active voice’ (‘shall be’ is passive)
- Identify the responsible entity or entities
- Include a ‘shall’ statement
- Identify the ‘conditions’ under which the performance is required
- Identify the required performance or outcome
- Avoid:
  - ‘Negatives’
  - Ambiguous or subjective terms
  - ‘How’
- Must be measurable

Avoid Use of Ambiguous Words

- Adequate
- Data
- Immediately
- Timely
- Detailed
- Sufficient
- Comprehensive
- As appropriate
- Coordinate

Measures

- Each Requirement must have at least one measure to identify what will use to assess compliance
- Avoid requiring specific types of evidence unless that is the **only** way to demonstrate compliance

Violation Risk Factors (VRFs)

- Each Requirement must have an associated VRF
  - Sub-requirements **do not need individual VRFs**
- VRFs identify the reliability-related impact to the BES of violating a requirement
- VRFs are used to determine sanctions

Violation Severity Levels (VSLs)

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

- Violation Severity Levels (VSLs) tell how badly the entity ‘missed’ being fully compliant with a requirement or sub-requirement
- VSLs do not identify importance of a violation
- VSLs do not identify reliability-related impact of a violation
- Each requirement needs a set of violation severity levels

Ready to Post?

- Did the drafting team address all issues identified in Issues Database?
- Does the standard meet NERC's benchmarks for reliability standards?

Implementation Plan

- Tells stakeholders how and when the standard will be implemented and identifies:
  - Any prerequisites for implementation — such as another standard that needs to be implemented first
  - Any already approved standards that should be modified as a result of the proposed standards
  - Functions that must comply
  - When entities must be compliant
  - Reasons for any recommended delay in implementation such as time to develop procedures, time to provide training, or to modify software

Comment Forms

- Ask very pointed questions
- Ask only questions that will result in responses that you will use
- If you've made changes, ask for feedback
- If you've defined terms, ask for feedback on the terms
- Ask for feedback on implementation plan
- Ask if field testing is needed

Responding to Comments

- Read through comments to get a ‘sense’ of stakeholders’ reactions
- Consider & respond to every comment
  - Responses must be respectful
  - Responses should provide a justification
- Develop a ‘summary response’ to each question
- Make conforming changes to the standard
- Can’t expand scope of SAR but can develop a standard that is smaller than the scope of the SAR

References

- Reliability Standards Development Plan — Volume I
- Reliability Standards Development Procedure
- Standard Drafting Team Guidelines

Questions?

NERC

NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Cyber Security Standards: Development Proposal

Scott Mix, CISSP

Manager of Situation Awareness and Infrastructure Security

SDT Kickoff Meeting

NIST Headquarters

October 6, 2008

to ensure the reliability of the bulk power system

VSL Development

- VSLs now required for each requirement of a standard (currently also for sub-requirements)
- Project Team to complete VSLs for approved (existing) standards has formed
- Announcement at September 22-23, 2008 Standards Committee meeting
- Note: VSL (and VRF) development for revised standards will be developed by SDT as part of the normal standard development process (this process)

CIP Auditor Training

- NERC is developing training for NERC and Regional compliance auditor staff
  - Restricted to NERC and Regional Compliance Audit staff
- Multiple training sessions have been scheduled for the remainder of this year, and early next year

Future Plans

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

- All very tentative pending discussions with SDT
  - Meet Face-to-Face every other week ~2 – 3 days
  - Teleconference / WebEx capability at meetings
  - Proposing 3 (3+) phases
    1. “Low Hanging Fruit”, high priority items
    2. Majority of issues
    3. Large, challenging issues

       3+ Extremely large and challenging issues
- Guidelines will need to be addressed

Development Schedule

- Three development phases
  1. Low Hanging Fruit and High Priority Items
     - "Easy" and "Need-to-do" issues
     - Complete to Commission in 6 months (March, 2009)
  2. Majority of Issues
     - Not hard, but lots of them
     - Complete and to Commission 18 months following #1 (October 2010)
  3. Challenging Issues
     - Expect difficulty in reaching consensus
     - Following #2 (exact time depends on how many and how hard)

Guidelines

- FERC Order 706 provides for the development of reference documents (guidelines) to assist with compliance
  - Guidelines are not Standards nor Requirements
  - Compliance with a guideline is optional
- About 25 guideline topics have been identified in the order
- The SDT will need to determine whether a topic should be addressed through a guideline, modifications to the requirements of a standard, or both
  - Choice must be made on a topic by topic basis
  - Guideline development will be controlled by the SDT's decision on these options

Process

- Develop modifications to Standards Language
  - Requirements, Measures, etc
- Develop VRF / VSL for requirements
  - Effort for existing standards as a starting point
- Develop implementation timeline and effective date
  - Less complicated than existing implementation plan
  - Tie to FERC approval date?
  - Tie to existing implementation plan timeline?
- Industry review and comment
- Industry Ballot
- BoT Approval
- Submit to Commission

Low-Hanging Fruit

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

- Mostly non-contentious issues
- Initial edits “easy”
  - But final language may not be
- NERC Staff proposal for consideration by the SDT
- Other areas may be added so long as they do not adversely effect the schedule

Phase 1 schedule

- Working backwards:
  - Submit to Commission (end of) March 2009
  - BoT approval March 23
  - BoT notice Feb 20 (30 days)
  - Second Ballot Feb 5 (includes responses to comments)
  - First Ballot Jan 15
  - Ballot posting Dec 15 (30 days) (includes responses to comments)
  - Draft to industry for comments on October 30 (45 days)
- May be able to cut back on some posting timeframes (but not all)

Need-to-do issues

- Reasonable Business Judgment
  - NERC Staff edit to remove sentence in all standards
- Critical Asset Identification
  - Needs work
  - See Critical Asset Identification Guideline for ideas
- Risk Acceptance / Technical Feasibility
  - Needs Work
  - NIST Framework for ideas
  - NERC Filings to FERC for ideas

Low Hanging Fruit

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

- Proposed edits done by NERC Staff
  - Minor formatting (version numbers, etc)
  - Removal of “Reasonable Business Judgment” language from all standards
  - Change “Regional Reliability Organization” to “Regional Entity”
    - Question: do we need to keep both?
  - No work preformed on Measures or Compliance sections

Low Hanging Fruit

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

- CIP-002
  - Newly identified Critical Assets
  - Newly identified Critical Cyber Assets
  - Senior Manager approval of Risk-based Asset Identification Methodology
  - Reliability Coordinator approval of lists

Low Hanging Fruit

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

- CIP-003
  - Clarification of who the Senior manager is
  - Senior Manager Delegation process
  - Escorting clarification

Low Hanging Fruit

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

- CIP-004
  - “Implement” awareness and training programs
  - Clarification for training program
  - Train prior to access
  - Additional mandatory elements of training program
  - PRA prior to access
  - PRA clarifications for new hires and emergencies

Low Hanging Fruit

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

- CIP-005
  - Implement secure dial-up procedure
  - Update documentation in 30 days (from 90)

Low Hanging Fruit

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

- CIP-006
  - Implement Physical Security plan and physical security procedures
  - Update procedures in 30 days (from 90)

Low Hanging Fruit

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

- CIP-007
  - Implement procedures
  - Update documentation in 30 days (from 90)

Low Hanging Fruit

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

- CIP-008
  - Implement procedures
  - Update procedures in 30 days (from 90)
  - Procedures for when documented procedures are not followed
  - Update of response plans for new situations
  - Clarification on testing – not required to remove equipment from service to test

Low Hanging Fruit

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

- CIP-009
  - Update procedures in 30 days (from 90)
  - Procedures for when documented procedures are not followed
  - Update of response plans for new situations

Need-do-do Issues

- Edits *not* performed by NERC staff:
  - Critical Cyber Asset identification updates (CIP-002)
  - Technical Feasibility and Risk Management (CIP-003)
- Work teams and schedules need to be developed at this meeting

Majority of Issues

- Lots of issues
  - List available
  - Everything that is neither a “Low Hanging Fruit” issues nor a “challenging” issue
- May include sub-phases
- Items may move into phase 3 if consensus cannot be reached in allocated timeframe
- Can start tackling some now if resources available

Challenging Issues

- May have 2 sub-phases
  - Will be based on SDT resource and industry comment
- Will include issues that we can't come to consensus with in phase 2
- Will take time to reach consensus in SDT
  - Will take longer to reach industry consensus
- Can start at any time (pending resources)
  - Should not hold up our ability to submit at the 18-month development milestone for phase 2

Challenging Issues

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

- Proposed list of Phase 3 issues:
  - Design Basis Threat (258) **
  - Misuse of control centers (282)
  - Non-routable protocols (285)
  - “immediate” revocation of access privileges (460, 461)
  - Two or more defensive measures in a defense in depth posture when constructing an electronic security perimeter (496, etc)

** -- may be a Phase “3+”

Challenging Issues

- Exception process and demonstration of untolerable delays for defense in depth electronic security perimeter (498)
- Fail-safe defensive measures (500)
- Specific verification technologies, authentication technology in general (511)
- Use of encryption (511)
- Log review processes, response to log review alerts, log sampling (525 - 528)

Challenging Issues

- Vulnerability Assessments (541, 543, 544, 547)
- “Full live vulnerability Assessments” (542) **
- “Two or more different security procedures when establishing a physical security perimeter” (572 - 575)
- Test environment requirements (609 - 611)
- Safeguards against introduction of malware (621, 622)
- Log review procedures (628, 629)

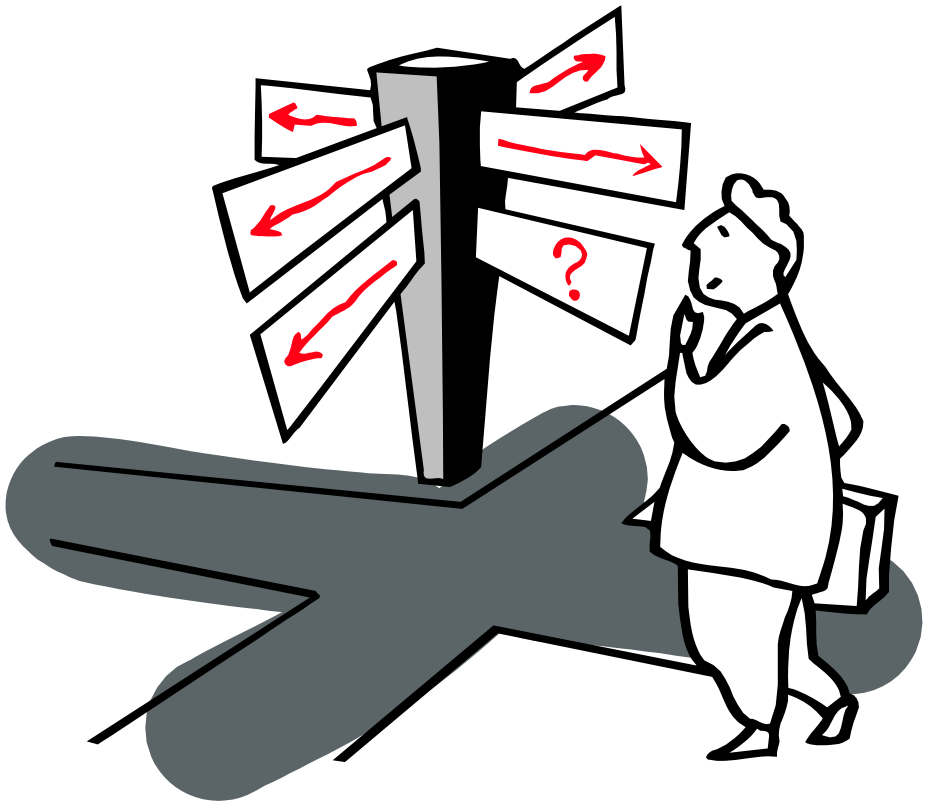
** -- may be a Phase “3+”

Challenging Issues

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

- Vulnerability Assessments (643)
- Incident reporting (661)
- Mandatory government reporting (673, 675)
- Report time requirements (674, 676)
- Relationship between CIP-001 and CIP-008 (677)
- Forensic data practices (706 – 710)
- Recovery exercises (725)
- Backup, storage, testing of media (739 – 740, 748)

Questions



Scott Mix, CISSP
Manager of Situation Awareness
and Infrastructure Security
Scott.Mix@NERC.net
215-853-8204

NIST Objectives

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

- Describe the NIST Risk Management Framework and related NIST standards and guidelines (hereafter referred to as the "RMF model")
- Present our understanding of the NERC CIP model
- Compare the RMF model with the NERC CIP model
- Explore harmonizing the NERC CIPs with NIST SP 800-53, Rev 2 Moderate Baseline
- Suggest modifications to the NERC CIPs
- Assist NERC in adopting the modifications, if requested

Setting the Stage

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

- Attempting to do a fair analysis and comparison of the two approaches
- Acknowledge we may not have full understanding of the NERC approach/model — encourage discussion on this topic as we more forward
- Want to provide NERC drafting committee with a better understanding of the NIST approach/model
- Share insights learned performing analysis/comparison of the two approaches
- Committee decides on direction of the modified CIPs
- NIST is ready to help if the committee wishes to incorporate any of the NIST approach into the CIPs

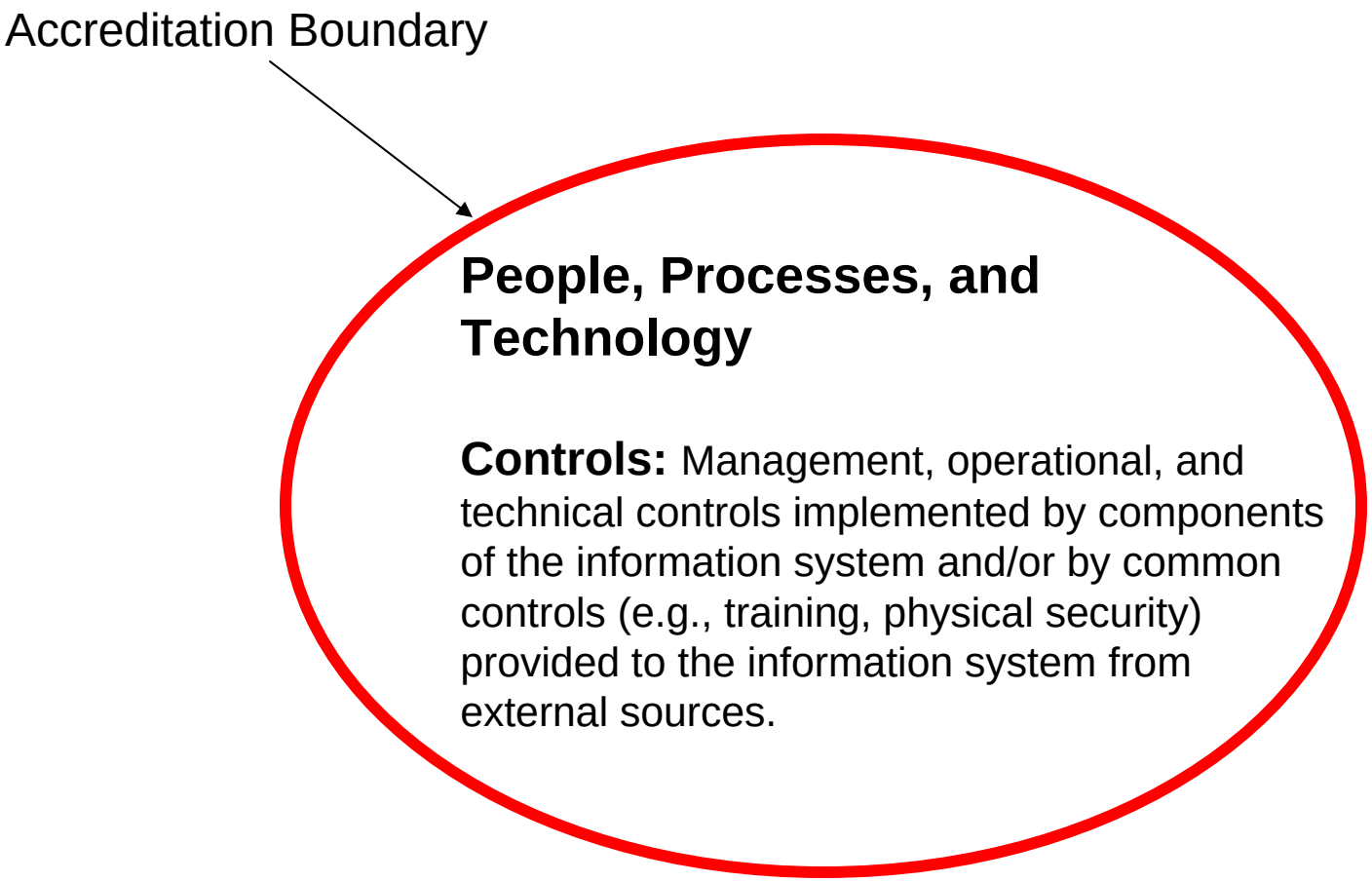
NIST Risk Management Framework

Terms from the NIST Glossary:

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

- **Information System:** [44 U.S.C., Sec. 3502][OMB Circular A-130, Appendix III] A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. [Note: Information systems consist of people, processes, and technology.]
- **Accreditation (authorization to operate):** [FIPS 200, NIST SP 800-37] The official management decision given by a senior agency official to authorize operation of an information system and to explicitly accept the risk to agency operations (including mission, functions, image, or reputation), agency assets, or individuals, based on the implementation of an agreed-upon set of security controls.
- **Certification (assessment of security controls):** [FIPS 200, NIST SP 800-37] A comprehensive assessment of the management, operational, and technical security controls in an information system, made in support of security accreditation, to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system.
- **Accreditation Boundary:** [NIST SP 800-37] All components of an information system to be accredited by an authorizing official and excludes separately accredited systems, to which the information system is connected. Synonymous with the term security perimeter defined in CNSS Instruction 4009 and DCID 6/3.

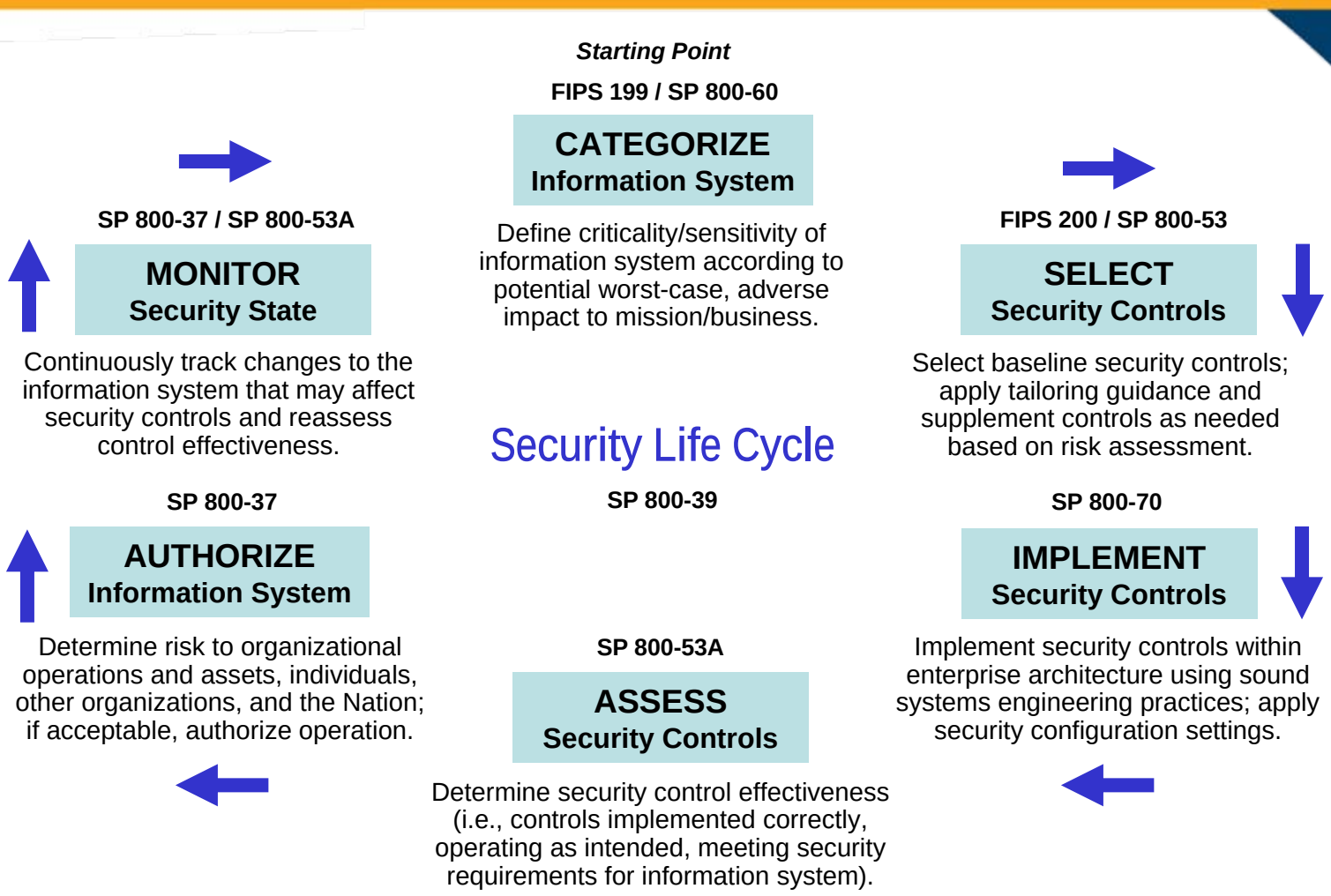
Information System



NIST Risk Management Framework

- The information/control system under consideration is defined by the accreditation boundary.
- All information system components are within the logical boundary (i.e., there are no information system components on the boundary, unlike the ESP boundary defined in the CIPs).
- Selected security controls from SP 800-53 (i.e., requirements) are satisfied by the information system components and/or by common controls.
- Common controls (e.g., training, physical security) are provided to the information system from external sources.
- Security controls are implemented within the components of the information system as determined (i.e., allocated) by the system design and engineering
- Security controls are not expected to be implemented in every component of the information system, unlike the CIPs.

Risk Management Framework



Important Concepts within the RMF

- Information system focus, including accreditation boundary concept (all components of the information system are within the accreditation boundary)
- Risk management framework defines overall risk management process to be followed for an information system
- Categorization of potential impact required (Low, Moderate, High)
- Level of rigor is based on categorization
- Information system control selection includes baseline, tailoring, and supplementation based on risk assessment
- Security Plan required for each information system
- Security controls are implemented:
  - Within the components of the information system as determined (i.e., allocated) by the system design and engineering
  - By common controls (e.g., training, physical security) provided to the information system from external sources.

Important Concepts within the RMF

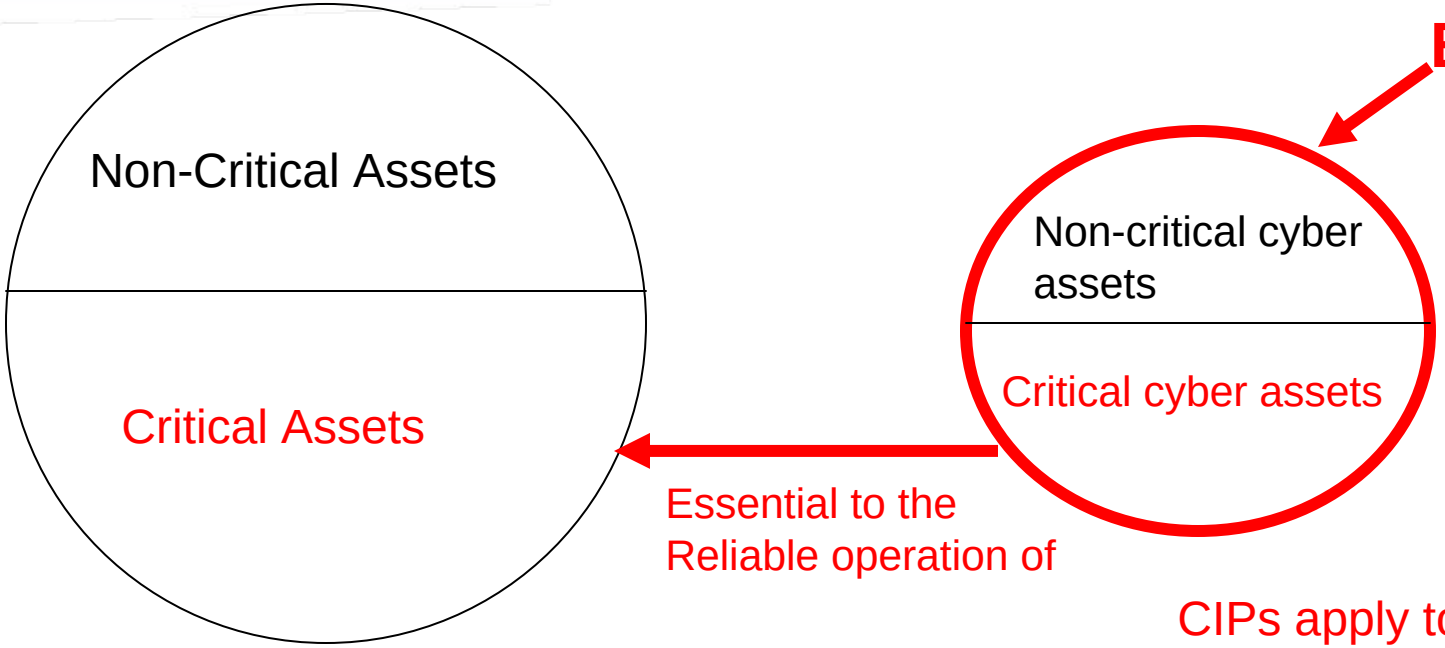
- Security assessment plan is required
  - Control-specific assessment procedures are defined
  - Assessment of controls by independent assessor
- Organization official authorizes system operation based on acceptance of residual risk
- Continuous monitoring of the status of security controls and system configuration changes
- Addresses trust model and trust relationships with business partners and external service providers

NERC and CIP Model

Terms from the NERC Glossary:

- **Assets:** Facilities, systems, and equipment
- **Critical Assets:** Facilities, systems, and equipment which, if destroyed, degraded, or otherwise rendered unavailable, would affect the reliability or operability of the Bulk Electric System.
- **Cyber Assets:** Programmable electronic devices and communication networks including hardware, software, and data.
- **Critical Cyber Assets:** Cyber Assets essential to the reliable operation of Critical Assets.

CIP Model



Assets: Facilities, systems, and equipment

Critical Assets: Facilities, systems, and equipment which, if destroyed, degraded, or otherwise rendered unavailable, would affect the reliability or operability of the Bulk Electric System.

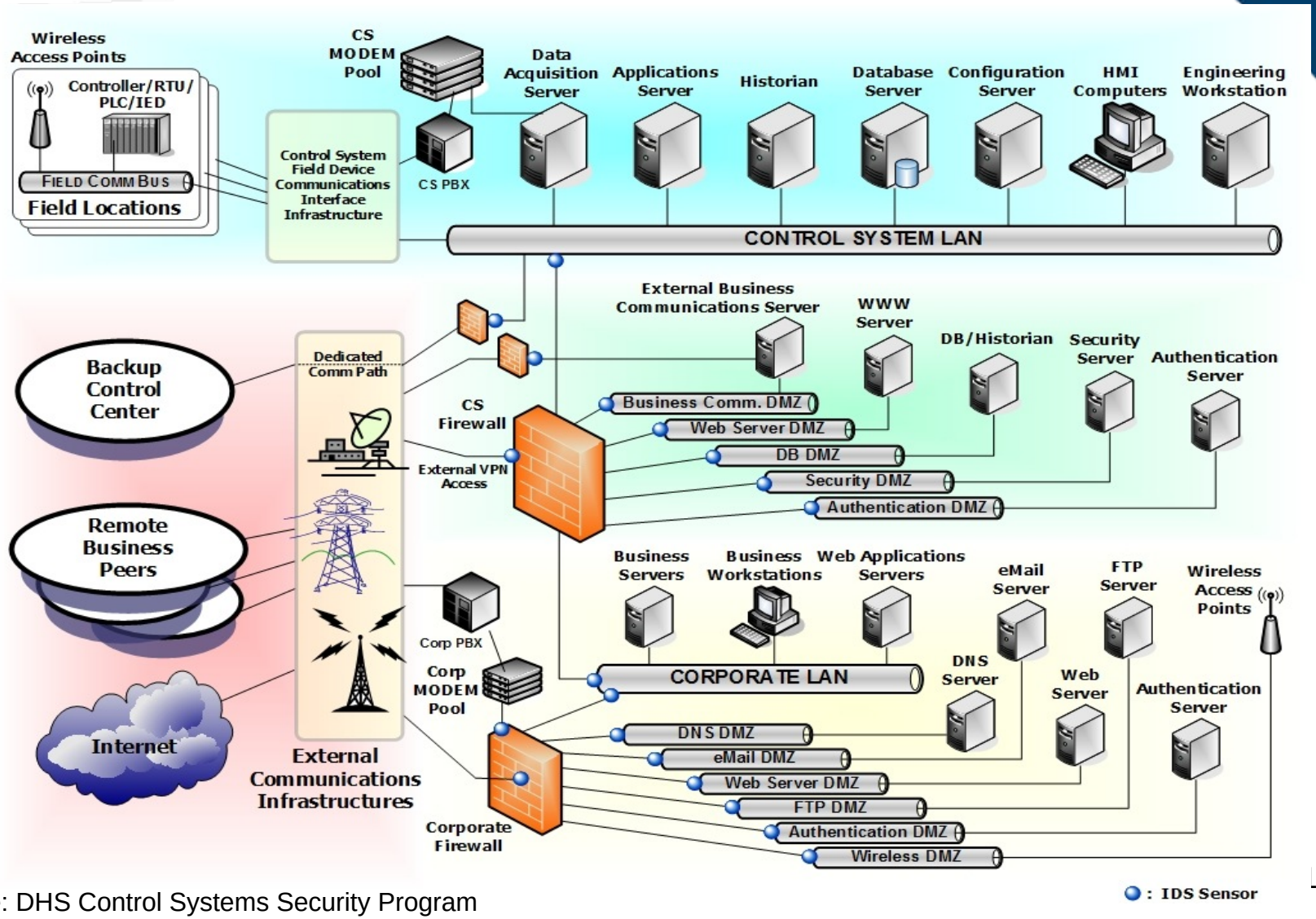
CIPs apply to the ESP and cyber assets within the ESP

The ESP contains critical cyber assets and, possibly non-critical cyber assets.

CIP Applicability

- ESP (CIP 005)
- Cyber assets within the ESP (CIP 007)
- Support of cyber assets
  - Security management (CIP 003)
  - Personal & training (CIP 004)
  - Physical security (CIP 006)
  - Incident reporting & response planning (CIP 008)
  - Recover plans for critical cyber assets (CIP 009)

Generic Control System Model



Source: DHS Control Systems Security Program

Electronic Security Perimeter

- The logical border surrounding a network to which Critical Cyber Assets are connected and for which access is controlled.
  - CIP-005 R.1 & R1.4 imply that an ESP contains both critical and non-critical cyber assets
  - Critical and non-critical cyber assets within an ESP are under the control of the Responsible Entity (RE).

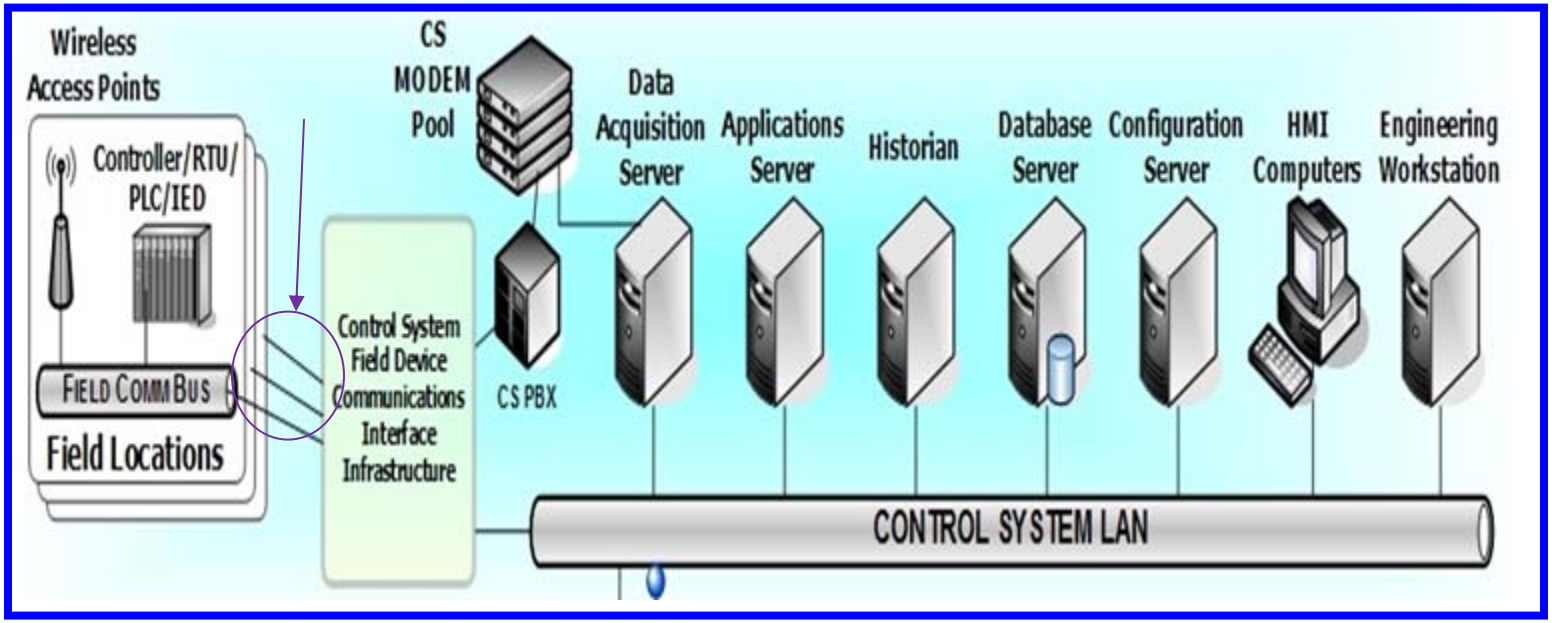
R1. Electronic Security Perimeter — The Responsible Entity shall ensure that every Critical Cyber Asset resides within an Electronic Security Perimeter. The Responsible Entity shall identify and document the Electronic Security Perimeter(s) and all access points to the perimeter(s).

R1.4. Any non-critical Cyber Asset within a defined Electronic Security Perimeter shall be identified and protected pursuant to the requirements of Standard CIP-005.

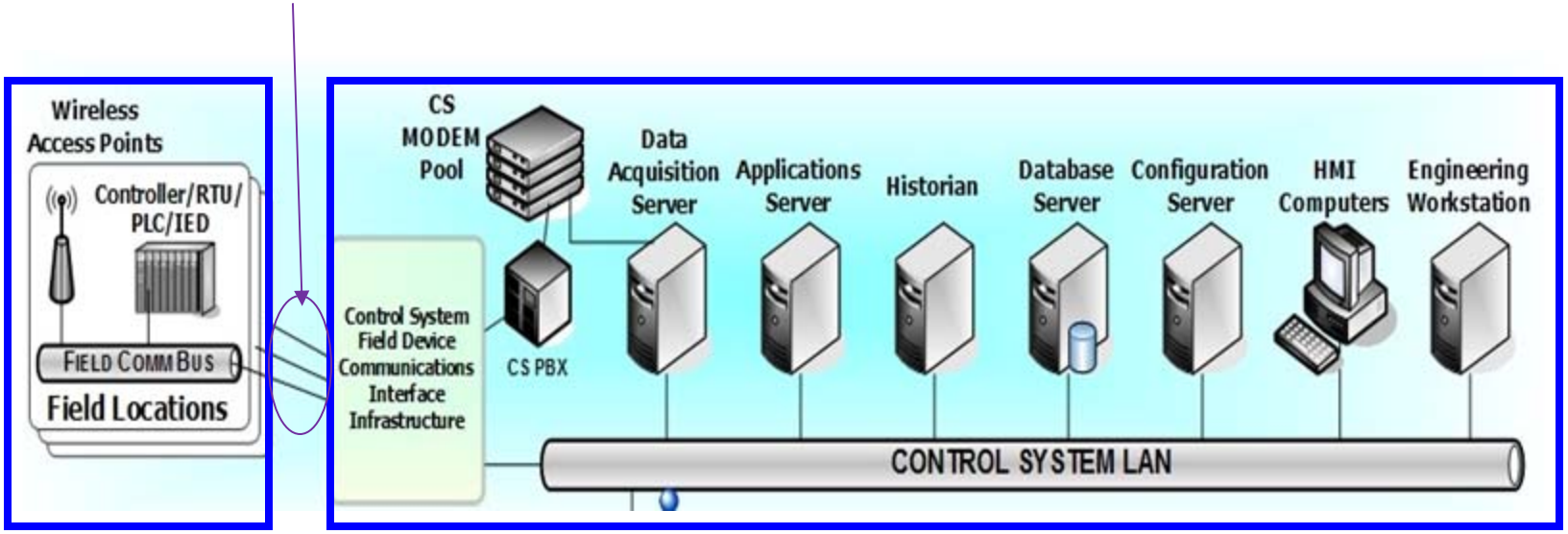
Determining the ESP (or ESPs) in the Generic Control System Model.

Are all of the following reasonable ESP configurations?

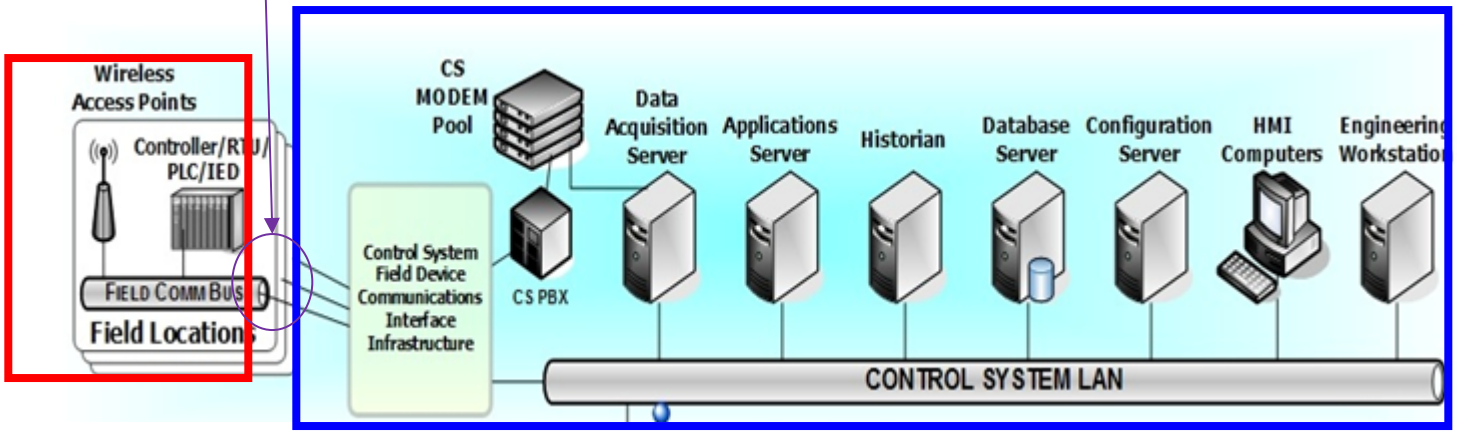
One ESP: All cyber assets, including the communication paths, are under the control of the Responsible Entity (RE)



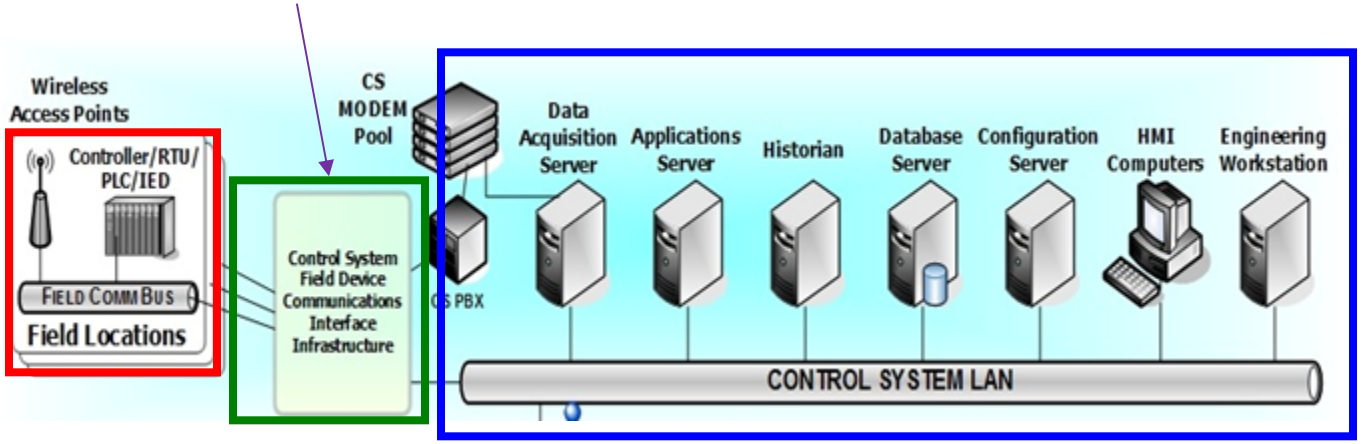
One ESP: All cyber assets, except the communication paths, are under the control of the Responsible Entity (RE)



Two ESPs: The ESPs are under the control of different REs. The communications paths are not under the control of either RE.



Three ESPs: The communications are in an ESP. Each ESP is under the control of a different RE.



Compare NIST & the NERC/CIP approach

Similarities

- Holistic approaches: both address technology, management & operational aspects of security
- Concepts of external/internal to boundary (ESP & accreditation boundary)

Conceptual Model Differences

- NIST
  - Information system view
  - All information system components are within accreditation boundary, including people, processes, and technology
  - Security requirements are allocated to components
  - Allows holistic defense-in-depth approach through system design & engineering
- NERC
  - Critical asset, cyber asset, & critical cyber asset view
  - Concept of protecting perimeter (i.e., ESP) & contents within ESP; contents only include cyber assets. People & processes addressed by additional CIPs.
  - Security requirements are applied to all components (i.e., all cyber assets)
  - Treating boundary and contents separately (e.g., in CIPs 5 & 7) can lead to inefficiency, inconsistency, and vulnerabilities

Additional Differences

- RMF concepts
  - Management of risk vs. compliance with requirements (CIPs)
  - Categorization of potential impact (Low, Moderate, High)
  - Security plan
  - Security testing and evaluation procedures and methods
  - Authorization to operate
  - Continuous Monitoring
  - Common controls
  - Trust model as basis for trust between business partners & external service providers
- Wireless not addressed in CIPs

Explore Harmonizing the NERC CIPs with NIST's Moderate Baseline

- Add material to make the NERC CIPs comparable to NIST's Moderate baseline
  - Policy requirement to each CIP
  - Guidance
  - Augment CIP requirements
  - Security Test and Evaluation
- Replace the concept of technical feasibility with an exception process
- Merge CIPs 005 & 007

Example of CIP Augmentation

- Process followed
  - Examined mapping exercise results
  - Reviewed CIP 005 & 800-53 Moderate baseline to identify gaps
  - Added material to existing requirements or added new requirements to close gaps
- Provide CIP 005 augmentation example to NERC development team
- Assist NERC in augmenting remaining CIPs, if requested

Example CIP-005 Policy Requirement

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

B. Requirements

R0. Cyber Security Perimeter Policy and Procedures — The Responsible Entity shall: develop, disseminate, and periodically review update: (i) a formal, documented, policy on the protection of all Cyber Security Perimeter(s), the cyber assets contained within, and identification and authentication. This policy shall address purpose, scope, roles, responsibilities, management commitment, coordination among Responsible Entity's sub-entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of this policy and associated controls.

GUIDANCE: this requirement does not prescribe an organization structure for the Responsible Entity 's cyber security policy. The Cyber Security Perimeter Policy and Procedures may be included as part of the general information security policy for the Responsible Entity, or the ICS cyber security policy.

CIP-005
B. Requirements

R0. Policy and Procedures

R1. Electronic Security Perimeter

R2. Electronic Access Controls

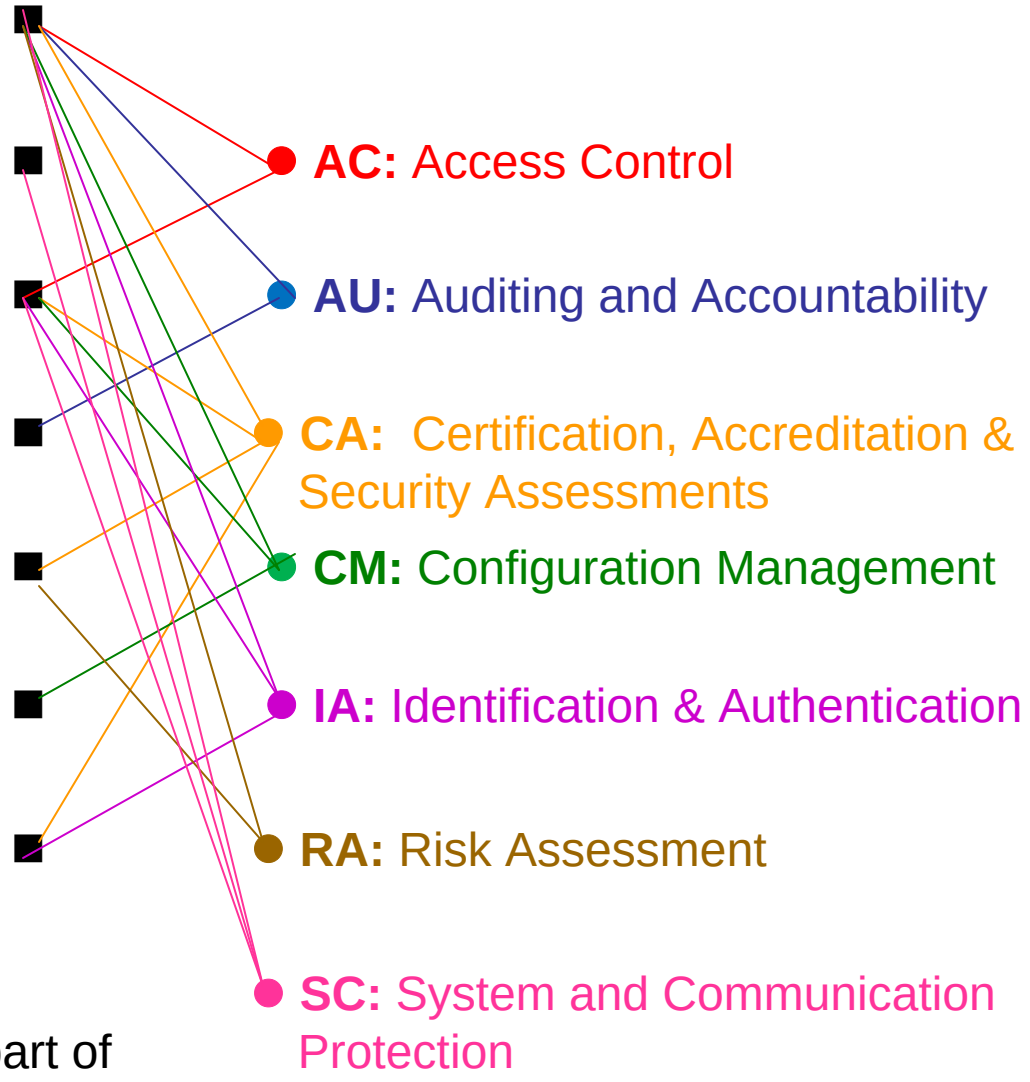
R3. Monitoring Electronic Access

R4. Cyber Vulnerability Assessment

R5. Documentation Review and Maintenance

R6. Identification and Authentication

NIST SP 800-53
Relevant Control Families



——— Indicates controls (or part of controls) added to CIP requirement

CIP-005
B. Requirements

R0. Policy and Procedures

R1. Electronic Security Perimeter

R2. Electronic Access Controls

R3. Monitoring Electronic Access

R4. Cyber Vulnerability Assessment

R5. Documentation Review and Maintenance

R6. Identification and Authentication

——— Indicates controls (or part of controls) added to CIP requirement

NIST SP 800-53
Access Control

- AC-1 Access Control Policy and Procedures
- AC-2 Account Management
- AC-3 Access Enforcement
- AC-4 Information Flow Enforcement
- AC-5 Separation of Duties
- AC-6 Least Privilege
- AC-7 Unsuccessful Login Attempts
- AC-8 System Use Notification
- AC-9 Previous Logon Notification
- AC-10 Concurrent Session Control
- AC-11 Session Lock
- AC-12 Session Termination
- AC-13 Supervision and Review—Access Control
- AC-14 Permitted Actions without Identification or Authentication
- AC-15 Automated Marking
- AC-16 Automated Labeling
- AC-17 Remote Access
- AC-18 Wireless Access Restrictions
- AC-19 Access Control for Portable and Mobile Devices
- AC-20 Use of External Information Systems

CIP-005
B. Requirements

R0. Policy and Procedures

R1. Electronic Security Perimeter

R2. Electronic Access Controls

R3. Monitoring Electronic Access

R4. Cyber Vulnerability Assessment

R5. Documentation Review and Maintenance

R6. Identification and Authentication

NIST SP 800-53
Identification & Authentication

IA-1 Identification and Authentication Policy and Procedures

IA-2 User Identification and Authentication

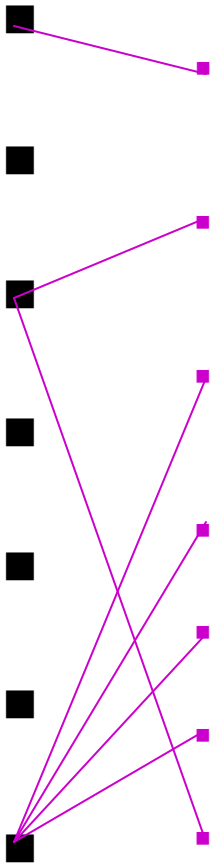
IA-3 Device Identification and Authentication

IA-4 Identifier Management

IA-5 Authenticator Management

IA-6 Authenticator Feedback

IA-7 Cryptographic Module Authentication



Indicates controls (or part of controls) added to CIP requirement

CIP-005
B. Requirements

R0. Policy and Procedures

R1. Electronic Security Perimeter

R2. Electronic Access Controls

R3. Monitoring Electronic Access

R4. Cyber Vulnerability Assessment

R5. Documentation Review and Maintenance

R6. Identification and Authentication

NIST SP 800-53
Configuration Management

CM-1 Configuration Management Policy and Procedures

CM-2 Baseline Configuration

CM-3 Configuration Change Control

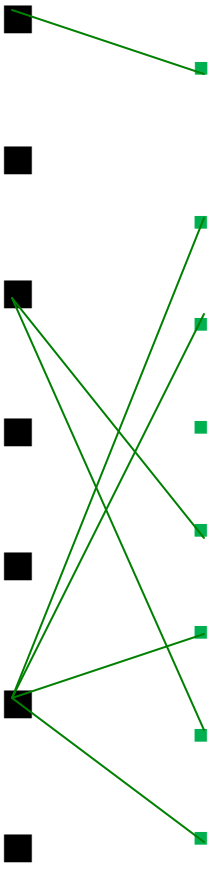
CM-4 Monitoring Configuration Changes

CM-5 Access Restrictions for Change

CM-6 Configuration Settings

CM-7 Least Functionality

CM-8 Information System Component Inventory



Indicates controls (or part of controls) added to CIP requirement

CIP-005
B. Requirements

R0. Policy and Procedures

R1. Electronic Security Perimeter

R2. Electronic Access Controls

R3. Monitoring Electronic Access

R4. Cyber Vulnerability Assessment

R5. Documentation Review and Maintenance

R6. Identification and Authentication

NIST SP 800-53
Auditing and Accountability

- **AU-1** Audit and Accountability Policy and Procedures
- **AU-2** Auditable Events
- **AU-3** Content of Audit Record
- **AU-4** Audit Storage Capacity
- **AU-5** Response to Audit Processing Failures
- **AU-6** Audit Monitoring, Analysis, and Reporting
- **AU-7** Audit Reduction and Report Generation
- **AU-8** Time Stamps
- **AU-9** Protection of Audit Information
- **AU-10** Non-repudiation
- **AU-11** Audit Record Retention

——— Indicates controls (or part of controls) added to CIP requirement

CIP-005
B. Requirements

- **R0.** Policy and Procedures
- **R1.** Electronic Security Perimeter
- **R2.** Electronic Access Controls
- **R3.** Monitoring Electronic Access
- **R4.** Cyber Vulnerability Assessment
- **R5.** Documentation Review and Maintenance
- **R6.** Identification and Authentication

NIST SP 800-53
Risk Assessment

- **RA-1 Risk Assessment** Policy and Procedures
- **RA-2** Security Categorization
- **RA-3** Risk Assessment
- **RA-4** Risk Assessment Update
- **RA-5** Vulnerability Scanning

——— Indicates controls (or part of controls) added to CIP requirement

CIP-005
B. Requirements

R0. Policy and Procedures

R1. Electronic Security Perimeter

R2. Electronic Access Controls

R3. Monitoring Electronic Access

R4. Cyber Vulnerability Assessment

R5. Documentation Review and Maintenance

R6. Identification and Authentication

NIST SP 800-53
SC: System and Communication Protection

SC-1 System and Communication Protection Policy and Procedures

SC-7 Boundary Protection

SC-9 Transmission Confidentiality

Indicates controls (or part of controls) added to CIP requirement

CIP-005
B. Requirements

R0. Policy and Procedures

R1. Electronic Security Perimeter

R2. Electronic Access Controls

R3. Monitoring Electronic Access

R4. Cyber Vulnerability Assessment

R5. Documentation Review and Maintenance

R6. Identification and Authentication

NIST SP 800-53
Certification, Accreditation, and Security Assessments

- **CA-1** Configuration Management Policy and Procedures
- **CA-2** Security Assessments
- **CA-3** Information System Connections
- **CA-4** Security Certification
- **CA-5** Plan of Action and Milestones
- **CA-6** Security Accreditation
- **CA-7** Continuous Monitoring

——— Indicates controls (or part of controls) added to CIP requirement

Security Assessment Suggestions

- Add a new security assessment requirement based on:
  - SP 800-53 CA-2 Security Assessments
  - SP 800-53A Section 3.2 contains security assessment requirements
- **Example requirement:** Responsible Entity must develop detailed information security testing standards, processes, and procedures that provide direction and guidance on security testing.
  - See example augmented CIP-005 R4 for additional details
- SP 800-53A *Guide for Assessing the Security Controls in Federal Information Systems* can serve as the basis for selection and tailoring of processes and procedures.

Suggestion for Replacing “Technical Feasibility” with an “Exception Process”

- The Responsible Entity may take exception to any Requirement based on specified conditions. See example augmented CIP-005 Section A.6 for details
- The Responsible Entity shall document all exceptions in an Exception Plan provided to the ERO and Regional Reliability Organization.
- The Exception Plan must be approved annually by a Responsibility Entity senior manager.
- The Exception Plan must be approved annually by the Regional Reliability Organization, or the ERO if there is no applicable RRO.
- The ERO must annually audit compliance with the Exception Plan and provide FERC with an annual high-level, wide-area analysis regarding the effects of all exceptions on the reliability of the Bulk-Power System.

Merge CIP-005 & CIP-007

- CIP-005 R4 and CIP-007 R8 are quite similar.
  - CIP-005 addresses the perimeter
  - CIP-007 addresses the contents of the perimeter.
- Treating perimeter and contents separately can lead to inefficiency, inconsistency, and vulnerabilities

NIST Standards Development Process

A Partnership Between Government and Industry

Keith Stouffer
National Institute of Standards and Technology

US Federal Standards and Guidelines

- Measurement standards
  - Length
  - Mass
  - Time
  - Ohm
  - Etc.
- Principle-based and prescriptive standards and guidelines
  - Federal Information Processing Standards (FIPS)
  - Special Publication (SP) 800 Series documents
- NIST does not perform enforcement – Government Accountability Office (GOA) and Inspector Generals (IGs)

Federal Information Standards (FIPS)

- Approved by the Secretary of Commerce
- Compulsory and binding standards for federal agencies non-national security information systems
- Voluntary adoption by federal national security community and private sector
- Examples
  - FIPS 140-2 Security Requirements for Cryptographic Modules
  - FIPS 200 - Minimum Security Requirements for Federal Information and Information Systems

Special Publication (SP) 800 Series Documents

- Special Publications in the 800 series are documents of general interest to the computer security community, established in 1990
- Reports on guidance, research, and outreach efforts in computer security, and collaborative activities with industry, government, and academic organizations
- Documents receive 3 public vetting cycles before being finalized
  - Initial public draft - 90 day review period
  - 2nd public draft - 60 day review period
  - Final public draft - 30 day review period
- Agencies must follow 800 series guidance documents, but 800 series documents generally allow agencies latitude in their application
- Voluntary adoption by private sector – heavily used
- FIPS may mandate specific 800 series documents
  - FIPS 200 mandates NIST SP 800-53 security controls

NIST Approach to Standards Development

- NIST standards only apply to non-national security part of US government (USG)
- NSA standards apply to the national security part of the USG (i.e., classified systems, intelligence-related systems)
- Use of NIST standards is mandatory by government agencies; guidelines require mandatory “consideration”
- Use of NIST standards and guidelines is always voluntary by the commercial sector

NIST Approach to Standards Development

- In order of priority:
  - Adopt or adapt existing voluntary industry standards, if available and acceptable
  - Join voluntary industry standards efforts to develop common government-industry standards; adopt or adapt the completed standard for government use.
  - Use NIST mandated authority and internal resources to develop standards and guidelines for federal agencies

NIST Approach to Standards Development

- Seek heavy commercial sector involvement
- Attempt to develop “dual use” standards
  - Appropriate for use by government & industry
  - Contributions to voluntary standards groups (IEEE, ISO)
- Accept technical contributions from all parties
- Hold open workshops & public briefings
- Have open public comment periods
- Revisions based on public comments
- International coordination & cooperation
  - For example: Japan & India

Why This Approach?

- 90% of critical infrastructure (CI) is owned by the private sector
- All systems within a CI need appropriate, consistent, & comparable protection-should be seamless protection across government & private CI systems
- Government approach is to encourage private sector to strengthen its CI protection
- Private sector is more likely to adopt standards and guidelines if these are developed in an open consensus environment

Why This Approach?

- Product developers are more likely to implement/meet standards if developed in an open consensus environment (e.g., DES, AES, FIPS 140) due to larger market
- Results in larger selection of products for all sectors to chose from
- Results in best possible/stronger standards
  - Wide diversity of technical advice
  - Realistic view of what is technically feasible

Why This Approach?

- Often considered as “best practice” or “due diligence” by private sector
  - “Good enough for government is good enough for us”
  - Promoted through government CI sector liaisons to their CI counterparts
- Better interoperability between government & private sector systems
- Provides general public/citizens with visibility & comfort into how the government is protecting systems that contain personal/private information about them

Consensus-Building Process

NIST Special Publication 800-53

- Employ extensive vetting process for Special Publication 800-53
  - Three full published drafts of document
  - Three public comment periods to obtain feedback from the public and private sectors
- Carefully assess feedback received during the public comment periods; incorporate material into publication, as appropriate
- Provide sufficient time for organizations to become familiar with Special Publication 800-53 before transitioning to FIPS 200

Special Publication 800-53

- Formal and informal comments received from a wide variety of constituencies in the public and private sectors including—
  - Federal, State, and Local Governments
  - Critical Infrastructure Entities (e.g., power companies, telecommunications providers)
  - Fortune 500 Companies
  - Healthcare Providers
  - Financial Industry
  - Consortia (e.g., National Realtors Association)
  - Private citizens

Significant Comments

- Received over 800 comments on the initial public draft of Special Publication 800-53
- Comments indicated that—
  - ✓ Security controls contained too much implementation detail
  - ✓ Security control baselines (low, moderate, high) included too many controls for a minimum set
  - ✓ There was insufficient flexibility in the security control selection process for organizations to effectively apply the controls in specific operational environments
  - ✓ The “high-water mark” approach required organizations to employ unnecessary security controls

NIST Response

- In response to the initial public comments, NIST re-engineered Special Publication 800-53
- Fundamental changes included—
  - ✓ Streamlining the security control structure and control content to focus on “token-level” requirements
  - ✓ Redesigning the security control enhancement approach to facilitate ease-of-use for organizations requiring additional security controls based on risk assessment
  - ✓ Incorporating scoping guidance to help organizations effectively apply the NIST guidance in specific operational environments
  - ✓ Reducing the number of security controls in the control baselines

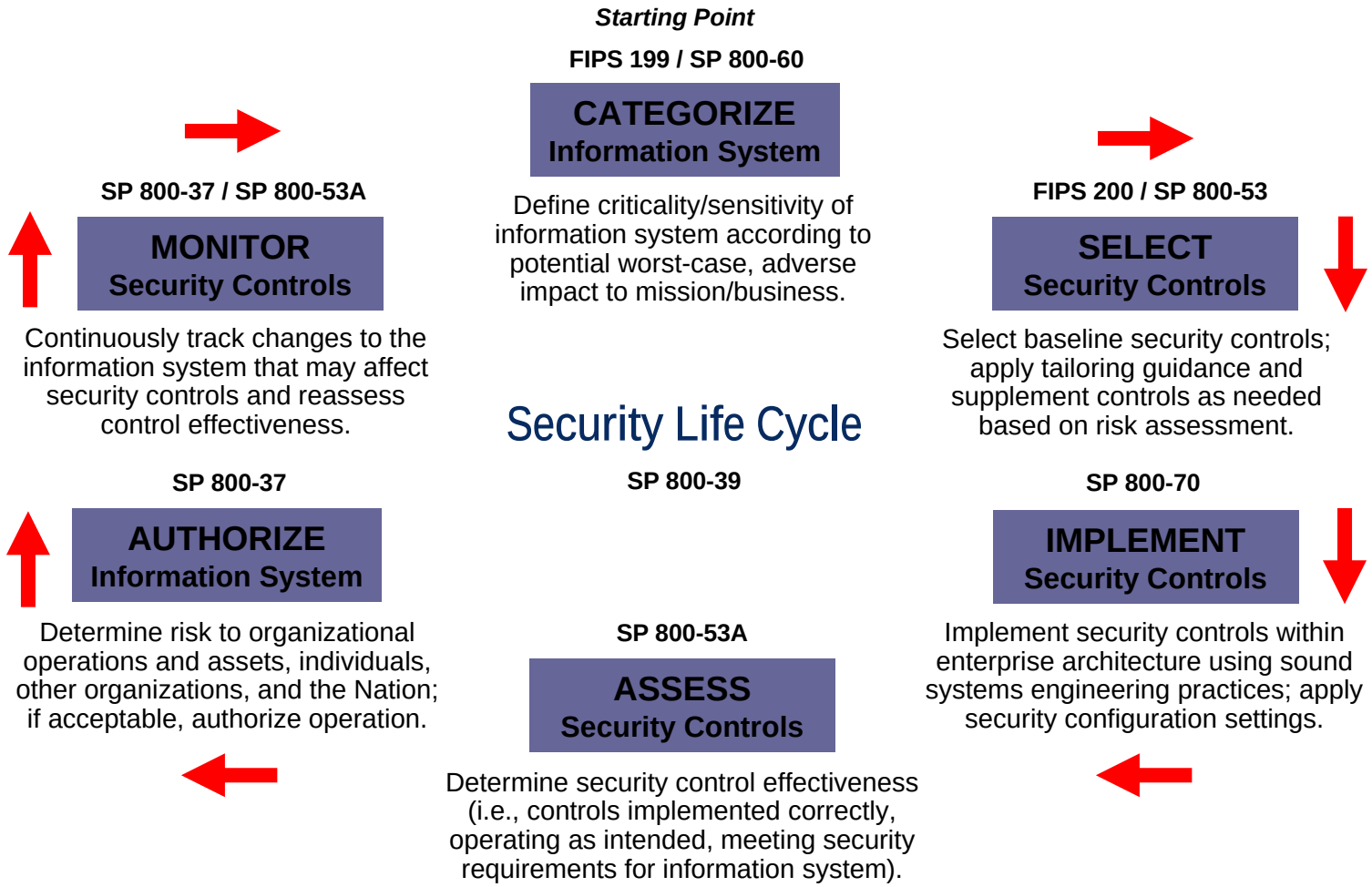
Key Milestones

- NIST Special Publication 800-53
  - Initial Public Draft **(October 2003)**
  - Second Public Draft **(September 2004)**
  - Final Public Draft **(January 2005)**
  - Final Publication **(February 2005)**
- FIPS 200
  - Initial Public Draft **(Projected for May 2005)**
  - Second Public Draft **(Projected for August 2005)**
  - Final Publication **(Projected for December 2005)**

Summary

- Public vetting process proved extremely effective and allowed NIST to build a truly consensus-based security guideline to serve both public and private sector needs
- Extended development cycle and expanded public review periods allowed federal agencies to be better prepare for the transition to FIPS 200, when the security controls become mandatory
- Increasing voluntary acceptance of NIST Special Publication 800-53 by the private sector will help provide greater information security for the nation's critical infrastructure

NIST Risk Management Framework



Federal ICS Security Standards and Guidelines Strategy

- Add control systems domain expertise to:
  - Already available IT security Risk Management Framework
  - Provide workable, practical solutions for control systems – without causing more harm than the incidents we are working to prevent

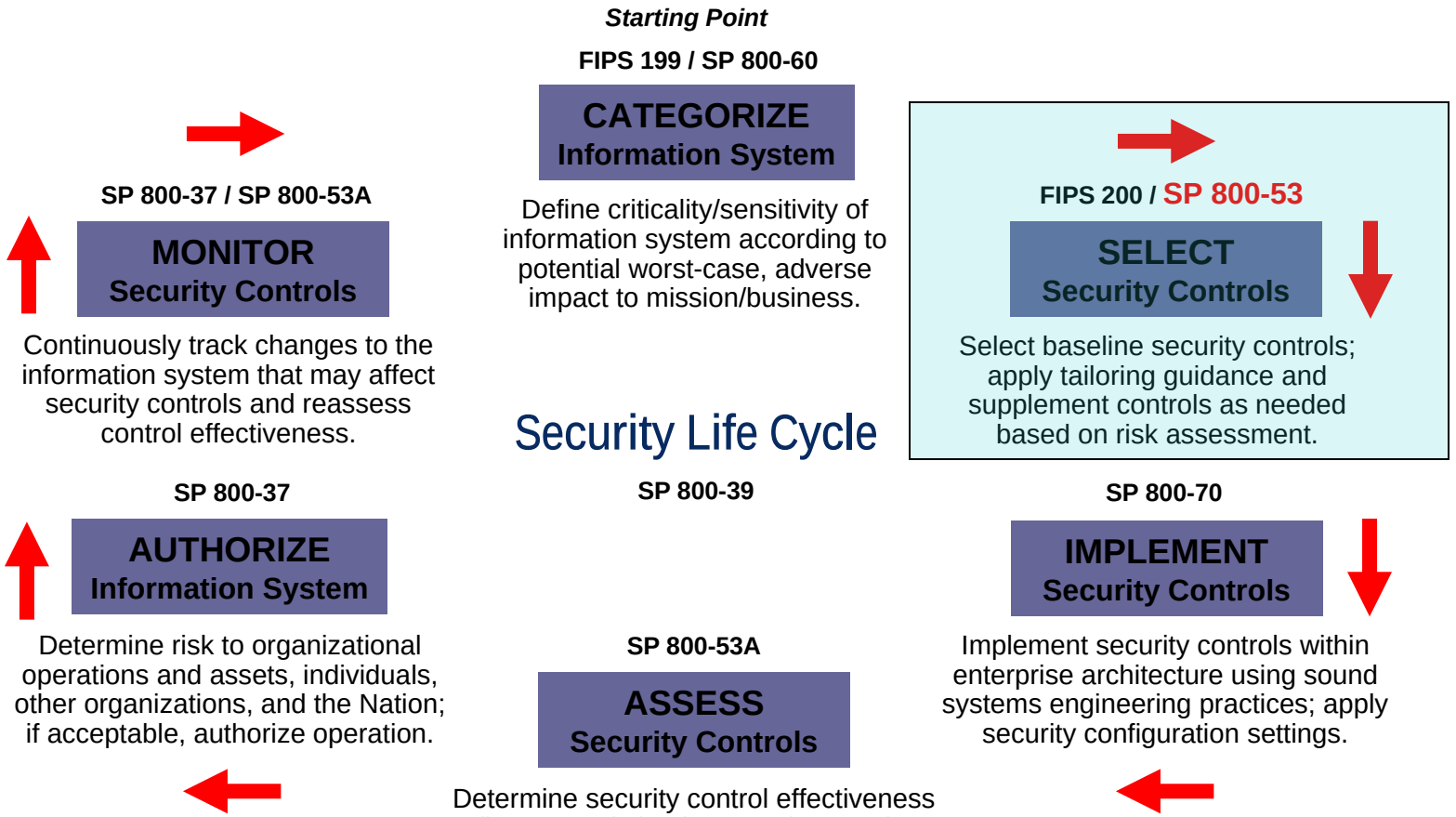
- This expertise takes the form of specific cautions, recommendations & requirements for application to control systems - throughout both technologies and programs
  - ICS Augmentation of NIST SP 800-53 *Recommended Security Controls for Federal Information Systems*
  - NIST SP 800-82 *Guide to Industrial Control System (ICS) Security*

NIST ICS Security Project

- Joint MEL/ITL project, in collaboration with federal and industry stakeholders, to develop standards, guidelines and test methods to help secure these critical control systems in harmony with their demanding safety and reliability requirements.

http://csrc.nist.gov/sec-cert/ics

NIST Risk Management Framework



NIST SP 800-53

- NIST SP 800-53 *Recommended Security Controls for Federal Information Systems*, which was developed for traditional IT systems, contains mandatory information security requirements for all non-national security information and information systems that are owned, operated, or controlled by federal agencies.
- NIST SP 800-53 provides the security controls that need to be applied to secure the system. It does not specify how the controls need to be implemented.
- When organizations attempted to utilize SP 800-53 to protect ICS, difficulties were encountered in implementing SP 800-53 counter-measures because of ICS-unique needs
- Held 2 Workshops (April 2006 and March 2007) with stakeholders to discuss issues and develop ICS material for SP 800-53. 2 drafts were released for public vetting before finalized in December 2007.

NIST SP 800-53 Structure

17 Control Families
171 Controls (Requirements)

- Access Control
- Awareness and Training
- Audit and Accountability
- Certification, Accreditation, and Security Assessments
- Configuration Management
- Contingency Planning
- Identification and Authentication
- Incident Response
- Maintenance
- Media Protection
- Physical and Environmental
- Planning
- Personnel Security
- Risk Assessment
- Systems and Services Acquisition
- System and Communications Protection
- System and Information

NIST SP 800-53 Control Example

AU-6 AUDIT MONITORING, ANALYSIS, AND REPORTING

Control: The organization regularly reviews/analyzes information system audit records for indications of inappropriate or unusual activity, investigates suspicious activity or suspected violations, reports findings to appropriate officials, and takes necessary actions.

Supplemental Guidance: Organizations increase the level of audit monitoring and analysis activity within the information system whenever there is an indication of increased risk to organizational operations, organizational assets, or individuals based on law enforcement information, intelligence information, or other credible sources of information.

Control Enhancements:

(1) The organization employs automated mechanisms to integrate audit monitoring, analysis, and reporting into an overall process for investigation and response to suspicious activities.

(2) The organization employs automated mechanisms to alert security personnel of the following inappropriate or unusual activities with security implications: [*Assignment: organization-defined list of inappropriate or unusual activities that are to result in alerts*].

LOW Not Selected	**MOD** AU-6 (2)	**HIGH** AU-6 (1) (2)

Changes made to NIST SP 800-53 to address ICS

- Original NIST SP 800-53 controls were not changed
- Additional guidance was added to 65 of 171 controls to address ICS
  - ICS Supplemental Guidance
  - ICS Enhancement Supplemental Guidance
- ICS Supplemental Guidance provides information on how the control applies in ICS environments, or provides information as to why the control may not be applicable in ICS environments.

Example:

SC-13 USE OF CRYPTOGRAPHY

ICS Supplemental Guidance:

ICS security objectives typically follow the priority of availability, integrity and confidentiality, in that order. The use of cryptography is determined after careful consideration of the security needs and the potential ramifications on system performance. For example, the organization considers whether latency induced from the use of cryptography would adversely impact the operational performance of the ICS.

Key Take Away

- NIST SP 800-53, Revision 2 is a security standard that addresses both general IT systems as well as ICS. This allows federal agencies, as well as the private sector if desired, to use one document to determine the proper security controls for their IT systems as well as to effectively secure their industrial control systems while addressing their unique requirements.

  http://csrc.nist.gov/publications/nistpubs/800-53-Rev2/sp800-53-rev2-final.pdf

- Federal ICS using NIST SP 800-53, Revision 2
  - Bonneville Power Administration (BPA)
  - Southwestern Power Administration (SWPA)
  - Tennessee Valley Authority (TVA)
  - Western Area Power Administration (WAPA)
  - Federal Aviation Administration (FAA)
  - Department of the Interior, Bureau of Reclamation

NIST SP 800-53 Security Baselines

- LOW Baseline - Selection of a subset of security controls from the master catalog consisting of ***basic*** level controls
- MOD Baseline - Builds on LOW baseline. Selection of a subset of controls from the master catalog—***basic*** level controls, additional controls, and control ***enhancements***
- HIGH Baseline - Builds on MOD baseline. Selection of a subset of controls from the master catalog—***basic*** level controls, additional controls, and control ***enhancements***

- ***How do we categorize ICS?***

Low Impact System

Possible ICS Impact Level Definitions

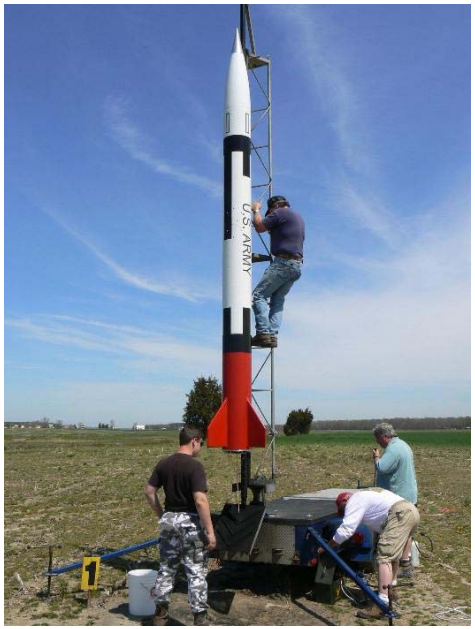
- **Low Impact**
  - **Product Controlled:** Non hazardous materials or products, Non-ingested consumer products
  - **Industry Examples:** Plastic Injection Molding, Warehouse Applications
  - **Security Concerns:** Protecting people, Capital investment, Ensuring uptime

Moderate Impact Systems

Possible ICS Impact Level Definitions

- **Moderate Impact**
  - **Product Controlled:** Some hazardous products and/or steps during production, High amount of proprietary information
  - **Industry Examples:** Automotive Metal Industries, Pulp & Paper, Semi-conductors
  - **Security Concerns:** Protecting people, Trade secrets, Capital investment, Ensuring uptime

High Impact System



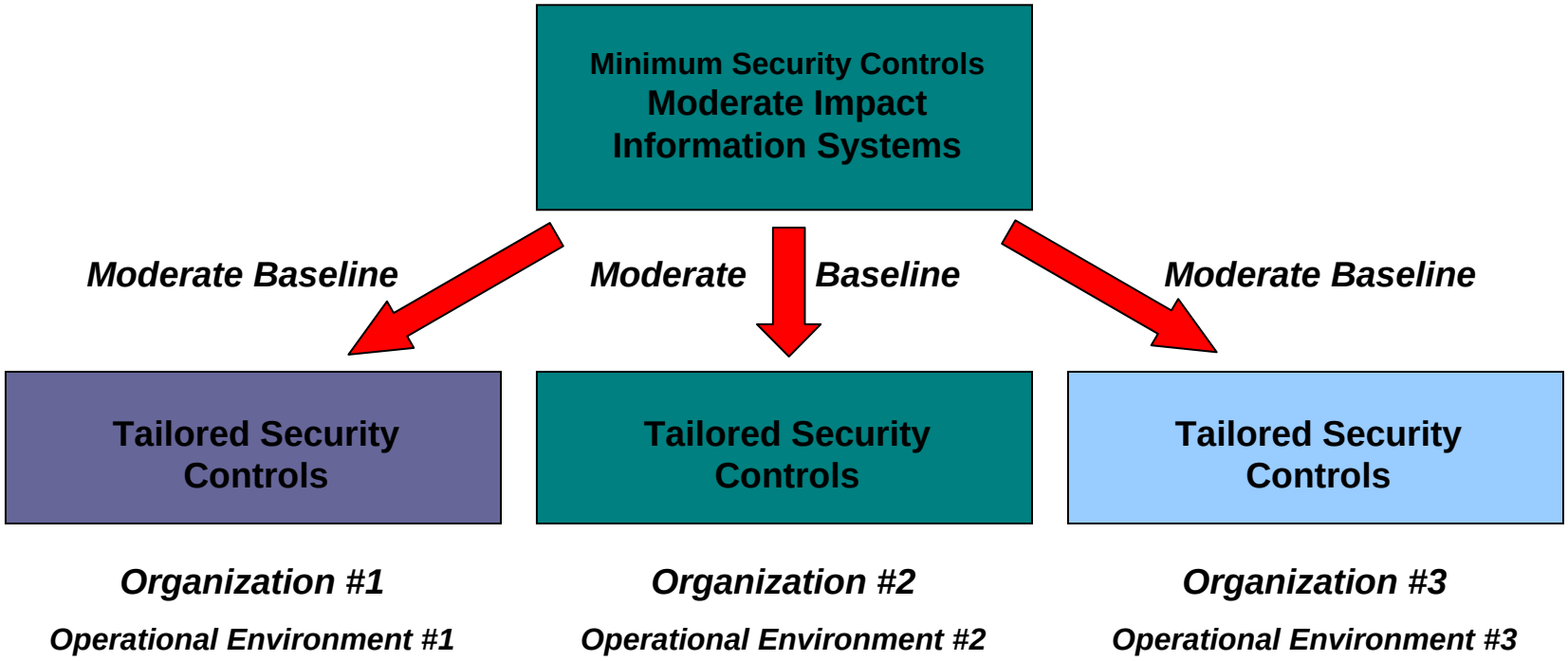
High Impact System !!!

Possible ICS Impact Level Definitions

- **High Impact**
  - **Product Controlled:** Critical Infrastructure, Hazardous Materials, Ingested Products
  - **Industry Examples:** Utilities, PetroChemical, Food & Beverage, Pharmaceutical
  - **Security Concerns:** Protecting human life, Ensuring basic social services, Protecting environment

Tailoring Security Controls

Scoping, Parameterization, and Compensating Controls



Cost effective, risk-based approach to achieving information security…

NIST SP 800-82

- Guide to Industrial Control Systems Security
  - Provide guidance for establishing secure ICS, including implementation guidance for SP 800-53 controls
- Content
  - Overview of ICS
  - ICS Characteristics, Threats and Vulnerabilities
  - ICS Security Program Development and Deployment
  - Network Architecture
  - ICS Security Controls
  - Appendixes
    - Current Activities in Industrial Control Systems Security
    - Emerging Security Capabilities
    - ICS in the FISMA Paradigm

NIST SP 800-82

- Initial public draft released September 2006 - public comment period through December 2006
- Second public draft released September 2007 - public comment period through November 2007
- Final public draft released September 2008 – public comment period through November 2008
- Downloaded over 500,000 times since initial release
- Current document available at:
  - http://csrc.nist.gov/publications/drafts.html

Private Sector ICS Security Standards

- Where the rubber hits the road!
- 90+% of ICS are owned by the private sector
- Standards for the ICS industry, if widely implemented, will raise the level of control systems security
- Greatest chance for industry acceptance and adoption is to have security requirements published in cross industry standards
  - **ISA99 *Industrial Automation and Control System Security* standard**
  - **IEC 62443 *Security for Industrial Process Measurement and Control – Network and System Security* standard**

ISA99

- Co-Chairs: Bryan Singer, Eric Cosman
- Developing an ANSI Standard for Industrial Automation and Control System Security
  - Part 1 – Models and Terminology
  - Part 2 – Establishing an Industrial Automation and Control Systems Program

    Part 3 – Operating an Industrial Automation and Control Systems Program
  - Part 4 – Technical Security Requirements for Industrial Automation and Control Systems

  - NIST SP800-53, Rev 2 have been provided to ISA99 as references to consider in the development of the standard

http://www.isa.org/MSTemplate.cfm?MicrosoftID=988&CommitteeID=6821

IEC 62443

- Convenor: Tom Phinney (US)
- Scope: Establish requirements for securing access to industrial process measurement and control networks and devices on those networks
- IEC 62443 *Security for industrial process measurement and control – Network and system security* standard
  - 62443-1, *Framework and threat-risk analysis*
  - 62443-2, *Security assurance: principles, policy and practice*
  - 62443-3, *Sets of security requirements for security elements in typical scenarios*

  - NIST SP800-53, Rev 2 have been provided to IEC TC65/WG10 as references to consider in the development of the standard

http://www.iec.ch/cgi-bin/procgi.pl/www/iecwww.p?wwwlang=e&wwwprog=dirwg.p&progdb=db1&ctnum=2931

NIST ICS Security Project Contact Information

Project Leaders

Keith Stouffer
(301) 975-3877
keith.stouffer@nist.gov

Dr. Stu Katzke
(301) 975-4768
skatzke@nist.gov

sec-ics@nist.gov

Web Pages

Federal Information Security Management Act (FISMA) Implementation Project

http://csrc.nist.gov/sec-cert

NIST ICS Security Project

http://csrc.nist.gov/sec-cert/ics

NIST Example Augmentation of Standard CIP–005

Cyber Security — Cyber Security Perimeter Protection

October 7, 2008

========== General comments ==========

Discussion (set off by "======" and colored blue) is not part of the NIST augmentation. It is provided to assist the drafting committee.

Order 706 ¶ 61 gives the ERO direction to provide additional guidance in the CIPs or in a separate reference document. For convenience, the guidance is placed in this manuscript. This guidance is part of NIST's augmentation.

==========

A. Introduction

1. Title: Cyber Security — ~~Electronic~~ Cyber Security Perimeter~~(s)~~ (CSP) Protection

2. Number: CIP-005-~~1~~2

3. Purpose: Standard CIP-005 requires the identification and protection of the Electronic Security Perimeter(s) inside which all Critical Cyber Assets reside, as well as all access points on the perimeter. Standard CIP-005 should be read as part of a group of standards numbered Standards CIP-002 through CIP-009. Responsible Entities should interpret and apply Standards CIP-002 through CIP-009 ~~using reasonable business judgment~~.

4. Applicability

4.1. [4.1] Within the text of Standard CIP-005, "Responsible Entity" shall mean all entities that could affect the reliability of the bulk electric grid by virtue of cyber connection to any control system component of the bulk electric system.. Responsible Entities include, but are not limited to:

==========

NIST recommends that all entities that could affect the reliability of the bulk electric grid should be included. Advances in digital electronics technology and computer hardware and software have obsoleted prior distinctions among computing, communications, and control systems. Today, all are collectively considered Information Technology (IT). Until recently, Industrial Control Systems (ICS) had little resemblance to traditional information systems in that they were isolated systems running proprietary software and control protocols. However, as these systems have been increasingly integrated more closely into mainstream organizational information systems to promote connectivity, efficiency, and remote access capabilities, they have started to resemble the more traditional information systems. Increasingly, ICS use the same commercially available hardware and software components as are used in the Responsible Entity's traditional information systems. While the change in industrial control system architecture supports new information system capabilities, it also provides significantly less isolation from the outside world for these systems, introducing many of the same vulnerabilities that exist in current networked information systems. The result is an even greater need to secure ICS.

The interconnection of infrastructures has obsoleted prior distinctions. Distribution Systems and Energy Management Systems should be included. Enumeration can be helpful as examples, providing the enumeration states "including, but not limited to."

==========

- Reliability Coordinator.
- Balancing Authority.
- Interchange Authority.
- Transmission Service Provider.

- Transmission Owner.
- Transmission Operator.
- Generator Owner.
- Generator Operator.
- Load Serving Entity.
- NERC.
- Regional Reliability Organizations.

4.2. [4.2] The following are exempt from Standard CIP-005:

4.2.1 [4.2.1] Facilities regulated by the U.S. Nuclear Regulatory Commission or the Canadian Nuclear Safety Commission.

==========

NIST notes that on September 18, 2008 FERC issued the following Proposed Clarification: facilities within a nuclear generation plant in the United States that are not regulated by the U.S. Nuclear Regulatory Commission are subject to compliance with the eight mandatory "CIP" Reliability Standards approved in Commission Order No. 706.

==========

4.2.2 [4.2.2] Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters that are not under the direct control and management of the Responsible Entity..

4.2.3 [4.3.3] Responsible Entities that, in compliance with Standard CIP-002, identify that they have no Critical Cyber Assets.

5. Effective Date: ~~June 1, 2006~~TBD

~~5.~~6. Exceptions

==========

In Order No. 706 FERC directed the development of a framework to provide accountability when a Responsible Entity relies on technical infeasibility or certain other factors to take exception to specific Requirements. FERC specified that the structural elements of this framework include mitigation steps, a remediation plan, a timeline for eliminating use of the technical feasibility exception unless appropriate justification otherwise is provided, regular review of whether it continues to be necessary to invoke the exception, internal approval by the senior manager, wide-area approval through the ERO's audit process, and cooperation with the ERO to provide the Commission with high-level, wide-area analysis regarding the effects the technical feasibility exception on the reliability of the Bulk-Power System. See ¶ 152, 157-163, 178-187, 192-195, and 209-222.

==========

6.1. The Responsible Entity may take exception to any Requirement based on the Responsible Entity's determination that any of the following conditions apply:

- The Requirement interferes with ICS functions
- The Requirement poses a risk to the reliability of the bulk electric grid
- The ICS cannot support the use of the required mechanisms or implement the required function
- The Requirement will have a significant adverse impact on performance, safety, or reliability

6.2. The Responsible Entity shall document all exceptions in an Exception Plan provided to the ERO and Regional Reliability Organization containing:

6.2.1 A convincing argument why the exception is necessary

6.2.2 Compensating controls or mitigation steps to address the intent of the Requirement

6.2.3 A plan of action, milestones, and schedule for implementing the compensating controls or mitigation steps

6.3. The Exception Plan must be approved annually by a Responsibility Entity senior manager.

6.4. The Exception Plan must be approved annually by the Regional Reliability Organization, or the ERO if there is no applicable RRO.

6.5. The ERO must annually audit compliance with the Exception Plan and provide FERC with an annual high-level, wide-area analysis regarding the effects of all exceptions on the reliability of the Bulk-Power System.

B. Requirements

The Responsible Entity shall comply with the following requirements of Standard CIP-005:

==========

Information may be stored, transmitted, and processed using multiple digital and analog media including electro-magnetic fields in space on media in frequencies commonly described as electrical and optical. For example, fiber optic, infrared, and radio wireless communications are all common, but are not "electronic." NIST believes that "Electronic" is too limited a term and has replaced it with "Cyber" as being more inclusive. "Logical" is another term that could be used.

==========

R0. Cyber Security Perimeter Policy and Procedures — The Responsible Entity shall: develop, disseminate, and periodically review and update: (i) a formal, documented, policy on the protection of all Cyber Security Perimeter(s), the cyber assets contained within, and identification and authentication. This policy shall address purpose, scope, roles, responsibilities, management commitment, coordination among Responsible Entity's sub-entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of this policy and associated controls.

GUIDANCE: This requirement does not prescribe an organization structure for the Responsible Entity 's cyber security policy. The Cyber Security Perimeter Policy and Procedures may be included as part of the general information security policy for the Responsible Entity, or the ICS cyber security policy.

========== based on AC-1 & IA-1 ==========

~~R0.~~R1. [R1] ~~Electronic~~ Cyber Security Perimeter — The Responsible Entity shall ensure that every Critical Cyber Asset resides within a~~n Electronic~~ Cyber Security Perimeter. The Responsible Entity shall identify and document the ~~Electronic~~ Cyber Security Perimeter(s) and all access points to the perimeter(s).

~~R0.1.~~R1.1. [R1.1] Access points to the ~~Electronic~~ Cyber Security Perimeter(s) shall include any externally connected communication ~~end~~ interface point (for example, dial-up modems) terminating at any device at ~~within~~ the ~~Electronic~~ Cyber Security Perimeter(s).

==========

The concept of logically locating the modem at the Perimeter eliminates the need to physically protect the circuit between the modem and the Perimeter, as required in CIP-006.

==========

~~R0.2.~~R1.2. [R1.2] For a dial-up accessible Critical Cyber ~~Asset that~~Asset that uses a non-routable protocol, the Responsible Entity shall define an ~~Electronic~~ Cyber Security Perimeter for that single access point at the dial-up device or shall include the Asset within a defined Cyber Security Perimeter.~~.~~

~~R0.3.~~R1.3. [R1.3] Communication links that are not under the direct control and management of any Responsible Entity connecting discrete Electronic Security Perimeters shall not be considered part of the Electronic Security Perimeter. However, ~~end~~ interface points of these communication links ~~within~~ at the Electronic Security Perimeter(s) shall be considered access points to the Electronic Security Perimeter(s).

==========

The interface between assets controlled by the Responsible Entity and assets controlled by another party is not necessarily the end point for communication. The interface may simply be the demarcation between two domains of responsibility and may also provide changes in information representation or addressing (e.g., optical to electronic, network access translation (NAT)).

==========

~~R0.4.~~R1.4. [R1.4] Any non-critical Cyber Asset within a defined ~~Electronic~~ Cyber Security Perimeter shall be identified and protected pursuant to the requirements of Standard CIP-005.

~~R0.5.~~R1.5. [R1.5] Cyber Assets used in the access control and monitoring of the ~~Electronic~~ Cyber Security Perimeter(s) shall be afforded the protective measures as a specified in Standard CIP-003, Standard CIP-004 Requirement R3, Standard CIP-005 Requirements R2 and R3, Standard CIP-006 Requirements R2 and R3, Standard CIP-007, Requirements R1 and R3 through R9, Standard CIP-008, and Standard CIP-009.

~~R0.6.~~R1.6. [R1.6] The Responsible Entity shall maintain documentation of ~~Electronic~~ Cyber Security Perimeter(s), all interconnected Critical and non-critical Cyber Assets within the Electronic Security Perimeter(s), all ~~electronic~~ access points to the ~~Electronic~~ Cyber Security Perimeter(s) and the Cyber Assets deployed for the access control and monitoring of these access points.

GUIDANCE: Any connections to the Internet, or other external networks, communication systems, cyber assets, or information systems that are not under the control of the Responsible Entity, occur through managed interfaces consisting of appropriate boundary protection devices (e.g., proxies, gateways, routers, firewalls, guards, encrypted tunnels) arranged in an effective architecture (e.g., routers protecting firewalls and application gateways residing on a protected subnetwork commonly referred to as a demilitarized zone or DMZ). Cyber assets at any designated alternate processing sites are provided the same levels of protection as that of the primary site.

As part of a defense-in-depth protection strategy, the Responsible Entity considers partitioning higher-impact cyber assets into separate physical domains (or environments) and applying the concepts of managed interfaces described above to restrict or prohibit network access in accordance with the Responsible Entity's assessment of risk .

The Responsible Entity carefully considers the intrinsically shared nature of commercial telecommunications services in the implementation of security controls associated with the use of such services. Commercial telecommunications services are

commonly based on network components and consolidated management systems shared by all attached commercial customers, and may include third party provided access lines and other service elements. Consequently, such interconnecting transmission services may represent sources of increased risk despite contract security provisions. Therefore, when this situation occurs, the Responsible Entity implements appropriate compensating security controls.

========== guidance based on SC-7 ==========

R1.7. The Responsible Entity physically allocates publicly accessible cyber assets to separate subnetworks with separate, physical network interfaces.

GUIDANCE: Publicly accessible cyber assets include, for example, emergency cut-off activators. Generally, public access to ICS information is not permitted.

========== based on SC-7 control enhancement 1 Appx F & I==========

R1.8. The Responsible Entity shall prevent public access into the Responsible Entity's internal networks except as appropriately mediated.

========== based on SC-7 control enhancement 2 ==========

~~R0.7.~~R1.9. The Responsible Entity shall limit the number of access points to the Cyber Security Perimeter to allow for better monitoring of inbound and outbound network traffic.

========== based on SC-7 enhancement 3 ==========

~~R0.8.~~R1.10. The Responsible Entity shall implement a managed interface (boundary protection devices in an effective security architecture) with any external telecommunication service, implementing controls appropriate to the required protection of the confidentiality and integrity of the information being transmitted.

========== based on SC-7 enhancement 4 ==========

~~R1.~~R2. [R2] ~~Electronic~~ Cyber Access Controls — The Responsible Entity shall implement and document the organizational processes and technical and procedural mechanisms for control of ~~electronic~~ cyber access at all ~~electronic~~ cyber access points ~~to~~ at the ~~Electronic~~ Cyber Security Perimeter(s)~~.~~, and at key internal boundaries within the Cyber Security Perimeter(s).

~~R1.1.~~R2.1. [R2.5] The required documentation shall, at least, identify and describe:

~~R1.1.1.~~R2.1.1. [R2.5.1] The processes for access request and authorization.

~~R1.1.2.~~R2.1.2. [R2.5.2]The authentication methods.

~~R1.1.3.~~R2.1.3. [R2.5.3] The review process for authorization rights, in accordance with Standard CIP-004 Requirement R4.

~~R1.1.4.~~R2.1.4. [R2.5.4] The controls used to secure dial-up accessible connections.

GUIDANCE: Any connections to the Internet, or other external networks or information systems, occur through managed interfaces consisting of appropriate boundary protection devices (e.g., proxies, gateways, routers, firewalls, guards, encrypted tunnels) arranged in an effective architecture (e.g., routers protecting firewalls and application gateways residing on a protected subnetwork commonly referred to as a demilitarized zone or DMZ). Cyber security boundary protections at any designated alternate processing sites provide the same levels of protection as that of the primary site.

As part of a defense-in-depth protection strategy, the Responsible Entity considers partitioning higher-impact information systems into separate physical domains (or

environments) and applies the concepts of managed interfaces described above to restrict or prohibit network access in accordance with an Responsible Entity's assessment of risk.

The Responsible Entity carefully considers the intrinsically shared nature of commercial telecommunications services in the implementation of security controls associated with the use of such services. Commercial telecommunications services are commonly based on network components and consolidated management systems shared by all attached commercial customers, and may include third party provided access lines and other service elements. Consequently, such interconnecting transmission services may represent sources of increased risk despite contract security provisions.

========== based on SC-7 ==========

~~R1.2.~~R2.2. [R2.1] These processes and mechanisms shall use an access control model that denies access by default, such that explicit access permissions must be specified.

R2.3. [R2.3] The Responsible Entity shall maintain a procedure for securing dial-up access to the Electronic Security Perimeter(s). The Responsible Entity shall:

R2.3.1. Employ automated mechanisms to facilitate the monitoring and control of dial-up access.

R2.3.2. Determine if cryptography is required to protect the confidentiality and integrity of dial-up access sessions.

R2.3.3. Permit dial-up access for privileged functions only for compelling operational needs and documents the rationale for such access in the security plan for the Cyber Security Perimeter .

GUIDANCE: The Responsible Entity restricts access achieved through dial-up connections (e.g., limiting dial-up access based upon source of request) or protects against unauthorized connections or subversion of authorized connections (e.g., using virtual private network technology). NIST Special Publication 800-63 provides guidance on remote electronic authentication. NIST Special Publication 800-77 provides guidance on IPsec-based virtual private networks.

Dial-up access to ICS locations (e.g., control centers, field locations) is only enabled when necessary, approved, and authenticated. In situations where the ICS cannot support the use of automated mechanisms for monitoring and control of dial-up access methods, the Responsible Entity employs nonautomated mechanisms or procedures as compensating controls (e.g., following manual authentication, dial-in remote access may be enabled for a specified period of time or a call may be placed from the ICS site to the authenticated remote entity).

Cryptography is used for the protection of information and communications. At the core of all products offering cryptographic services is the cryptographic module. Weaknesses such as poor design or weak algorithms can render a product insecure and place highly sensitive information at risk. Adequate testing and validation of the cryptographic module and its underlying cryptographic algorithms against established standards is essential to provide security assurance.

The NIST Cryptographic Module Validation Program (CMVP) validates commercial cryptographic modules to Federal Information Processing Standard (FIPS) 140-2 and other cryptography based standards such as algorithms.

ICS security objectives typically follow the priority of availability, integrity and confidentiality, in that order. The use of cryptography is determined after careful

consideration of the security needs and the potential ramifications on system performance. For example, the Responsible Entity considers whether latency induced from the use of cryptography would adversely impact the operational performance of the ICS.

In situations where the ICS cannot support the use of cryptographic mechanisms to protect the confidentiality and integrity of remote sessions, or the components cannot use cryptographic mechanisms due to significant adverse impact on performance, safety, or reliability, the Responsible Entity employs appropriate compensating controls (e.g., providing increased auditing measures for remote sessions or limiting remote access privileges to key personnel).

==== based on AC-17, IA-7 Appx F&I and other NIST publications===

~~R1.3.~~R2.4. The Responsible Entity shall authorize and document all connections between cyber assets inside the Cyber Security Perimeter and cyber assets outside of the Cyber Security Perimeter.

GUIDANCE: The Responsible Entity carefully considers the risks that may be introduced when cyber assets are connected to other cyber assets with different security requirements and security controls, both within the Responsible Entity and external to the Responsible Entity. Risk considerations also include cyber assets sharing the same networks.

========== additions based on CA-3 ==========

~~R1.4.~~R2.5. [R2.4] Where ~~external interactive~~ access through ~~into~~ the ~~Electronic~~ Cyber Security Perimeter has been authorized and enabled, the Responsible Entity shall implement multifactor ~~strong~~ procedural or technical controls at the access points to ensure authenticity of the accessing ~~party~~parties, ~~where technically feasible~~and monitors/controls the access on an ongoing basis.

GUIDANCE: Multifactor authentication is a system wherein more than one different factors are used to authenticate, thereby delivering a higher level of authentication assurance. Using more than one factor is sometimes called strong authentication.

========== based on IA-2 control enhancement 1 ==========

R2.6. The Responsible Entity shall:

R2.6.1. Employ automated mechanisms to facilitate the monitoring and control of remote access methods.

R2.6.2. Determine if cryptography is required to protect the confidentiality and integrity of remote access sessions.

R2.6.3. Control all remote accesses through a limited number of managed access control points.

R2.6.4. Permit remote access for privileged functions only for compelling operational needs and documents the rationale for such access in the security plan for the Cyber Security Perimeter .

GUIDANCE: Remote access is any access to an Cyber Security Perimeter by a user (or a cyber asset) communicating through an external network not under the control of the Responsible Entity (e.g., the Internet, public switched telephone network). Examples of remote access methods include dial-up, broadband, and wireless. The Responsible Entity protects against unauthorized connections or subversion of authorized connections (e.g., using virtual private network technology). NIST Special

Publication 800-63 provides guidance on remote electronic authentication. NIST Special Publication 800-77 provides guidance on IPsec-based virtual private networks.

Remote access to ICS locations (e.g., control centers, field locations) is only enabled when necessary, approved, and authenticated. In situations where the ICS cannot support the use of automated mechanisms for monitoring and control of remote access methods, the Responsible Entity employs nonautomated mechanisms or procedures as compensating controls.

Cryptography is used for the protection of information and communications. At the core of all products offering cryptographic services is the cryptographic module. Weaknesses such as poor design or weak algorithms can render a product insecure and place highly sensitive information at risk. Adequate testing and validation of the cryptographic module and its underlying cryptographic algorithms against established standards is essential to provide security assurance.

The NIST Cryptographic Module Validation Program (CMVP) validates commercial cryptographic modules to Federal Information Processing Standard (FIPS) 140-2 and other cryptography based standards such as algorithms.

ICS security objectives typically follow the priority of availability, integrity and confidentiality, in that order. The use of cryptography is determined after careful consideration of the security needs and the potential ramifications on system performance. For example, the Responsible Entity considers whether latency induced from the use of cryptography would adversely impact the operational performance of the ICS.

In situations where the ICS cannot support the use of cryptographic mechanisms to protect the confidentiality and integrity of remote sessions, or the components cannot use cryptographic mechanisms due to significant adverse impact on performance, safety, or reliability, the Responsible Entity employs appropriate compensating controls (e.g., providing increased auditing measures for remote sessions or limiting remote access privileges to key personnel).

==== based on AC-17, IA-7 Appx F&I and other NIST publications====

R2.7. The Responsible Entity shall:

R2.7.1. Develop a list of privileged functions

R2.7.2. Develop a list of authorized actions that can be taken with respect to privileged functions

~~R1.4.1.~~**R2.7.3.** Document the criteria and procedures for granting authorization to identified persons and entities.

The Responsible Entity shall manage cyber asset accounts, including establishing, activating, modifying, reviewing, disabling, and removing accounts. Privilege authorizations shall be granted in accordance with established policy and recorded. The Responsible Entity shall determine and implement the frequency for reviewing said accounts, at least annually.

GUIDANCE: Account management includes the identification of account types (i.e., individual, group, and system), establishment of conditions for group membership, and assignment of associated authorizations. The Responsible Entity identifies authorized users of the cyber assets and specifies access rights/privileges. The Responsible Entity grants access to the cyber assets based on: (i) a valid need-to-know/need-to-share that is determined by assigned official duties and satisfying all personnel security criteria; and (ii) intended usage. The Responsible Entity requires proper identification for

requests to establish accounts and approves all such requests. The Responsible Entity specifically authorizes and monitors the use of guest/anonymous accounts and removes, disables, or otherwise secures unnecessary accounts. Account managers are notified when cyber asset users are terminated or transferred and associated accounts are removed, disabled, or otherwise secured. Account managers are also notified when users' cyber asset usage or need-to-know/need-to-share changes.

==========requirement and guidance based on AC-2 ==========

~~R1.5.~~R2.8. The cyber assets shall enforce assigned authorizations for controlling access in accordance with applicable policy.

GUIDANCE: Access control policies (e.g., identity-based policies, role-based policies, rule-based policies) and associated access enforcement mechanisms (e.g., access control lists, access control matrices, cryptography) are employed to control access between users (or processes acting on behalf of users) and objects (e.g., devices, files, records, processes, programs, domains) within the cyber security perimeter. In addition to controlling access at the network layer of the ISO Reference Architecture, access enforcement mechanisms are employed at the application layer, when necessary, to provide increased information security. Consideration is given to the implementation of a controlled, audited, and manual override of automated mechanisms in the event of emergencies or other serious events.

The Responsible Entity ensures that access enforcement mechanisms do not adversely impact the operational performance of the ICS.

========== requirement & guidance based on AC-3 Appx F & I ==========

~~R1.6.~~R2.9. The cyber assets shall restrict access to privileged functions (deployed in hardware, software, and firmware) and security-relevant information to explicitly authorized personnel.

GUIDANCE: Explicitly authorized personnel include, for example, security administrators, system and network administrators, and other privileged users. Privileged users are individuals who have access to system control, monitoring, or administration functions (e.g., system administrators, information system security officers, maintainers, system programmers).

Within ICS, it is commonly the case that having access to specific devices (e.g., workstations, remote terminal units, field devices) is the equivalent to having privileged access; thereby restricting access to these devices is also restricting access to privileged functions and security-relevant information.

========== requirement & guidance based on AC-3 Appx F & I ==========

~~R1.7.~~R2.10. The Responsible Entity shall specify privileged functions that have impacts on facility, public, and environmental safety that require dual authorization.

GUIDANCE: The Responsible Entity does not employ dual-approval mechanisms when an immediate response is necessary to ensure public and environmental safety.

========== requirement & guidance based on AC-3 ICS-1 ==========

~~R1.8.~~R2.11. The cyber assets shall enforce assigned authorizations for controlling the flow of information within the Cyber Security Perimeter and between interconnected Cyber Security Perimeters in accordance with applicable policy.

GUIDANCE: Information flow control regulates where information is allowed to travel within a Cyber Security Perimeter and between Cyber Security Perimeters (as

opposed to who is allowed to access the information) and without explicit regard to subsequent accesses to that information. A few, of many, generalized examples of possible restrictions that are better expressed as flow control than access control are: keeping export controlled information from being transmitted in the clear to the Internet, blocking outside traffic that claims to be from within the Responsible Entity, and not passing any web requests to the Internet that are not from the internal web proxy. Information flow control policies and enforcement mechanisms are commonly employed by Responsible Entities to control the flow of information between designated sources and destinations (e.g., networks, individuals, devices) within Cyber Security Perimeters and between interconnected Cyber Security Perimeters. Flow control is based on the characteristics of the information and/or the information path. Specific examples of flow control enforcement can be found in boundary protection devices (e.g., proxies, gateways, guards, encrypted tunnels, firewalls, and routers) that employ rule sets or establish configuration settings that restrict information system services or provide a packet filtering capability.

========== requirement & guidance based on AC-4 ==========

~~R1.9.~~R2.12. The Responsible Entity shall identify roles and responsibilities where separation of duties is necessary. The cyber assets enforces separation of duties through assigned access authorizations.

GUIDANCE: The Responsible Entity establishes appropriate divisions of responsibility and separates duties as needed to eliminate conflicts of interest in the responsibilities and duties of individuals. There is access control software on the cyber assets that prevents users from having all of the necessary authority or information access to perform fraudulent activity without collusion. Examples of separation of duties include: (i) mission functions and distinct support functions are divided among different individuals/roles; (ii) different individuals perform cyber asset support functions (e.g., system management, systems programming, quality assurance/testing, configuration management, and network security); and (iii) security personnel who administer access control functions do not administer audit functions. In situations where the ICS cannot support the differentiation of roles or a single individual performs all roles within the ICS, the Responsible Entity shall employ appropriate compensating controls (e.g., providing increased personnel security and auditing measures).

========== requirement & guidance based on AC-5 Appx F&I ==========

R2.13. The Responsible Entity shall:

R2.13.1. Approve individual access privileges and enforce cyber access restrictions associated with changes to the critical cyber assets

~~R1.9.1.~~R2.13.2. Generate, retain, and review records reflecting all such changes.

GUIDANCE: Planned or unplanned changes to the hardware, software, and/or firmware components of the cyber assets can have significant effects on the overall security of the system. Accordingly, only qualified and authorized individuals obtain access to information system components for purposes of initiating changes, including upgrades, and modifications. In situations where the ICS cannot support the use of automated mechanisms to enforce access restrictions and support auditing of enforcement actions, the Responsible Entity employs nonautomated mechanisms or procedures as compensating controls

======== based on CM-5 from Appendixes F & I ==========

~~R1.10.~~R2.14. [R2.2] At all access points to the ~~Electronic~~ Cyber Security Perimeter(s) and at all Cyber Assets contained within the Perimeter, the Responsible Entity ~~shall enable~~shall enable only ports, functions, capabilities, and/or ~~services required~~services required for operations ~~and for~~ including monitoring Cyber Assets within the ~~Electronic~~ Cyber Security Perimeter, and shall document, individually or by specified grouping, the configuration of those ports, functions, capabilities, and services.

GUIDANCE: Cyber Assets are capable of providing a wide variety of functions and services. Some of the functions and services, provided by default, may not be necessary to support essential Responsible Entity operations (e.g., key missions, functions). Additionally, it is sometimes convenient to provide multiple services from a single component of a Cyber Asset, but doing so increases risk over limiting the services provided by any one component. The Responsible Entity limits component functionality to a single function per device (e.g., email server or web server, not both). The functions and services provided by Cyber Assets, or individual components of Cyber Assets, should be carefully reviewed to determine which functions and services are candidates for elimination (e.g., Voice Over Internet Protocol, Instant Messaging, File Transfer Protocol, Hyper Text Transfer Protocol, file sharing).

========== additions to requirement based on CM-7 ==========

R2.15. The Responsible Entity shall define and the cyber assets shall automatically enforce:

R2.15.1. A limit of consecutive invalid access attempts by a user during a specified time period, and restrictions on further accesses including

R2.15.2. A defined time period to lock the account, preventing access

~~R1.10.1.~~R2.15.3. A defined time period and algorithm to delays next login prompt.

GUIDANCE: Due to the potential for denial of service, automatic lockouts initiated by the cyber assets are usually temporary and automatically release after a predetermined time period established by the Responsible Entity.

In situations where the ICS cannot support account/node locking or delayed login attempts, or the ICS cannot perform account/node locking or delayed logins due to significant adverse impact on performance, safety, or reliability, the Responsible Entity employs appropriate compensating controls (e.g., logging or recording all unsuccessful login attempts and alerting security personnel though alarms or other means when the number of Responsible Entity-defined consecutive invalid access attempts is exceeded).

========== additions to requirement based on AC-7 Appx F & I ==========

~~R1.11.~~R2.16. The Responsible Entity shall define an interval of user inactivity after which the cyber assets shall initiate a session lock. The session lock remains in effect until the user reestablishes access using appropriate identification and authentication procedures.

GUIDANCE: Users can directly initiate session lock mechanisms. The ICS employs session lock to prevent access to specified workstations/nodes. The ICS activates session lock mechanisms automatically after a time period defined by the Responsible Entity for designated workstations/nodes on the ICS. In some cases, session lock for ICS operator workstations/nodes is not advised (e.g., when immediate operator responses are required in emergency situations). Session lock is not a substitute for logging out of the ICS. In situations where the ICS cannot support session lock, the Responsible Entity employs appropriate compensating controls (e.g., providing increased physical security, personnel security, and auditing measures)

========== additions based on AC-11 Appx F & I ==========

~~R1.12.~~R2.17. For remote access sessions, the Responsible Entity shall define an interval of user inactivity after which the cyber assets shall automatically terminate the session.

GUIDANCE: In situations where the ICS cannot support the automatic termination of remote sessions after a specified period of inactivity, or the ICS cannot automatically terminate remote sessions due to significant adverse impact on performance, safety, or reliability, the Responsible Entity employs nonautomated mechanisms or procedures as compensating controls (e.g., providing increased auditing measures for such sessions or limiting remote access privileges to key personnel).

========== based on AC-12 Appx F & I ==========

~~R1.13.~~R2.18. The Responsible Entity shall identify and document specific user actions that can be performed on the cyber assets without identification or authentication.

GUIDANCE: Emergency switches to stop operations are accessible to any individual with authorized physical access.

========== based on AC-14 ==========

~~R1.14.~~R2.19. [R2.6] Appropriate Use Banner — ~~Where technically feasible, electronic~~ ~~a~~Access control devices shall display an appropriate use banner on the user screen upon all interactive access attempts. The banner shall inform potential users: (i) that the user is accessing a private system; (ii) that system usage may be monitored, recorded, and subject to audit; (iii) that unauthorized use of the system is prohibited and subject to criminal and civil penalties; and (iv) that use of the system indicates consent to monitoring and recording. The banner shall provides appropriate privacy and security notices (based on associated privacy and security policies or summaries) and remains on the screen until the user takes explicit actions to log on. The Responsible Entity shall maintain a document identifying the content of the banner.

========== additions to requirement based on AC-8 ==========

~~R2.~~R3. [R3] Monitoring ~~Electronic~~ Cyber Access — The Responsible Entity shall define, periodically review, and update, a list of auditable events and uses that list to generate audit records. The Responsible Entity shall implement and document an electronic or manual process(es) for monitoring and logging audit records for these events ~~access at access points to the Electronic Security Perimeter(s)~~twenty-four hours a day, seven days a week.

========== additions to requirement based on AU-2 ==========

GUIDANCE: The purpose of monitoring and logging audit records is to identify important events which need to be audited as significant and relevant to the reliability of the bulk electric grid. The Responsible Entity specifies which events require auditing and how the audition is implemented. Auditing activity can affect system performance. Therefore, the Responsible Entity decides, based upon a risk assessment, which events require auditing on a continuous basis and which events require auditing in response to specific situations. Audit records can be generated at various levels of abstraction, including at the packet level as information traverses the network. Selecting the right level of abstraction for audit record generation is a critical aspect of an audit capability and can facilitate the identification of root causes to problems. Additionally, the security audit function is coordinated with the network health and status monitoring function to enhance the mutual support between the two functions by the selection of information to be recorded by each function. The checklists and configuration guides at http://csrc.nist.gov/pcig/cig.html provide recommended lists of auditable events. The Responsible Entity defines auditable events that are adequate to support after-the-fact investigations of security incidents. Most auditing occurs at the application level. In situations where the Responsible Entity cannot support the use of automated mechanisms to generate

audit records, the Responsible Entity employs nonautomated mechanisms or procedures as compensating controls

========== based on AU-2 Appendix F & I ==========

~~R2.1.~~R3.1. Cyber assets shall produce audit records that contain sufficient information to establish what events occurred, the sources of the events, and the outcomes of the events. Cyber assets shall provide the capability to include additional, more detailed information in the audit records for audit events identified by type, location, or subject.

GUIDANCE: Audit record content includes, for most audit records: (i) date and time of the event; (ii) the component of the information system (e.g., software component, hardware component) where the event occurred; (iii) type of event; (iv) user/subject identity; and (v) the outcome (success or failure) of the event.

========== based on AU-3 ==========

~~R2.2.~~R3.2. The Responsible Entity allocates sufficient audit record storage capacity and configures auditing to reduce the likelihood of such capacity being exceeded.

========== based on AU-4 ==========

~~R2.3.~~R3.3. The Responsible Entity shall define actions to be taken in the event of an audit processing failure (e.g., overwrite oldest audit records, stop generating audit records). Cyber assets that perform auditing shall alert appropriate Responsible Entity officials and take these actions in the event of an audit processing failure.

GUIDANCE: Audit processing failures include, for example, software/hardware errors, failures in the audit capturing mechanisms, and audit storage capacity being reached or exceeded. In general, audit record processing is not performed on the ICS, but on a separate information system. In situations where the ICS cannot support auditing including response to audit failures, the Responsible Entity employs compensating controls (e.g., providing an auditing capability on a separate information system).

========== requirement based on AU-5 Appx F & I ==========

~~R2.4.~~R3.4. [R3.1] For dial-up accessible Critical Cyber Assets that use non-routable protocols, the Responsible Entity shall implement and document monitoring process(es) at each access point to the dial-up device~~, where technically feasible.~~.

~~R2.5.~~R3.5. [R3.2] ~~Where technically feasible, t~~The Responsible Entity's security monitoring process(es) shall regularly review/analyze audit records with respect to the enforcement and usage of cyber asset access controls for indications of inappropriate or unusual activity, investigate suspicious activity or suspected violations, detect and alert for attempts at or actual unauthorized accesses. These alerts shall provide for appropriate notification to designated response personnel who take necessary actions. The Responsible Entity shall employ automated mechanisms to facilitate the review of user activities. If the Responsible Entity takes an exception to ~~Where~~ alerting ~~is not technically feasible~~as specified in section A.6, the Responsible Entity shall review or otherwise assess ~~access logs~~audit records for attempts at or actual unauthorized ~~accesses~~ activities at least every ninety calendar days.

GUIDANCE: The Responsible Entity reviews audit records (e.g., user activity logs) for inappropriate activities in accordance with Responsible Entity procedures. The Responsible Entity investigates any unusual cyber asset-related activities and periodically reviews changes to access authorizations. The Responsible Entity reviews more frequently the activities of users with significant cyber asset roles and

responsibilities. In situations where the ICS cannot support the use of automated mechanisms for reviewing user activities, the Responsible Entity employs nonautomated mechanisms or procedures as compensating controls.

Responsible Entities increase the level of audit monitoring and analysis activity within the system whenever there is an indication of increased risk based on law enforcement information, intelligence information, or other credible sources of information.

========== based on AC-13 Appx F & I and AU-6 ==========

~~R2.6.~~R3.6. The Responsible Entity shall define a list of inappropriate or unusual activities with security implications that are to result in automated alerts that shall be sent to designated security personnel.

========== requirements based on AU-6 ==========

R3.7. The Responsible Entity shall provide an audit reduction and report generation capability. The audit reduction and report generation system shall provide the capability to automatically process audit records for events of interest based upon selectable, event criteria..

GUIDANCE: Audit reduction, review, and reporting tools support after-the-fact investigations of security incidents without altering original audit records. In general, audit record processing is not performed on the Critical Cyber Asset, but on a separate cyber asset.

========== based on AU-7 Appx F & I ==========

~~R2.7.~~R3.8. The Responsible Entity shall employ time stamps in audit record generation. The Responsible Entity shall define the frequency for synchronizing internal clocks. The cyber assets shall synchronize internal system clocks at this frequency.

GUIDANCE: Time stamps (including date and time) of audit records are generated using internal system clocks.

========== requirement based on AU-8 ==========

~~R2.8.~~R3.9. The Responsible Entity shall protect audit information and audit tools from unauthorized access, modification, and deletion.

GUIDANCE: Audit information includes all information (e.g., audit records, audit settings, and audit reports) needed to successfully audit information system activity

========== based on AU-9 ==========

R4. -Cyber Security Perimeter Assessment — The Responsible Entity shall establish a program to assess the security of the Cyber Security Perimeter.

R4.1. The Responsible Entity shall develop detailed Cyber Security Perimeter testing standards, processes, and procedures (called "CSP Security Assessment Guide") to provide direction and guidance on security testing; the Guides must:

R4.1.1. Identify who is to be held accountable and responsible for ensuring that information security tests comply with Responsible Entity requirements.

R4.1.2. Identify the Responsible Entity requirements with which security tests must comply, i.e., test scenarios must map to and support security requirements, must specify the minimum set of security controls evaluated during tests, as well as the depth and breadth of tests.

R4.1.3. Specify the appropriate roles and responsibilities, i.e., there must be well-qualified personnel in both security testing and analysis, and care must be

taken to ensure separation of duties when testing; for example, testing and analysis must be performed by an independent person(s).

R4.1.4. Adhere to established methodology that identify and test for security controls for the types of testing being performed, viz., NIST guidelines describe these methods as interview, examine and test.

R4.1.5. Specify a testing environment and criteria to be added per NIST SP 800-53A and SP 800-115 and describe these methods, such as the use of dedicated test equipment that must be used for security testing.

R4.1.6. State the frequency of assessmentswhen and how often testing is to be performed.

R4.1.7. Provide the documentation requirements, such as test plans and test results; i.e., adequately securing the results and analysis information and artifacts from testing.

R4.1.8. Specify the criteria for the analysis of the tests and the dissemination of results and recommendations.

R4.1.9. Develop a plan of action, milestones, and schedule to correct deficiencies found during testing.

~~R2.9.~~R4.2. [R4] Cyber Vulnerability Assessment — The Responsible Entity shall employ a qualified independent agent or team to conduct assessment of (a) ~~perform a~~ cyber vulnerabilities ~~y assessment~~ of the ~~electronic~~ access points to the ~~Electronic~~ Cyber Security Perimeter(s)- at least annually, or when significant new vulnerabilities potentially affecting the cyber assets are identified and reported.. The vulnerability assessment shall be conducted in accordance with the CSP Security Assessment Guide. The vulnerability assessment shall include, at a minimum, the following:

========== based on CA-4 and RA-5 ==========

~~R2.9.1.~~R4.2.1. [R4.1] A document identifying the vulnerability assessment process;

~~R2.9.2.~~R4.2.2. [R4.2] A review to verify that only ports and services required for operations at these access points are enabled;

~~R2.9.3.~~R4.2.3. [R4.3] The discovery of all access points to the ~~Electronic~~ Cyber Security Perimeter;

~~R2.9.4.~~R4.2.4. [R4.4] A review of controls for default accounts, passwords, and network management community strings; ~~and,~~

~~R2.9.5.~~R4.2.5. [R4.5] Documentation of the results of the assessment, the action plan to remediate or mitigate vulnerabilities identified in the assessment, and the execution status of that action plan.

========== based on CA-4 ==========

GUIDANCE: Vulnerability scanning is conducted using appropriate scanning tools and techniques. The Responsible Entity trains selected personnel in the use and maintenance of vulnerability scanning tools and techniques. Vulnerability scans are scheduled and/or random in accordance with Responsible Entity policy and assessment of risk. The information obtained from the vulnerability scanning process is freely shared with appropriate personnel throughout the Responsible Entity to help eliminate similar vulnerabilities in other cyber assets. Vulnerability analysis for custom software and applications may require additional, more specialized approaches (e.g., vulnerability scanning tools for applications, source code reviews, static analysis of source code).

Vulnerability scanning tools are used with care on ICS networks to ensure that ICS functions are not adversely impacted by the scanning process. Production ICS may need to be taken off-line, or replicated to the extent feasible, before scanning can be conducted. If ICS are taken off-line for scanning, scans are scheduled to occur during planned ICS outages whenever possible. If vulnerability scanning tools are used on non-ICS networks, extra care is taken to ensure that they do not scan the ICS network. In situations where the Responsible Entity cannot, for operational reasons, conduct vulnerability scanning on a production ICS, the Responsible Entity employs compensating controls (e.g., providing a replicated system to conduct scanning)

========== guidance based on RA-5 Appx F & I ==========

~~R2.10.~~R4.3. Cyber Control Assessment - The Responsible Entity shall employ a qualified independent agent or team to conduct an assessment of the implementation of all the cyber security controls in the Cyber Security Perimeter at least annually, or when significant new vulnerabilities potentially affecting the cyber assets are identified and reported. The implementation assessment shall -determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements. The implementation assessment shall be conducted in accordance with the CSP Security Assessment Guide.

~~R3.~~R5. [R5] Documentation Review and Maintenance — The Responsible Entity shall review, update, and maintain all documentation to support compliance with the requirements of Standard CIP-005.

R5.1. The Responsible Entity shall develop, document, and maintain a current inventory of the cyber assets in the Cyber Security Perimeter and relevant ownership information. The Responsible Entity shall update the inventory of cyber assets as an integral part of component installations.

GUIDANCE: The Responsible Entity determines the appropriate level of granularity for the cyber asset components included in the inventory that are subject to management control (i.e., tracking, and reporting). The inventory of cyber asset components includes any information determined to be necessary by the Responsible Entity to achieve effective property accountability (e.g., manufacturer, model number, serial number, software license information, system/component owner). The component inventory is consistent with the Cyber Security Perimeter.

========== based on CM-8 ==========

R5.2. The Responsible Entity shall develop, document, and maintain a current baseline configuration of all the cyber assets in the Cyber Security Perimeter.

GUIDANCE: This requirement establishes a baseline configuration for the cyber assets. The baseline configuration provides information about a particular component's makeup (e.g., the standard software load for a workstation or notebook computer including updated patch information) and the component's logical placement within the cyber assets architecture. The baseline configuration also provides the Responsible Entity with a well-defined and documented specification to which the cyber assets are built and deviations, if required, are documented in support of mission needs/objectives.

========== based on CM-2 ==========

R5.3. [R5.1] The Responsible Entity shall ensure that all documentation required by Standard CIP-005 reflect the current ~~configurations~~baseline configurations and processes and

shall review the documents and procedures referenced in Standard CIP-005 at least annually.

========== based on CM-2 ==========

R5.4. The Responsible Entity shall:

R5.4.1. Authorize, document, and control changes to the cyber assets in the Cyber Security Perimeter.

R5.4.2. Test, validate, and document changes (e.g., patches and updates) before implementing the changes on the operational CSP.

~~R3.1.1.~~R5.4.3. Employ automated mechanisms to: (i) document proposed changes to the cyber assets; (ii) notify appropriate approval authorities; (iii) highlight approvals that have not been received in a timely manner; (iv) inhibit change until necessary approvals are received; and (v) document completed changes to the cyber assets.

GUIDANCE: The Responsible Entity manages configuration changes to the information system using an Responsible Entity-approved process (e.g., a chartered Configuration Control Board). Configuration change control involves the systematic proposal, justification, implementation, test/evaluation, review, and disposition of changes to the information system, including upgrades and modifications. Configuration change control includes changes to the configuration settings for information technology products (e.g., operating systems, firewalls, routers). The Responsible Entity includes emergency changes in the configuration change control process, including changes resulting from the remediation of flaws. The approvals to implement a change to the information system include successful results from the security analysis of the change. The Responsible Entity audits activities associated with configuration changes to the information system.

The Responsible Entity ensures that testing does not interfere with ICS functions. The individual/group conducting the tests fully understands the Responsible Entity information security policies and procedures, the ICS security policies and procedures, and the specific health, safety, and environmental risks associated with a particular facility and/or process. A production ICS may need to be taken off-line, or replicated to the extent feasible, before testing can be conducted. If an ICS must be taken off-line for testing, the tests are scheduled to occur during planned ICS outages whenever possible. In situations where the Responsible Entity cannot, for operational reasons, conduct live testing of a production ICS, the Responsible Entity employs compensating controls (e.g., providing a replicated system to conduct testing).

In situations where the ICS cannot support the use of automated mechanisms to implement configuration change control, the Responsible Entity employs nonautomated mechanisms or procedures as compensating controls.

========== based on CM-3 ==========

~~R3.2.~~R5.5. [R5.2] The Responsible Entity shall update the documentation to reflect the modification of the cyber assets in the Cyber Security Perimeter~~network or controls~~ within ninety calendar days of the change.

R5.6. The Responsible Entity shall:

R5.6.1. Establish mandatory configuration settings for cyber assets employed within the Cyber Security Perimeter

R5.6.2. Configure the security settings of cyber assets to the most restrictive mode consistent with operational requirements

R5.6.3. Document the configuration settings

R5.6.4. Enforce the configuration settings in all cyber assets

R5.6.5. Employ automated mechanisms to centrally manage, apply, and verify configuration settings. In situations where the cyber assets cannot support the use of automated mechanisms to centrally manage, apply, and verify configuration settings, the Responsible Entity shall employ nonautomated mechanisms or procedures as compensating controls.

==========requirement based on CM-6 Appx F & I ==========

~~R3.3.~~R5.7. [R5.3] The Responsible Entity shall retain electronic access logs for at least ninety calendar days. Logs related to reportable incidents shall be kept in accordance with the requirements of Standard CIP-008.

R6. Identification and Authentication — The Responsible Entity shall maintain identification and authentication to support access control.

~~R3.4.~~R6.1. The Responsible Entity shall require critical cyber assets to uniquely identify and authenticate users (or processes acting on behalf of users).

GUIDANCE: Authentication is the process of establishing confidence in user identities presented. Authentication of user identities is accomplished through the use of passwords, tokens, biometrics, or in the case of multifactor authentication, some combination thereof. Human authentication factors are generally classified into three cases: (1) Something the user has (e.g., ID card, security token, software token, phone, or cell phone); (2) Something the user knows (e.g., a password, pass phrase, or personal identification number (PIN)); and (3) Something the user is or does (e.g., fingerprint or retinal pattern, DNA sequence (there are assorted definitions of what is sufficient), signature or voice recognition, unique bio-electric signals, or another biometric identifier)[1]. The Office of Management and Budget (OMB) has issued guidance that defines levels of authentication[2]. NIST has published further guidance[3].

Where users function as a single group (e.g., control room operators), user identification and authentication may be role-based, group-based, or device-based. For certain ICS, the capability for immediate operator interaction is critical. Local emergency actions for ICS must not be hampered by identification or authentication requirements. Access to these systems may be restricted by appropriate physical security controls. In situations where the ICS cannot support user identification and authentication, or the Responsible Entity determines it is not advisable to perform user identification and authentication due to significant adverse impact on performance, safety, or reliability, the Responsible Entity employs appropriate compensating controls (e.g., providing increased physical security, personnel security, and auditing measures). For example, manual voice authentication of remote personnel and local, manual actions may be required in order to establish a remote access.

Local and remote user access to ICS components is enabled only when necessary, approved, and authenticated. Remote access refers to access to a cyber asset by a user

[1] Derived from *Wikipedia* http://en.wikipedia.org/wiki/Two-factor_authentication, there being no authoritative definition available.

[2] *E-Authentication Guidance for Federal Agencies*, Office of Management and Budget memorandum M 04-04, December 2003.

[3] *Electronic Authentication Guideline*, NIST Special Publication 800-63 Version 1.0.1, September 2004.

(or a cyber asset) communicating through an external network not controlled by the Responsible Entity.

========== based on CA-3 & IA-2 Appx F&I ==========

~~R3.5.~~R6.2. The Responsible Entity shall manage user identifiers by:

- Uniquely identifying each user
- Verifying the identity of each user
- Receiving authorization to issue a user identifier from an appropriate Responsible Entity official
- Issuing the user identifier to the intended party
- Define and implement a period of inactivity for disabling a user identifier
- Archiving user identifiers.

GUIDANCE: Where users function as a single group (e.g., control room operators), user identification may be role-based, group-based, or device-based.

==========requirement based on IA-4 Appx F&I ==========

~~R3.6.~~R6.3. The cyber assets shall identify and authenticate specific devices before establishing a connection.

GUIDANCE: In situations where the ICS cannot support device identification and authentication (e.g., serial devices), the Responsible Entity employs compensating controls

========= requirements and guidance based on IA-3 Appx F&I ==========

R6.4. The Responsible Entity shall manage authenticators by:

R6.4.1. Defining initial authenticator content

R6.4.2. Establishing administrative procedures for initial authenticator distribution, for lost/compromised, or damaged authenticators, and for revoking authenticators

R6.4.3. Changing default authenticators upon information system installation

~~R3.6.1.~~R6.4.4. Changing/refreshing authenticators periodically.

GUIDANCE: Authenticators include, for example, tokens, PKI certificates, biometrics, passwords, and key cards. Users take reasonable measures to safeguard authenticators including maintaining possession of their individual authenticators, not loaning or sharing authenticators with others, and reporting lost or compromised authenticators immediately. For password-based authentication, the cyber assets: (i) protects passwords from unauthorized disclosure and modification when stored and transmitted; (ii) prohibits passwords from being displayed when entered; (iii) enforces password minimum and maximum lifetime restrictions; and (iv) prohibits password reuse for a specified number of generations. For PKI-based authentication, the cyber assets: (i) validates certificates by constructing a certification path to an accepted trust anchor; (ii) establishes user control of the corresponding private key; and (iii) maps the authenticated identity to the user account.

Many ICS devices and software are shipped with factory default authentication credentials to allow for initial installation and configuration. However, factory default authentication credentials are often well known, easily discoverable, present a great

security risk, and therefore must be changed. Authentication may be role-based, group-based, or device-based.

========== requirement and guidance based on IA-5 Appx F&I ==========

~~R3.7.~~R6.5. Cyber Assets shall obscure feedback of authentication information during an interactive human authentication process to protect the information from possible exploitation/use by unauthorized individuals.

GUIDANCE: The feedback from the cyber assets does not provide information that would allow an unauthorized user to compromise the authentication mechanism. Displaying asterisks when a user types in a password is an example of obscuring feedback of authentication information.

========== based on IA-6 ==========

C. Measures

The following measures will be used to demonstrate compliance with the requirements of Standard CIP-005. Responsible entities may document controls either individually or by specified applicable grouping.

M1. Documents about the Electronic Security Perimeter as specified in Requirement R1.

M2. Documentation of the electronic access controls to the Electronic Security Perimeter(s), as specified in Requirement R2.

M3. Documentation of controls implemented to log and monitor access to the Electronic Security Perimeter(s) as specified in Requirement R3.

M4. Documentation of the Responsible Entity's ~~annual vulnerability~~Cyber Security Perimeter assessment as specified in Requirement R4.

M5. Access logs and documentation of review, changes, and log retention as specified in Requirement R5.

M6. Documentation of the indetification and authentication controls as specified in Requirement R6.

~~M5.~~M7. Documentation of the Exception Plans as specified in Section A.6 Exemptions.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Monitoring Responsibility

1.1.1 Regional Reliability Organizations for Responsible Entities.

1.1.2 NERC for Regional Reliability Organization.

1.1.3 Third-party monitor without vested interest in the outcome for NERC.

1.2. Compliance Monitoring Period and Reset Time Frame

Annually.

1.3. Data Retention

1.3.1 The Responsible Entity shall keep logs for a minimum of ninety calendar days, unless longer retention is required pursuant to Standard CIP-008, Requirement R2.

1.3.2 The Responsible Entity shall keep other documents and records required by Standard CIP-005 from the previous full calendar year.

1.3.3 The compliance monitor shall keep audit records for three years.

1.4. Additional Compliance Information

1.4.1 Responsible Entities shall demonstrate compliance through self-certification or audit, as determined by the Compliance Monitor.

1.4.2 Instances where the Responsible Entity cannot conform to its cyber security policy must be documented as exceptions and approved by the designated senior manager or delegate(s). Duly authorized exceptions will not result in noncompliance. Refer to CIP-003 Requirement R3.

2. Levels of Noncompliance

2.1. Level 1:

2.1.1 All document(s) identified in CIP-005 exist, but have not been updated within ninety calendar days of any changes as required; or,

2.1.2 Access to less than 15% of electronic security perimeters is not controlled, monitored; and logged;

2.1.3 Document(s) exist confirming that only necessary network ports and services have been enabled, but no record documenting annual reviews exists; or,

2.1.4 At least one, but not all, of the Electronic Security Perimeter vulnerability assessment items has been performed in the last full calendar year.

2.1.5 The Exception Plan exists but has been approved, but not in the last full calendar year by a Responsibility Entity senior manager.

2.2. Level 2:

2.2.1 All document(s) identified in CIP-005 but have not been updated or reviewed in the previous full calendar year as required; or,

2.2.2 Access to between 15% and 25% of electronic security perimeters is not controlled, monitored; and logged; or,

2.2.3 Documentation and records of vulnerability assessments of the Electronic Security Perimeter(s) exist, but a vulnerability assessment has not been performed in the previous full calendar year.

~~2.2.3~~2.2.4 The Exception Plan exists and has been approved in the last full calendar year by a Responsibility Entity senior manager, but has not been approved in the last full calendar year by the Regional Reliability Organization.

2.3. Level 3:

2.3.1 A document defining the Electronic Security Perimeter(s) exists, but there are one or more Critical Cyber Assets not within the defined Electronic Security Perimeter(s); or,

2.3.2 One or more identified non-critical Cyber Assets is within the Electronic Security Perimeter(s) but not documented; or,

2.3.3 Electronic access controls document(s) exist, but one or more access points have not been identified; or

2.3.4 Electronic access controls document(s) do not identify or describe access controls for one or more access points; or,

2.3.5 Electronic Access Monitoring:

2.3.5.1 Access to between 26% and 50% of Electronic Security Perimeters is not controlled, monitored; and logged; or,

2.3.5.2 Access logs exist, but have not been reviewed within the past ninety calendar days; or,

2.3.6 Documentation and records of vulnerability assessments of the Electronic Security Perimeter(s) exist, but a vulnerability assessment has not been performed for more than two full calendar years.

~~2.3.6~~2.3.7 The Exception Plan exists but has not has been approved in the last full calendar year by a Responsibility Entity senior manager, and has not been approved in the last full calendar year by the Regional Reliability Organization.

2.4. Level 4:

2.4.1 No documented Electronic Security Perimeter exists; or,

2.4.2 No records of access exist; or,

2.4.3 51% or more Electronic Security Perimeters are not controlled, monitored, and logged; or,

2.4.4 Documentation and records of vulnerability assessments of the Electronic Security Perimeter(s) exist, but a vulnerability assessment has not been performed for more than three full calendar years; or,

2.4.5 No documented vulnerability assessment of the Electronic Security Perimeter(s) process exists.

2.4.6 The Exception Plan does not exists.

E. Regional Differences

None identified.

~~**Version History**~~

~~Version~~	~~Date~~	~~Action~~	~~Change Tracking~~
~~1~~	~~01/16/06~~	~~D.2.3.1 Change "Critical Assets," to "Critical Cyber Assets" as intended.~~	~~03/24/06~~

NIST Augmented CIP Glossary

Definitions of Terms Used in Standard

This section includes all newly defined or revised terms used in the proposed standard. Terms already defined in the Reliability Standards Glossary of Terms are not repeated here. New or revised definitions listed below become approved when the proposed standard is approved. When the standard becomes effective, these defined terms will be removed from the individual standard and added to the Glossary.

Critical Assets: Those facilities, systems, and equipment which, if destroyed, damaged, degraded, or otherwise rendered unavailable, would have a significant impact on the ability to serve large quantities of customers for an extended period of time, would have a detrimental impact on the reliability or operability of the Bulk Electric System, or would cause significant risk to public health and safety.

Cyber Assets: Those programmable electronic devices and communication networks including hardware, software, and data.

Critical Cyber Assets: Those Cyber Assets essential to the reliable operation of Critical Assets.

Cyber Security Incident: Any malicious act or suspicious event that:

. • Compromises, or was an attempt to compromise, the Electronic Security Perimeter or Physical Security Perimeter of a Critical Cyber Asset, or,

. • Disrupts, or was an attempt to disrupt, the operation of a Critical Cyber Asset.

~~Electronic~~ Cyber Security Perimeter: The logical border surrounding a network to which Critical Cyber Assets are connected ~~and~~, for which access is controlled. Critical and non-critical Cyber Asset within a defined Cyber Security Perimeter shall protected pursuant to the requirements of the CIPs.

==========

[Discussion is not part of the recommendation. It is provided to assist the drafting committee.]

Information may be stored, transmitted, and processed using multiple ditital and analog media including electro-magnetic fields in space on on media in frequencies commonly described as electrical and optical. For example, fibre optic, infrared, and radio wireless communications are all common, but are not “electronic.” NIST believes that “Electronic” is too limited a term and has replaced it with “Cyber” as being more inclusive.

The last sentence is added to incorporate CIP-005 requirement R1.4.

==========

Dial-up: Use of public or private switched telephone network to establish data communication between modems. Call establishment in the switched telephone network occurs prior to the data communication.

Industrial Control System (ICS): An information system (e.g., a discrete set of information resources) used to control industrial processes such as the bulk electric grid. Industrial control systems include supervisory control and data acquisition (SCADA) systems used to control geographically dispersed assets, as well as distributed control systems (DCS) and smaller control systems using programmable logic controllers to control localized processes. All cyber assets within the Cyber Security Perimeter are part of the ICS.

=========Based on SP 800-53 glossary and 44 U.S.C., Sec. 3502==========

Multifactor Authentication: Electronic authentication (E-authentication) is the process of establishing confidence in user identities electronically presented to an information system. Multifactor authentication is a system wherein more than one different factors are used to authenticate, thereby delivering a higher level of authentication assurance. Using more than one factor is sometimes called strong authentication. Human authentication factors are generally classified into three cases: (1) Something the user has (e.g., ID card, security token, software token, phone, or cell phone); (2) Something the user knows (e.g., a password, pass phrase, or personal identification number (PIN)); and (3) Something the user is or does (e.g., fingerprint or retinal pattern, DNA sequence (there are assorted definitions of what is sufficient), signature or voice recognition, unique bio-electric signals, or another biometric identifier).

===Based on PC Magazine Encyclopedia http://www.pcmag.com/category2/0,2806,1846380,00.asp===

Physical Security Perimeter: The physical six-wall border surrounding computer rooms, telecommunications rooms, operations centers, and other locations in which Critical Cyber Assets are housed and for which access is controlled.

Remote Access: Any access to an Cyber Security Perimeter by a user (or a cyber asset) communicating through an external network not under the control of the Responsible Entity (e.g., the Internet, public switched telephone network).

==========Based on SP 800-53 glossary ==========

Routing of Data Communications Protocols:

Data communication protocols consist of a header, which contains addressing and other information, followed by user data. Data communication protocols can be Routable or Non-routable.

In Routable protocols, the header contains a network address as well as a device address. The network address allows message units (packets or frames) to be

forwarded from a device in one network to a device in another. Examples of routable protocols are TCP/IP, IPX, and DECnet.

In Non-routable protocols, the header contains only a device address and not a network address. They do not incorporate an addressing scheme for sending data from one network to another (i.e., the communicating devices must reside in the same network). Examples of non-routable protocols are NetBIOS and DEC's LAT protocols.

Security Plan: Formal document that provides an overview of the security requirements for the Cyber Security Perimeter and all cyber assets within the Cyber Security Perimeter, and describes the security controls in place or planned for meeting those requirements.

==========Based on SP 800-53 glossary ==========

NIST Example Augmentation of Standard CIP–005

Cyber Security — Cyber Security Perimeter Protection

October 7, 2008

========== General comments ==========

Discussion (set off by "======" and colored blue) is not part of the NIST augmentation. It is provided to assist the drafting committee.

Order 706 ¶ 61 gives the ERO direction to provide additional guidance in the CIPs or in a separate reference document. For convenience, the guidance is placed in this manuscript. This guidance is part of NIST's augmentation.

==========

A. Introduction

1. Title: Cyber Security — ~~Electronic~~ Cyber Security Perimeter~~(s)~~ (CSP) Protection

2. Number: CIP-005-~~1~~2

3. Purpose: Standard CIP-005 requires the identification and protection of the Electronic Security Perimeter(s) inside which all Critical Cyber Assets reside, as well as all access points on the perimeter. Standard CIP-005 should be read as part of a group of standards numbered Standards CIP-002 through CIP-009. Responsible Entities should interpret and apply Standards CIP-002 through CIP-009 ~~using reasonable business judgment~~.

4. Applicability

4.1. [4.1] Within the text of Standard CIP-005, "Responsible Entity" shall mean all entities that could affect the reliability of the bulk electric grid by virtue of cyber connection to any control system component of the bulk electric system.. Responsible Entities include, but are not limited to:

==========

NIST recommends that all entities that could affect the reliability of the bulk electric grid should be included. Advances in digital electronics technology and computer hardware and software have obsoleted prior distinctions among computing, communications, and control systems. Today, all are collectively considered Information Technology (IT). Until recently, Industrial Control Systems (ICS) had little resemblance to traditional information systems in that they were isolated systems running proprietary software and control protocols. However, as these systems have been increasingly integrated more closely into mainstream organizational information systems to promote connectivity, efficiency, and remote access capabilities, they have started to resemble the more traditional information systems. Increasingly, ICS use the same commercially available hardware and software components as are used in the Responsible Entity's traditional information systems. While the change in industrial control system architecture supports new information system capabilities, it also provides significantly less isolation from the outside world for these systems, introducing many of the same vulnerabilities that exist in current networked information systems. The result is an even greater need to secure ICS.

The interconnection of infrastructures has obsoleted prior distinctions. Distribution Systems and Energy Management Systems should be included. Enumeration can be helpful as examples, providing the enumeration states "including, but not limited to."

==========

- Reliability Coordinator.
- Balancing Authority.
- Interchange Authority.
- Transmission Service Provider.

- Transmission Owner.
- Transmission Operator.
- Generator Owner.
- Generator Operator.
- Load Serving Entity.
- NERC.
- Regional Reliability Organizations.

4.2. [4.2] The following are exempt from Standard CIP-005:

4.2.1 [4.2.1] Facilities regulated by the U.S. Nuclear Regulatory Commission or the Canadian Nuclear Safety Commission.

==========

NIST notes that on September 18, 2008 FERC issued the following Proposed Clarification: facilities within a nuclear generation plant in the United States that are not regulated by the U.S. Nuclear Regulatory Commission are subject to compliance with the eight mandatory "CIP" Reliability Standards approved in Commission Order No. 706.

==========

4.2.2 [4.2.2] Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters that are not under the direct control and management of the Responsible Entity..

4.2.3 [4.3.3] Responsible Entities that, in compliance with Standard CIP-002, identify that they have no Critical Cyber Assets.

5. Effective Date: ~~June 1, 2006~~TBD

~~5.~~6. Exceptions

==========

In Order No. 706 FERC directed the development of a framework to provide accountability when a Responsible Entity relies on technical infeasibility or certain other factors to take exception to specific Requirements. FERC specified that the structural elements of this framework include mitigation steps, a remediation plan, a timeline for eliminating use of the technical feasibility exception unless appropriate justification otherwise is provided, regular review of whether it continues to be necessary to invoke the exception, internal approval by the senior manager, wide-area approval through the ERO's audit process, and cooperation with the ERO to provide the Commission with high-level, wide-area analysis regarding the effects the technical feasibility exception on the reliability of the Bulk-Power System. See ¶ 152, 157-163, 178-187, 192-195, and 209-222.

==========

6.1. The Responsible Entity may take exception to any Requirement based on the Responsible Entity's determination that any of the following conditions apply:

- The Requirement interferes with ICS functions
- The Requirement poses a risk to the reliability of the bulk electric grid
- The ICS cannot support the use of the required mechanisms or implement the required function
- The Requirement will have a significant adverse impact on performance, safety, or reliability

6.2. The Responsible Entity shall document all exceptions in an Exception Plan provided to the ERO and Regional Reliability Organization containing:

6.2.1 A convincing argument why the exception is necessary

6.2.2 Compensating controls or mitigation steps to address the intent of the Requirement

6.2.3 A plan of action, milestones, and schedule for implementing the compensating controls or mitigation steps

6.3. The Exception Plan must be approved annually by a Responsibility Entity senior manager.

6.4. The Exception Plan must be approved annually by the Regional Reliability Organization, or the ERO if there is no applicable RRO.

6.5. The ERO must annually audit compliance with the Exception Plan and provide FERC with an annual high-level, wide-area analysis regarding the effects of all exceptions on the reliability of the Bulk-Power System.

B. Requirements

The Responsible Entity shall comply with the following requirements of Standard CIP-005:

==========

Information may be stored, transmitted, and processed using multiple digital and analog media including electro-magnetic fields in space on media in frequencies commonly described as electrical and optical. For example, fiber optic, infrared, and radio wireless communications are all common, but are not "electronic." NIST believes that "Electronic" is too limited a term and has replaced it with "Cyber" as being more inclusive. "Logical" is another term that could be used.

==========

R0. Cyber Security Perimeter Policy and Procedures — The Responsible Entity shall: develop, disseminate, and periodically review and update: (i) a formal, documented, policy on the protection of all Cyber Security Perimeter(s), the cyber assets contained within, and identification and authentication. This policy shall address purpose, scope, roles, responsibilities, management commitment, coordination among Responsible Entity's sub-entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of this policy and associated controls.

GUIDANCE: This requirement does not prescribe an organization structure for the Responsible Entity 's cyber security policy. The Cyber Security Perimeter Policy and Procedures may be included as part of the general information security policy for the Responsible Entity, or the ICS cyber security policy.

========== based on AC-1 & IA-1 ==========

~~R0.~~R1. [R1] ~~Electronic~~ Cyber Security Perimeter — The Responsible Entity shall ensure that every Critical Cyber Asset resides within a~~n Electronic~~ Cyber Security Perimeter. The Responsible Entity shall identify and document the ~~Electronic~~ Cyber Security Perimeter(s) and all access points to the perimeter(s).

~~R0.1.~~R1.1. [R1.1] Access points to the ~~Electronic~~ Cyber Security Perimeter(s) shall include any externally connected communication ~~end~~ interface point (for example, dial-up modems) terminating at any device at ~~within~~ the ~~Electronic~~ Cyber Security Perimeter(s).

==========

The concept of logically locating the modem at the Perimeter eliminates the need to physically protect the circuit between the modem and the Perimeter, as required in CIP-006.

==========

~~R0.2.~~R1.2. [R1.2] For a dial-up accessible Critical Cyber ~~Asset that~~Asset that uses a non-routable protocol, the Responsible Entity shall define an ~~Electronic~~ Cyber Security Perimeter for that single access point at the dial-up device or shall include the Asset within a defined Cyber Security Perimeter.~~.~~

~~R0.3.~~R1.3. [R1.3] Communication links that are not under the direct control and management of any Responsible Entity connecting discrete Electronic Security Perimeters shall not be considered part of the Electronic Security Perimeter. However, ~~end~~ interface points of these communication links ~~within~~ at the Electronic Security Perimeter(s) shall be considered access points to the Electronic Security Perimeter(s).

==========

The interface between assets controlled by the Responsible Entity and assets controlled by another party is not necessarily the end point for communication. The interface may simply be the demarcation between two domains of responsibility and may also provide changes in information representation or addressing (e.g., optical to electronic, network access translation (NAT)).

==========

~~R0.4.~~R1.4. [R1.4] Any non-critical Cyber Asset within a defined ~~Electronic~~ Cyber Security Perimeter shall be identified and protected pursuant to the requirements of Standard CIP-005.

~~R0.5.~~R1.5. [R1.5] Cyber Assets used in the access control and monitoring of the ~~Electronic~~ Cyber Security Perimeter(s) shall be afforded the protective measures as a specified in Standard CIP-003, Standard CIP-004 Requirement R3, Standard CIP-005 Requirements R2 and R3, Standard CIP-006 Requirements R2 and R3, Standard CIP-007, Requirements R1 and R3 through R9, Standard CIP-008, and Standard CIP-009.

~~R0.6.~~R1.6. [R1.6] The Responsible Entity shall maintain documentation of ~~Electronic~~ Cyber Security Perimeter(s), all interconnected Critical and non-critical Cyber Assets within the Electronic Security Perimeter(s), all ~~electronic~~ access points to the ~~Electronic~~ Cyber Security Perimeter(s) and the Cyber Assets deployed for the access control and monitoring of these access points.

GUIDANCE: Any connections to the Internet, or other external networks, communication systems, cyber assets, or information systems that are not under the control of the Responsible Entity, occur through managed interfaces consisting of appropriate boundary protection devices (e.g., proxies, gateways, routers, firewalls, guards, encrypted tunnels) arranged in an effective architecture (e.g., routers protecting firewalls and application gateways residing on a protected subnetwork commonly referred to as a demilitarized zone or DMZ). Cyber assets at any designated alternate processing sites are provided the same levels of protection as that of the primary site.

As part of a defense-in-depth protection strategy, the Responsible Entity considers partitioning higher-impact cyber assets into separate physical domains (or environments) and applying the concepts of managed interfaces described above to restrict or prohibit network access in accordance with the Responsible Entity's assessment of risk .

The Responsible Entity carefully considers the intrinsically shared nature of commercial telecommunications services in the implementation of security controls associated with the use of such services. Commercial telecommunications services are

commonly based on network components and consolidated management systems shared by all attached commercial customers, and may include third party provided access lines and other service elements. Consequently, such interconnecting transmission services may represent sources of increased risk despite contract security provisions. Therefore, when this situation occurs, the Responsible Entity implements appropriate compensating security controls.

========== guidance based on SC-7 ==========

R1.7. The Responsible Entity physically allocates publicly accessible cyber assets to separate subnetworks with separate, physical network interfaces.

GUIDANCE: Publicly accessible cyber assets include, for example, emergency cut-off activators. Generally, public access to ICS information is not permitted.

========== based on SC-7 control enhancement 1 Appx F & I==========

R1.8. The Responsible Entity shall prevent public access into the Responsible Entity's internal networks except as appropriately mediated.

========== based on SC-7 control enhancement 2 ==========

~~R0.7.~~R1.9. The Responsible Entity shall limit the number of access points to the Cyber Security Perimeter to allow for better monitoring of inbound and outbound network traffic.

========== based on SC-7 enhancement 3 ==========

~~R0.8.~~R1.10. The Responsible Entity shall implement a managed interface (boundary protection devices in an effective security architecture) with any external telecommunication service, implementing controls appropriate to the required protection of the confidentiality and integrity of the information being transmitted.

========== based on SC-7 enhancement 4 ==========

~~R1.~~R2. [R2] ~~Electronic~~ Cyber Access Controls — The Responsible Entity shall implement and document the organizational processes and technical and procedural mechanisms for control of ~~electronic~~ cyber access at all ~~electronic~~ cyber access points ~~to~~ at the ~~Electronic~~ Cyber Security Perimeter(s)~~.~~, and at key internal boundaries within the Cyber Security Perimeter(s).

~~R1.1.~~R2.1. [R2.5] The required documentation shall, at least, identify and describe:

~~R1.1.1.~~R2.1.1. [R2.5.1] The processes for access request and authorization.

~~R1.1.2.~~R2.1.2. [R2.5.2]The authentication methods.

~~R1.1.3.~~R2.1.3. [R2.5.3] The review process for authorization rights, in accordance with Standard CIP-004 Requirement R4.

~~R1.1.4.~~R2.1.4. [R2.5.4] The controls used to secure dial-up accessible connections.

GUIDANCE: Any connections to the Internet, or other external networks or information systems, occur through managed interfaces consisting of appropriate boundary protection devices (e.g., proxies, gateways, routers, firewalls, guards, encrypted tunnels) arranged in an effective architecture (e.g., routers protecting firewalls and application gateways residing on a protected subnetwork commonly referred to as a demilitarized zone or DMZ). Cyber security boundary protections at any designated alternate processing sites provide the same levels of protection as that of the primary site.

As part of a defense-in-depth protection strategy, the Responsible Entity considers partitioning higher-impact information systems into separate physical domains (or

environments) and applies the concepts of managed interfaces described above to restrict or prohibit network access in accordance with an Responsible Entity's assessment of risk.

The Responsible Entity carefully considers the intrinsically shared nature of commercial telecommunications services in the implementation of security controls associated with the use of such services. Commercial telecommunications services are commonly based on network components and consolidated management systems shared by all attached commercial customers, and may include third party provided access lines and other service elements. Consequently, such interconnecting transmission services may represent sources of increased risk despite contract security provisions.

========== based on SC-7 ==========

~~R1.2.~~R2.2. [R2.1] These processes and mechanisms shall use an access control model that denies access by default, such that explicit access permissions must be specified.

R2.3. [R2.3] The Responsible Entity shall maintain a procedure for securing dial-up access to the Electronic Security Perimeter(s). The Responsible Entity shall:

R2.3.1. Employ automated mechanisms to facilitate the monitoring and control of dial-up access.

R2.3.2. Determine if cryptography is required to protect the confidentiality and integrity of dial-up access sessions.

R2.3.3. Permit dial-up access for privileged functions only for compelling operational needs and documents the rationale for such access in the security plan for the Cyber Security Perimeter .

GUIDANCE: The Responsible Entity restricts access achieved through dial-up connections (e.g., limiting dial-up access based upon source of request) or protects against unauthorized connections or subversion of authorized connections (e.g., using virtual private network technology). NIST Special Publication 800-63 provides guidance on remote electronic authentication. NIST Special Publication 800-77 provides guidance on IPsec-based virtual private networks.

Dial-up access to ICS locations (e.g., control centers, field locations) is only enabled when necessary, approved, and authenticated. In situations where the ICS cannot support the use of automated mechanisms for monitoring and control of dial-up access methods, the Responsible Entity employs nonautomated mechanisms or procedures as compensating controls (e.g., following manual authentication, dial-in remote access may be enabled for a specified period of time or a call may be placed from the ICS site to the authenticated remote entity).

Cryptography is used for the protection of information and communications. At the core of all products offering cryptographic services is the cryptographic module. Weaknesses such as poor design or weak algorithms can render a product insecure and place highly sensitive information at risk. Adequate testing and validation of the cryptographic module and its underlying cryptographic algorithms against established standards is essential to provide security assurance.

The NIST Cryptographic Module Validation Program (CMVP) validates commercial cryptographic modules to Federal Information Processing Standard (FIPS) 140-2 and other cryptography based standards such as algorithms.

ICS security objectives typically follow the priority of availability, integrity and confidentiality, in that order. The use of cryptography is determined after careful

consideration of the security needs and the potential ramifications on system performance. For example, the Responsible Entity considers whether latency induced from the use of cryptography would adversely impact the operational performance of the ICS.

In situations where the ICS cannot support the use of cryptographic mechanisms to protect the confidentiality and integrity of remote sessions, or the components cannot use cryptographic mechanisms due to significant adverse impact on performance, safety, or reliability, the Responsible Entity employs appropriate compensating controls (e.g., providing increased auditing measures for remote sessions or limiting remote access privileges to key personnel).

==== based on AC-17, IA-7 Appx F&I and other NIST publications===

~~R1.3.~~R2.4. The Responsible Entity shall authorize and document all connections between cyber assets inside the Cyber Security Perimeter and cyber assets outside of the Cyber Security Perimeter.

GUIDANCE: The Responsible Entity carefully considers the risks that may be introduced when cyber assets are connected to other cyber assets with different security requirements and security controls, both within the Responsible Entity and external to the Responsible Entity. Risk considerations also include cyber assets sharing the same networks.

========== additions based on CA-3 ==========

~~R1.4.~~R2.5. [R2.4] Where ~~external interactive~~ access through ~~into~~ the ~~Electronic~~ Cyber Security Perimeter has been authorized and enabled, the Responsible Entity shall implement multifactor ~~strong~~ procedural or technical controls at the access points to ensure authenticity of the accessing ~~party~~parties, ~~where technically feasible~~and monitors/controls the access on an ongoing basis.

GUIDANCE: Multifactor authentication is a system wherein more than one different factors are used to authenticate, thereby delivering a higher level of authentication assurance. Using more than one factor is sometimes called strong authentication.

========== based on IA-2 control enhancement 1 ==========

R2.6. The Responsible Entity shall:

R2.6.1. Employ automated mechanisms to facilitate the monitoring and control of remote access methods.

R2.6.2. Determine if cryptography is required to protect the confidentiality and integrity of remote access sessions.

R2.6.3. Control all remote accesses through a limited number of managed access control points.

R2.6.4. Permit remote access for privileged functions only for compelling operational needs and documents the rationale for such access in the security plan for the Cyber Security Perimeter .

GUIDANCE: Remote access is any access to an Cyber Security Perimeter by a user (or a cyber asset) communicating through an external network not under the control of the Responsible Entity (e.g., the Internet, public switched telephone network). Examples of remote access methods include dial-up, broadband, and wireless. The Responsible Entity protects against unauthorized connections or subversion of authorized connections (e.g., using virtual private network technology). NIST Special

Publication 800-63 provides guidance on remote electronic authentication. NIST Special Publication 800-77 provides guidance on IPsec-based virtual private networks.

Remote access to ICS locations (e.g., control centers, field locations) is only enabled when necessary, approved, and authenticated. In situations where the ICS cannot support the use of automated mechanisms for monitoring and control of remote access methods, the Responsible Entity employs nonautomated mechanisms or procedures as compensating controls.

Cryptography is used for the protection of information and communications. At the core of all products offering cryptographic services is the cryptographic module. Weaknesses such as poor design or weak algorithms can render a product insecure and place highly sensitive information at risk. Adequate testing and validation of the cryptographic module and its underlying cryptographic algorithms against established standards is essential to provide security assurance.

The NIST Cryptographic Module Validation Program (CMVP) validates commercial cryptographic modules to Federal Information Processing Standard (FIPS) 140-2 and other cryptography based standards such as algorithms.

ICS security objectives typically follow the priority of availability, integrity and confidentiality, in that order. The use of cryptography is determined after careful consideration of the security needs and the potential ramifications on system performance. For example, the Responsible Entity considers whether latency induced from the use of cryptography would adversely impact the operational performance of the ICS.

In situations where the ICS cannot support the use of cryptographic mechanisms to protect the confidentiality and integrity of remote sessions, or the components cannot use cryptographic mechanisms due to significant adverse impact on performance, safety, or reliability, the Responsible Entity employs appropriate compensating controls (e.g., providing increased auditing measures for remote sessions or limiting remote access privileges to key personnel).

==== based on AC-17, IA-7 Appx F&I and other NIST publications====

R2.7. The Responsible Entity shall:

R2.7.1. Develop a list of privileged functions

R2.7.2. Develop a list of authorized actions that can be taken with respect to privileged functions

~~R1.4.1.~~**R2.7.3.** Document the criteria and procedures for granting authorization to identified persons and entities.

The Responsible Entity shall manage cyber asset accounts, including establishing, activating, modifying, reviewing, disabling, and removing accounts. Privilege authorizations shall be granted in accordance with established policy and recorded. The Responsible Entity shall determine and implement the frequency for reviewing said accounts, at least annually.

GUIDANCE: Account management includes the identification of account types (i.e., individual, group, and system), establishment of conditions for group membership, and assignment of associated authorizations. The Responsible Entity identifies authorized users of the cyber assets and specifies access rights/privileges. The Responsible Entity grants access to the cyber assets based on: (i) a valid need-to-know/need-to-share that is determined by assigned official duties and satisfying all personnel security criteria; and (ii) intended usage. The Responsible Entity requires proper identification for

requests to establish accounts and approves all such requests. The Responsible Entity specifically authorizes and monitors the use of guest/anonymous accounts and removes, disables, or otherwise secures unnecessary accounts. Account managers are notified when cyber asset users are terminated or transferred and associated accounts are removed, disabled, or otherwise secured. Account managers are also notified when users' cyber asset usage or need-to-know/need-to-share changes.

==========requirement and guidance based on AC-2 ==========

~~R1.5.~~R2.8. The cyber assets shall enforce assigned authorizations for controlling access in accordance with applicable policy.

GUIDANCE: Access control policies (e.g., identity-based policies, role-based policies, rule-based policies) and associated access enforcement mechanisms (e.g., access control lists, access control matrices, cryptography) are employed to control access between users (or processes acting on behalf of users) and objects (e.g., devices, files, records, processes, programs, domains) within the cyber security perimeter. In addition to controlling access at the network layer of the ISO Reference Architecture, access enforcement mechanisms are employed at the application layer, when necessary, to provide increased information security. Consideration is given to the implementation of a controlled, audited, and manual override of automated mechanisms in the event of emergencies or other serious events.

The Responsible Entity ensures that access enforcement mechanisms do not adversely impact the operational performance of the ICS.

========== requirement & guidance based on AC-3 Appx F & I ==========

~~R1.6.~~R2.9. The cyber assets shall restrict access to privileged functions (deployed in hardware, software, and firmware) and security-relevant information to explicitly authorized personnel.

GUIDANCE: Explicitly authorized personnel include, for example, security administrators, system and network administrators, and other privileged users. Privileged users are individuals who have access to system control, monitoring, or administration functions (e.g., system administrators, information system security officers, maintainers, system programmers).

Within ICS, it is commonly the case that having access to specific devices (e.g., workstations, remote terminal units, field devices) is the equivalent to having privileged access; thereby restricting access to these devices is also restricting access to privileged functions and security-relevant information.

========== requirement & guidance based on AC-3 Appx F & I ==========

~~R1.7.~~R2.10. The Responsible Entity shall specify privileged functions that have impacts on facility, public, and environmental safety that require dual authorization.

GUIDANCE: The Responsible Entity does not employ dual-approval mechanisms when an immediate response is necessary to ensure public and environmental safety.

========== requirement & guidance based on AC-3 ICS-1 ==========

~~R1.8.~~R2.11. The cyber assets shall enforce assigned authorizations for controlling the flow of information within the Cyber Security Perimeter and between interconnected Cyber Security Perimeters in accordance with applicable policy.

GUIDANCE: Information flow control regulates where information is allowed to travel within a Cyber Security Perimeter and between Cyber Security Perimeters (as

opposed to who is allowed to access the information) and without explicit regard to subsequent accesses to that information. A few, of many, generalized examples of possible restrictions that are better expressed as flow control than access control are: keeping export controlled information from being transmitted in the clear to the Internet, blocking outside traffic that claims to be from within the Responsible Entity, and not passing any web requests to the Internet that are not from the internal web proxy. Information flow control policies and enforcement mechanisms are commonly employed by Responsible Entities to control the flow of information between designated sources and destinations (e.g., networks, individuals, devices) within Cyber Security Perimeters and between interconnected Cyber Security Perimeters. Flow control is based on the characteristics of the information and/or the information path. Specific examples of flow control enforcement can be found in boundary protection devices (e.g., proxies, gateways, guards, encrypted tunnels, firewalls, and routers) that employ rule sets or establish configuration settings that restrict information system services or provide a packet filtering capability.

========== requirement & guidance based on AC-4 ==========

~~R1.9.~~R2.12. The Responsible Entity shall identify roles and responsibilities where separation of duties is necessary. The cyber assets enforces separation of duties through assigned access authorizations.

GUIDANCE: The Responsible Entity establishes appropriate divisions of responsibility and separates duties as needed to eliminate conflicts of interest in the responsibilities and duties of individuals. There is access control software on the cyber assets that prevents users from having all of the necessary authority or information access to perform fraudulent activity without collusion. Examples of separation of duties include: (i) mission functions and distinct support functions are divided among different individuals/roles; (ii) different individuals perform cyber asset support functions (e.g., system management, systems programming, quality assurance/testing, configuration management, and network security); and (iii) security personnel who administer access control functions do not administer audit functions. In situations where the ICS cannot support the differentiation of roles or a single individual performs all roles within the ICS, the Responsible Entity shall employ appropriate compensating controls (e.g., providing increased personnel security and auditing measures).

========== requirement & guidance based on AC-5 Appx F&I ==========

R2.13. The Responsible Entity shall:

R2.13.1. Approve individual access privileges and enforce cyber access restrictions associated with changes to the critical cyber assets

~~R1.9.1.~~R2.13.2. Generate, retain, and review records reflecting all such changes.

GUIDANCE: Planned or unplanned changes to the hardware, software, and/or firmware components of the cyber assets can have significant effects on the overall security of the system. Accordingly, only qualified and authorized individuals obtain access to information system components for purposes of initiating changes, including upgrades, and modifications. In situations where the ICS cannot support the use of automated mechanisms to enforce access restrictions and support auditing of enforcement actions, the Responsible Entity employs nonautomated mechanisms or procedures as compensating controls

======== based on CM-5 from Appendixes F & I ==========

~~R1.10.~~R2.14. [R2.2] At all access points to the ~~Electronic~~ Cyber Security Perimeter(s) and at all Cyber Assets contained within the Perimeter, the Responsible Entity ~~shall enable~~shall enable only ports, functions, capabilities, and/or ~~services required~~services required for operations ~~and for~~ including monitoring Cyber Assets within the ~~Electronic~~ Cyber Security Perimeter, and shall document, individually or by specified grouping, the configuration of those ports, functions, capabilities, and services.

GUIDANCE: Cyber Assets are capable of providing a wide variety of functions and services. Some of the functions and services, provided by default, may not be necessary to support essential Responsible Entity operations (e.g., key missions, functions). Additionally, it is sometimes convenient to provide multiple services from a single component of a Cyber Asset, but doing so increases risk over limiting the services provided by any one component. The Responsible Entity limits component functionality to a single function per device (e.g., email server or web server, not both). The functions and services provided by Cyber Assets, or individual components of Cyber Assets, should be carefully reviewed to determine which functions and services are candidates for elimination (e.g., Voice Over Internet Protocol, Instant Messaging, File Transfer Protocol, Hyper Text Transfer Protocol, file sharing).

========== additions to requirement based on CM-7 ==========

R2.15. The Responsible Entity shall define and the cyber assets shall automatically enforce:

R2.15.1. A limit of consecutive invalid access attempts by a user during a specified time period, and restrictions on further accesses including

R2.15.2. A defined time period to lock the account, preventing access

~~R1.10.1.~~R2.15.3. A defined time period and algorithm to delays next login prompt.

GUIDANCE: Due to the potential for denial of service, automatic lockouts initiated by the cyber assets are usually temporary and automatically release after a predetermined time period established by the Responsible Entity.

In situations where the ICS cannot support account/node locking or delayed login attempts, or the ICS cannot perform account/node locking or delayed logins due to significant adverse impact on performance, safety, or reliability, the Responsible Entity employs appropriate compensating controls (e.g., logging or recording all unsuccessful login attempts and alerting security personnel though alarms or other means when the number of Responsible Entity-defined consecutive invalid access attempts is exceeded).

========== additions to requirement based on AC-7 Appx F & I ==========

~~R1.11.~~R2.16. The Responsible Entity shall define an interval of user inactivity after which the cyber assets shall initiate a session lock. The session lock remains in effect until the user reestablishes access using appropriate identification and authentication procedures.

GUIDANCE: Users can directly initiate session lock mechanisms. The ICS employs session lock to prevent access to specified workstations/nodes. The ICS activates session lock mechanisms automatically after a time period defined by the Responsible Entity for designated workstations/nodes on the ICS. In some cases, session lock for ICS operator workstations/nodes is not advised (e.g., when immediate operator responses are required in emergency situations). Session lock is not a substitute for logging out of the ICS. In situations where the ICS cannot support session lock, the Responsible Entity employs appropriate compensating controls (e.g., providing increased physical security, personnel security, and auditing measures)

========== additions based on AC-11 Appx F & I ==========

~~R1.12.~~R2.17. For remote access sessions, the Responsible Entity shall define an interval of user inactivity after which the cyber assets shall automatically terminate the session.

GUIDANCE: In situations where the ICS cannot support the automatic termination of remote sessions after a specified period of inactivity, or the ICS cannot automatically terminate remote sessions due to significant adverse impact on performance, safety, or reliability, the Responsible Entity employs nonautomated mechanisms or procedures as compensating controls (e.g., providing increased auditing measures for such sessions or limiting remote access privileges to key personnel).

========== based on AC-12 Appx F & I ==========

~~R1.13.~~R2.18. The Responsible Entity shall identify and document specific user actions that can be performed on the cyber assets without identification or authentication.

GUIDANCE: Emergency switches to stop operations are accessible to any individual with authorized physical access.

========== based on AC-14 ==========

~~R1.14.~~R2.19. [R2.6] Appropriate Use Banner — ~~Where technically feasible, electronic~~ ~~a~~Access control devices shall display an appropriate use banner on the user screen upon all interactive access attempts. The banner shall inform potential users: (i) that the user is accessing a private system; (ii) that system usage may be monitored, recorded, and subject to audit; (iii) that unauthorized use of the system is prohibited and subject to criminal and civil penalties; and (iv) that use of the system indicates consent to monitoring and recording. The banner shall provides appropriate privacy and security notices (based on associated privacy and security policies or summaries) and remains on the screen until the user takes explicit actions to log on. The Responsible Entity shall maintain a document identifying the content of the banner.

========== additions to requirement based on AC-8 ==========

~~R2.~~R3. [R3] Monitoring ~~Electronic~~ Cyber Access — The Responsible Entity shall define, periodically review, and update, a list of auditable events and uses that list to generate audit records. The Responsible Entity shall implement and document an electronic or manual process(es) for monitoring and logging audit records for these events ~~access at access points to the Electronic Security Perimeter(s)~~twenty-four hours a day, seven days a week.

========== additions to requirement based on AU-2 ==========

GUIDANCE: The purpose of monitoring and logging audit records is to identify important events which need to be audited as significant and relevant to the reliability of the bulk electric grid. The Responsible Entity specifies which events require auditing and how the audition is implemented. Auditing activity can affect system performance. Therefore, the Responsible Entity decides, based upon a risk assessment, which events require auditing on a continuous basis and which events require auditing in response to specific situations. Audit records can be generated at various levels of abstraction, including at the packet level as information traverses the network. Selecting the right level of abstraction for audit record generation is a critical aspect of an audit capability and can facilitate the identification of root causes to problems. Additionally, the security audit function is coordinated with the network health and status monitoring function to enhance the mutual support between the two functions by the selection of information to be recorded by each function. The checklists and configuration guides at http://csrc.nist.gov/pcig/cig.html provide recommended lists of auditable events. The Responsible Entity defines auditable events that are adequate to support after-the-fact investigations of security incidents. Most auditing occurs at the application level. In situations where the Responsible Entity cannot support the use of automated mechanisms to generate

audit records, the Responsible Entity employs nonautomated mechanisms or procedures as compensating controls

========== based on AU-2 Appendix F & I ==========

~~R2.1.~~R3.1. Cyber assets shall produce audit records that contain sufficient information to establish what events occurred, the sources of the events, and the outcomes of the events. Cyber assets shall provide the capability to include additional, more detailed information in the audit records for audit events identified by type, location, or subject.

GUIDANCE: Audit record content includes, for most audit records: (i) date and time of the event; (ii) the component of the information system (e.g., software component, hardware component) where the event occurred; (iii) type of event; (iv) user/subject identity; and (v) the outcome (success or failure) of the event.

========== based on AU-3 ==========

~~R2.2.~~R3.2. The Responsible Entity allocates sufficient audit record storage capacity and configures auditing to reduce the likelihood of such capacity being exceeded.

========== based on AU-4 ==========

~~R2.3.~~R3.3. The Responsible Entity shall define actions to be taken in the event of an audit processing failure (e.g., overwrite oldest audit records, stop generating audit records). Cyber assets that perform auditing shall alert appropriate Responsible Entity officials and take these actions in the event of an audit processing failure.

GUIDANCE: Audit processing failures include, for example, software/hardware errors, failures in the audit capturing mechanisms, and audit storage capacity being reached or exceeded. In general, audit record processing is not performed on the ICS, but on a separate information system. In situations where the ICS cannot support auditing including response to audit failures, the Responsible Entity employs compensating controls (e.g., providing an auditing capability on a separate information system).

========== requirement based on AU-5 Appx F & I ==========

~~R2.4.~~R3.4. [R3.1] For dial-up accessible Critical Cyber Assets that use non-routable protocols, the Responsible Entity shall implement and document monitoring process(es) at each access point to the dial-up device~~, where technically feasible.~~.

~~R2.5.~~R3.5. [R3.2] ~~Where technically feasible, t~~The Responsible Entity's security monitoring process(es) shall regularly review/analyze audit records with respect to the enforcement and usage of cyber asset access controls for indications of inappropriate or unusual activity, investigate suspicious activity or suspected violations, detect and alert for attempts at or actual unauthorized accesses. These alerts shall provide for appropriate notification to designated response personnel who take necessary actions. The Responsible Entity shall employ automated mechanisms to facilitate the review of user activities. If the Responsible Entity takes an exception to ~~Where~~ alerting ~~is not technically feasible~~as specified in section A.6, the Responsible Entity shall review or otherwise assess ~~access logs~~audit records for attempts at or actual unauthorized ~~accesses~~ activities at least every ninety calendar days.

GUIDANCE: The Responsible Entity reviews audit records (e.g., user activity logs) for inappropriate activities in accordance with Responsible Entity procedures. The Responsible Entity investigates any unusual cyber asset-related activities and periodically reviews changes to access authorizations. The Responsible Entity reviews more frequently the activities of users with significant cyber asset roles and

responsibilities. In situations where the ICS cannot support the use of automated mechanisms for reviewing user activities, the Responsible Entity employs nonautomated mechanisms or procedures as compensating controls.

Responsible Entities increase the level of audit monitoring and analysis activity within the system whenever there is an indication of increased risk based on law enforcement information, intelligence information, or other credible sources of information.

========== based on AC-13 Appx F & I and AU-6 ==========

~~R2.6.~~R3.6. The Responsible Entity shall define a list of inappropriate or unusual activities with security implications that are to result in automated alerts that shall be sent to designated security personnel.

========== requirements based on AU-6 ==========

R3.7. The Responsible Entity shall provide an audit reduction and report generation capability. The audit reduction and report generation system shall provide the capability to automatically process audit records for events of interest based upon selectable, event criteria..

GUIDANCE: Audit reduction, review, and reporting tools support after-the-fact investigations of security incidents without altering original audit records. In general, audit record processing is not performed on the Critical Cyber Asset, but on a separate cyber asset.

========== based on AU-7 Appx F & I ==========

~~R2.7.~~R3.8. The Responsible Entity shall employ time stamps in audit record generation. The Responsible Entity shall define the frequency for synchronizing internal clocks. The cyber assets shall synchronize internal system clocks at this frequency.

GUIDANCE: Time stamps (including date and time) of audit records are generated using internal system clocks.

========== requirement based on AU-8 ==========

~~R2.8.~~R3.9. The Responsible Entity shall protect audit information and audit tools from unauthorized access, modification, and deletion.

GUIDANCE: Audit information includes all information (e.g., audit records, audit settings, and audit reports) needed to successfully audit information system activity

========== based on AU-9 ==========

R4. -Cyber Security Perimeter Assessment — The Responsible Entity shall establish a program to assess the security of the Cyber Security Perimeter.

R4.1. The Responsible Entity shall develop detailed Cyber Security Perimeter testing standards, processes, and procedures (called "CSP Security Assessment Guide") to provide direction and guidance on security testing; the Guides must:

R4.1.1. Identify who is to be held accountable and responsible for ensuring that information security tests comply with Responsible Entity requirements.

R4.1.2. Identify the Responsible Entity requirements with which security tests must comply, i.e., test scenarios must map to and support security requirements, must specify the minimum set of security controls evaluated during tests, as well as the depth and breadth of tests.

R4.1.3. Specify the appropriate roles and responsibilities, i.e., there must be well-qualified personnel in both security testing and analysis, and care must be

taken to ensure separation of duties when testing; for example, testing and analysis must be performed by an independent person(s).

R4.1.4. Adhere to established methodology that identify and test for security controls for the types of testing being performed, viz., NIST guidelines describe these methods as interview, examine and test.

R4.1.5. Specify a testing environment and criteria to be added per NIST SP 800-53A and SP 800-115 and describe these methods, such as the use of dedicated test equipment that must be used for security testing.

R4.1.6. State the frequency of assessmentswhen and how often testing is to be performed.

R4.1.7. Provide the documentation requirements, such as test plans and test results; i.e., adequately securing the results and analysis information and artifacts from testing.

R4.1.8. Specify the criteria for the analysis of the tests and the dissemination of results and recommendations.

R4.1.9. Develop a plan of action, milestones, and schedule to correct deficiencies found during testing.

~~R2.9.~~R4.2. [R4] Cyber Vulnerability Assessment — The Responsible Entity shall employ a qualified independent agent or team to conduct assessment of (a) ~~perform a~~ cyber vulnerabilities ~~y assessment~~ of the ~~electronic~~ access points to the ~~Electronic~~ Cyber Security Perimeter(s)- at least annually, or when significant new vulnerabilities potentially affecting the cyber assets are identified and reported.. The vulnerability assessment shall be conducted in accordance with the CSP Security Assessment Guide. The vulnerability assessment shall include, at a minimum, the following:

========== based on CA-4 and RA-5 ==========

~~R2.9.1.~~R4.2.1. [R4.1] A document identifying the vulnerability assessment process;

~~R2.9.2.~~R4.2.2. [R4.2] A review to verify that only ports and services required for operations at these access points are enabled;

~~R2.9.3.~~R4.2.3. [R4.3] The discovery of all access points to the ~~Electronic~~ Cyber Security Perimeter;

~~R2.9.4.~~R4.2.4. [R4.4] A review of controls for default accounts, passwords, and network management community strings; ~~and,~~

~~R2.9.5.~~R4.2.5. [R4.5] Documentation of the results of the assessment, the action plan to remediate or mitigate vulnerabilities identified in the assessment, and the execution status of that action plan.

========== based on CA-4 ==========

GUIDANCE: Vulnerability scanning is conducted using appropriate scanning tools and techniques. The Responsible Entity trains selected personnel in the use and maintenance of vulnerability scanning tools and techniques. Vulnerability scans are scheduled and/or random in accordance with Responsible Entity policy and assessment of risk. The information obtained from the vulnerability scanning process is freely shared with appropriate personnel throughout the Responsible Entity to help eliminate similar vulnerabilities in other cyber assets. Vulnerability analysis for custom software and applications may require additional, more specialized approaches (e.g., vulnerability scanning tools for applications, source code reviews, static analysis of source code).

Vulnerability scanning tools are used with care on ICS networks to ensure that ICS functions are not adversely impacted by the scanning process. Production ICS may need to be taken off-line, or replicated to the extent feasible, before scanning can be conducted. If ICS are taken off-line for scanning, scans are scheduled to occur during planned ICS outages whenever possible. If vulnerability scanning tools are used on non-ICS networks, extra care is taken to ensure that they do not scan the ICS network. In situations where the Responsible Entity cannot, for operational reasons, conduct vulnerability scanning on a production ICS, the Responsible Entity employs compensating controls (e.g., providing a replicated system to conduct scanning)

========== guidance based on RA-5 Appx F & I ==========

~~R2.10.~~R4.3. Cyber Control Assessment - The Responsible Entity shall employ a qualified independent agent or team to conduct an assessment of the implementation of all the cyber security controls in the Cyber Security Perimeter at least annually, or when significant new vulnerabilities potentially affecting the cyber assets are identified and reported. The implementation assessment shall -determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements. The implementation assessment shall be conducted in accordance with the CSP Security Assessment Guide.

~~R3.~~R5. [R5] Documentation Review and Maintenance — The Responsible Entity shall review, update, and maintain all documentation to support compliance with the requirements of Standard CIP-005.

R5.1. The Responsible Entity shall develop, document, and maintain a current inventory of the cyber assets in the Cyber Security Perimeter and relevant ownership information. The Responsible Entity shall update the inventory of cyber assets as an integral part of component installations.

GUIDANCE: The Responsible Entity determines the appropriate level of granularity for the cyber asset components included in the inventory that are subject to management control (i.e., tracking, and reporting). The inventory of cyber asset components includes any information determined to be necessary by the Responsible Entity to achieve effective property accountability (e.g., manufacturer, model number, serial number, software license information, system/component owner). The component inventory is consistent with the Cyber Security Perimeter.

========== based on CM-8 ==========

R5.2. The Responsible Entity shall develop, document, and maintain a current baseline configuration of all the cyber assets in the Cyber Security Perimeter.

GUIDANCE: This requirement establishes a baseline configuration for the cyber assets. The baseline configuration provides information about a particular component's makeup (e.g., the standard software load for a workstation or notebook computer including updated patch information) and the component's logical placement within the cyber assets architecture. The baseline configuration also provides the Responsible Entity with a well-defined and documented specification to which the cyber assets are built and deviations, if required, are documented in support of mission needs/objectives.

========== based on CM-2 ==========

R5.3. [R5.1] The Responsible Entity shall ensure that all documentation required by Standard CIP-005 reflect the current ~~configurations~~baseline configurations and processes and

shall review the documents and procedures referenced in Standard CIP-005 at least annually.

========== based on CM-2 ==========

R5.4. The Responsible Entity shall:

R5.4.1. Authorize, document, and control changes to the cyber assets in the Cyber Security Perimeter.

R5.4.2. Test, validate, and document changes (e.g., patches and updates) before implementing the changes on the operational CSP.

~~R3.1.1.~~R5.4.3. Employ automated mechanisms to: (i) document proposed changes to the cyber assets; (ii) notify appropriate approval authorities; (iii) highlight approvals that have not been received in a timely manner; (iv) inhibit change until necessary approvals are received; and (v) document completed changes to the cyber assets.

GUIDANCE: The Responsible Entity manages configuration changes to the information system using an Responsible Entity-approved process (e.g., a chartered Configuration Control Board). Configuration change control involves the systematic proposal, justification, implementation, test/evaluation, review, and disposition of changes to the information system, including upgrades and modifications. Configuration change control includes changes to the configuration settings for information technology products (e.g., operating systems, firewalls, routers). The Responsible Entity includes emergency changes in the configuration change control process, including changes resulting from the remediation of flaws. The approvals to implement a change to the information system include successful results from the security analysis of the change. The Responsible Entity audits activities associated with configuration changes to the information system.

The Responsible Entity ensures that testing does not interfere with ICS functions. The individual/group conducting the tests fully understands the Responsible Entity information security policies and procedures, the ICS security policies and procedures, and the specific health, safety, and environmental risks associated with a particular facility and/or process. A production ICS may need to be taken off-line, or replicated to the extent feasible, before testing can be conducted. If an ICS must be taken off-line for testing, the tests are scheduled to occur during planned ICS outages whenever possible. In situations where the Responsible Entity cannot, for operational reasons, conduct live testing of a production ICS, the Responsible Entity employs compensating controls (e.g., providing a replicated system to conduct testing).

In situations where the ICS cannot support the use of automated mechanisms to implement configuration change control, the Responsible Entity employs nonautomated mechanisms or procedures as compensating controls.

========== based on CM-3 ==========

~~R3.2.~~R5.5. [R5.2] The Responsible Entity shall update the documentation to reflect the modification of the cyber assets in the Cyber Security Perimeter~~network or controls~~ within ninety calendar days of the change.

R5.6. The Responsible Entity shall:

R5.6.1. Establish mandatory configuration settings for cyber assets employed within the Cyber Security Perimeter

R5.6.2. Configure the security settings of cyber assets to the most restrictive mode consistent with operational requirements

R5.6.3. Document the configuration settings

R5.6.4. Enforce the configuration settings in all cyber assets

R5.6.5. Employ automated mechanisms to centrally manage, apply, and verify configuration settings. In situations where the cyber assets cannot support the use of automated mechanisms to centrally manage, apply, and verify configuration settings, the Responsible Entity shall employ nonautomated mechanisms or procedures as compensating controls.

==========requirement based on CM-6 Appx F & I ==========

~~R3.3.~~R5.7. [R5.3] The Responsible Entity shall retain electronic access logs for at least ninety calendar days. Logs related to reportable incidents shall be kept in accordance with the requirements of Standard CIP-008.

R6. Identification and Authentication — The Responsible Entity shall maintain identification and authentication to support access control.

~~R3.4.~~R6.1. The Responsible Entity shall require critical cyber assets to uniquely identify and authenticate users (or processes acting on behalf of users).

GUIDANCE: Authentication is the process of establishing confidence in user identities presented. Authentication of user identities is accomplished through the use of passwords, tokens, biometrics, or in the case of multifactor authentication, some combination thereof. Human authentication factors are generally classified into three cases: (1) Something the user has (e.g., ID card, security token, software token, phone, or cell phone); (2) Something the user knows (e.g., a password, pass phrase, or personal identification number (PIN)); and (3) Something the user is or does (e.g., fingerprint or retinal pattern, DNA sequence (there are assorted definitions of what is sufficient), signature or voice recognition, unique bio-electric signals, or another biometric identifier)[1]. The Office of Management and Budget (OMB) has issued guidance that defines levels of authentication[2]. NIST has published further guidance[3].

Where users function as a single group (e.g., control room operators), user identification and authentication may be role-based, group-based, or device-based. For certain ICS, the capability for immediate operator interaction is critical. Local emergency actions for ICS must not be hampered by identification or authentication requirements. Access to these systems may be restricted by appropriate physical security controls. In situations where the ICS cannot support user identification and authentication, or the Responsible Entity determines it is not advisable to perform user identification and authentication due to significant adverse impact on performance, safety, or reliability, the Responsible Entity employs appropriate compensating controls (e.g., providing increased physical security, personnel security, and auditing measures). For example, manual voice authentication of remote personnel and local, manual actions may be required in order to establish a remote access.

Local and remote user access to ICS components is enabled only when necessary, approved, and authenticated. Remote access refers to access to a cyber asset by a user

[1] Derived from *Wikipedia* http://en.wikipedia.org/wiki/Two-factor_authentication, there being no authoritative definition available.

[2] *E-Authentication Guidance for Federal Agencies*, Office of Management and Budget memorandum M 04-04, December 2003.

[3] *Electronic Authentication Guideline*, NIST Special Publication 800-63 Version 1.0.1, September 2004.

(or a cyber asset) communicating through an external network not controlled by the Responsible Entity.

========== based on CA-3 & IA-2 Appx F&I ==========

~~R3.5.~~R6.2. The Responsible Entity shall manage user identifiers by:

- Uniquely identifying each user
- Verifying the identity of each user
- Receiving authorization to issue a user identifier from an appropriate Responsible Entity official
- Issuing the user identifier to the intended party
- Define and implement a period of inactivity for disabling a user identifier
- Archiving user identifiers.

GUIDANCE: Where users function as a single group (e.g., control room operators), user identification may be role-based, group-based, or device-based.

==========requirement based on IA-4 Appx F&I ==========

~~R3.6.~~R6.3. The cyber assets shall identify and authenticate specific devices before establishing a connection.

GUIDANCE: In situations where the ICS cannot support device identification and authentication (e.g., serial devices), the Responsible Entity employs compensating controls

========= requirements and guidance based on IA-3 Appx F&I ==========

R6.4. The Responsible Entity shall manage authenticators by:

R6.4.1. Defining initial authenticator content

R6.4.2. Establishing administrative procedures for initial authenticator distribution, for lost/compromised, or damaged authenticators, and for revoking authenticators

R6.4.3. Changing default authenticators upon information system installation

~~R3.6.1.~~R6.4.4. Changing/refreshing authenticators periodically.

GUIDANCE: Authenticators include, for example, tokens, PKI certificates, biometrics, passwords, and key cards. Users take reasonable measures to safeguard authenticators including maintaining possession of their individual authenticators, not loaning or sharing authenticators with others, and reporting lost or compromised authenticators immediately. For password-based authentication, the cyber assets: (i) protects passwords from unauthorized disclosure and modification when stored and transmitted; (ii) prohibits passwords from being displayed when entered; (iii) enforces password minimum and maximum lifetime restrictions; and (iv) prohibits password reuse for a specified number of generations. For PKI-based authentication, the cyber assets: (i) validates certificates by constructing a certification path to an accepted trust anchor; (ii) establishes user control of the corresponding private key; and (iii) maps the authenticated identity to the user account.

Many ICS devices and software are shipped with factory default authentication credentials to allow for initial installation and configuration. However, factory default authentication credentials are often well known, easily discoverable, present a great

security risk, and therefore must be changed. Authentication may be role-based, group-based, or device-based.

========== requirement and guidance based on IA-5 Appx F&I ==========

~~R3.7.~~R6.5. Cyber Assets shall obscure feedback of authentication information during an interactive human authentication process to protect the information from possible exploitation/use by unauthorized individuals.

GUIDANCE: The feedback from the cyber assets does not provide information that would allow an unauthorized user to compromise the authentication mechanism. Displaying asterisks when a user types in a password is an example of obscuring feedback of authentication information.

========== based on IA-6 ==========

C. Measures

The following measures will be used to demonstrate compliance with the requirements of Standard CIP-005. Responsible entities may document controls either individually or by specified applicable grouping.

M1. Documents about the Electronic Security Perimeter as specified in Requirement R1.

M2. Documentation of the electronic access controls to the Electronic Security Perimeter(s), as specified in Requirement R2.

M3. Documentation of controls implemented to log and monitor access to the Electronic Security Perimeter(s) as specified in Requirement R3.

M4. Documentation of the Responsible Entity's ~~annual vulnerability~~Cyber Security Perimeter assessment as specified in Requirement R4.

M5. Access logs and documentation of review, changes, and log retention as specified in Requirement R5.

M6. Documentation of the indetification and authentication controls as specified in Requirement R6.

~~M5.~~M7. Documentation of the Exception Plans as specified in Section A.6 Exemptions.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Monitoring Responsibility

1.1.1 Regional Reliability Organizations for Responsible Entities.

1.1.2 NERC for Regional Reliability Organization.

1.1.3 Third-party monitor without vested interest in the outcome for NERC.

1.2. Compliance Monitoring Period and Reset Time Frame

Annually.

1.3. Data Retention

1.3.1 The Responsible Entity shall keep logs for a minimum of ninety calendar days, unless longer retention is required pursuant to Standard CIP-008, Requirement R2.

1.3.2 The Responsible Entity shall keep other documents and records required by Standard CIP-005 from the previous full calendar year.

1.3.3 The compliance monitor shall keep audit records for three years.

1.4. Additional Compliance Information

1.4.1 Responsible Entities shall demonstrate compliance through self-certification or audit, as determined by the Compliance Monitor.

1.4.2 Instances where the Responsible Entity cannot conform to its cyber security policy must be documented as exceptions and approved by the designated senior manager or delegate(s). Duly authorized exceptions will not result in noncompliance. Refer to CIP-003 Requirement R3.

2. Levels of Noncompliance

2.1. Level 1:

2.1.1 All document(s) identified in CIP-005 exist, but have not been updated within ninety calendar days of any changes as required; or,

2.1.2 Access to less than 15% of electronic security perimeters is not controlled, monitored; and logged;

2.1.3 Document(s) exist confirming that only necessary network ports and services have been enabled, but no record documenting annual reviews exists; or,

2.1.4 At least one, but not all, of the Electronic Security Perimeter vulnerability assessment items has been performed in the last full calendar year.

2.1.5 The Exception Plan exists but has been approved, but not in the last full calendar year by a Responsibility Entity senior manager.

2.2. Level 2:

2.2.1 All document(s) identified in CIP-005 but have not been updated or reviewed in the previous full calendar year as required; or,

2.2.2 Access to between 15% and 25% of electronic security perimeters is not controlled, monitored; and logged; or,

2.2.3 Documentation and records of vulnerability assessments of the Electronic Security Perimeter(s) exist, but a vulnerability assessment has not been performed in the previous full calendar year.

~~2.2.3~~2.2.4 The Exception Plan exists and has been approved in the last full calendar year by a Responsibility Entity senior manager, but has not been approved in the last full calendar year by the Regional Reliability Organization.

2.3. Level 3:

2.3.1 A document defining the Electronic Security Perimeter(s) exists, but there are one or more Critical Cyber Assets not within the defined Electronic Security Perimeter(s); or,

2.3.2 One or more identified non-critical Cyber Assets is within the Electronic Security Perimeter(s) but not documented; or,

2.3.3 Electronic access controls document(s) exist, but one or more access points have not been identified; or

2.3.4 Electronic access controls document(s) do not identify or describe access controls for one or more access points; or,

2.3.5 Electronic Access Monitoring:

2.3.5.1 Access to between 26% and 50% of Electronic Security Perimeters is not controlled, monitored; and logged; or,

2.3.5.2 Access logs exist, but have not been reviewed within the past ninety calendar days; or,

2.3.6 Documentation and records of vulnerability assessments of the Electronic Security Perimeter(s) exist, but a vulnerability assessment has not been performed for more than two full calendar years.

~~2.3.6~~2.3.7 The Exception Plan exists but has not has been approved in the last full calendar year by a Responsibility Entity senior manager, and has not been approved in the last full calendar year by the Regional Reliability Organization.

2.4. Level 4:

2.4.1 No documented Electronic Security Perimeter exists; or,

2.4.2 No records of access exist; or,

2.4.3 51% or more Electronic Security Perimeters are not controlled, monitored, and logged; or,

2.4.4 Documentation and records of vulnerability assessments of the Electronic Security Perimeter(s) exist, but a vulnerability assessment has not been performed for more than three full calendar years; or,

2.4.5 No documented vulnerability assessment of the Electronic Security Perimeter(s) process exists.

2.4.6 The Exception Plan does not exists.

E. Regional Differences

None identified.

~~**Version History**~~

~~Version~~	~~Date~~	~~Action~~	~~Change Tracking~~
~~1~~	~~01/16/06~~	~~D.2.3.1 Change "Critical Assets," to "Critical Cyber Assets" as intended.~~	~~03/24/06~~

A. Introduction

1. Title: Cyber Security — Critical Cyber Asset Identification

2. Number: CIP-002-~~1~~2

3. Purpose: NERC Standards CIP-002 through CIP-009 provide a cyber security framework for the identification and protection of Critical Cyber Assets to support reliable operation of the Bulk Electric System.

These standards recognize the differing roles of each entity in the operation of the Bulk Electric System, the criticality and vulnerability of the assets needed to manage Bulk Electric System reliability, and the risks to which they are exposed. ~~Responsible Entities should interpret and apply Standards CIP-002 through CIP-009 using reasonable business judgment.~~

Business and operational demands for managing and maintaining a reliable Bulk Electric System increasingly rely on Cyber Assets supporting critical reliability functions and processes to communicate with each other, across functions and organizations, for services and data. This results in increased risks to these Cyber Assets.

Standard CIP-002 requires the identification and documentation of the Critical Cyber Assets associated with the Critical Assets that support the reliable operation of the Bulk Electric System. These Critical Assets are to be identified through the application of a risk-based assessment.

4. Applicability:

4.1. Within the text of Standard CIP-002, "Responsible Entity" shall mean:

4.1.1 Reliability Coordinator.

4.1.2 Balancing Authority.

4.1.3 Interchange Authority.

4.1.4 Transmission Service Provider.

4.1.5 Transmission Owner.

4.1.6 Transmission Operator.

4.1.7 Generator Owner.

4.1.8 Generator Operator.

4.1.9 Load Serving Entity.

4.1.10 NERC.

4.1.11 Regional Reliability Organizations~~.~~

4.1.12 Regional Entities.

4.2. The following are exempt from Standard CIP-002:

4.2.1 Facilities regulated by the U.S. Nuclear Regulatory Commission or the Canadian Nuclear Safety Commission.

4.2.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

5. Effective Date: ~~June 1, 2006~~XXXX

B. Requirements

The Responsible Entity shall comply with the following requirements of Standard CIP-002:

R1. Critical Asset Identification Method — The Responsible Entity shall identify and document a risk-based assessment methodology to use to identify its Critical Assets.

R1.1. The Responsible Entity shall maintain documentation describing its risk-based assessment methodology that includes procedures and evaluation criteria.

R1.2. The risk-based assessment shall consider the following assets:

R1.2.1. Control centers and backup control centers performing the functions of the entities listed in the Applicability section of this standard.

R1.2.2. Transmission substations that support the reliable operation of the Bulk Electric System.

R1.2.3. Generation resources that support the reliable operation of the Bulk Electric System.

R1.2.4. Systems and facilities critical to system restoration, including blackstart generators and substations in the electrical path of transmission lines used for initial system restoration.

R1.2.5. Systems and facilities critical to automatic load shedding under a common control system capable of shedding 300 MW or more.

R1.2.6. Special Protection Systems that support the reliable operation of the Bulk Electric System.

R1.2.7. Any additional assets that support the reliable operation of the Bulk Electric System that the Responsible Entity deems appropriate to include in its assessment.

R2. Critical Asset Identification — The Responsible Entity shall develop a list of its identified Critical Assets determined through an annual application of the risk-based assessment methodology required in R1. The Responsible Entity shall review this list at least annually, and update it as necessary.

R3. Critical Cyber Asset Identification — Using the list of Critical Assets developed pursuant to Requirement R2, the Responsible Entity shall develop a list of associated Critical Cyber Assets essential to the operation of the Critical Asset. Examples at control centers and backup control centers include systems and facilities at master and remote sites that provide monitoring and control, automatic generation control, real-time power system modeling, and real-time inter-utility data exchange. The Responsible Entity shall review this list at least annually, and update it as necessary. For the purpose of Standard CIP-002, Critical Cyber Assets are further qualified to be those having at least one of the following characteristics:

R3.1. The Cyber Asset uses a routable protocol to communicate outside the Electronic Security Perimeter; or,

R3.2. The Cyber Asset uses a routable protocol within a control center; or,

R3.3. The Cyber Asset is dial-up accessible.

R4. Annual Approval — A senior manager or delegate(s) shall approve annually the risk-based assessment methodology, the list of Critical Assets and the list of Critical Cyber Assets. Based on Requirements R1, R2, and R3 the Responsible Entity may determine that it has no Critical Assets or Critical Cyber Assets. The Responsible Entity shall keep a signed and dated record of the senior manager or delegate(s)'s approval of the risk-based assessment methodology, the list of Critical Assets and the list of Critical Cyber Assets (even if such lists are null.)

C. Measures

The following measures will be used to demonstrate compliance with the requirements of Standard CIP-002:

M1. The risk-based assessment methodology documentation as specified in Requirement R1.

M2. The list of Critical Assets as specified in Requirement R2.

M3. The list of Critical Cyber Assets as specified in Requirement R3.

M4. The records of annual approvals as specified in Requirement R4.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Monitoring Responsibility

1.1.1 Regional Reliability Organizations for Responsible Entities.

1.1.2 NERC for Regional Reliability Organization.

1.1.3 Third-party monitor without vested interest in the outcome for NERC.

1.2. Compliance Monitoring Period and Reset Time Frame

Annually.

1.3. Data Retention

1.3.1 The Responsible Entity shall keep documentation required by Standard CIP-002 from the previous full calendar year

1.3.2 The compliance monitor shall keep audit records for three calendar years.

1.4. Additional Compliance Information

1.4.1 Responsible Entities shall demonstrate compliance through self-certification or audit, as determined by the Compliance Monitor.

2. Levels of Non-Compliance

2.1 Level 1: The risk assessment has not been performed annually.

2.2 Level 2: The list of Critical Assets or Critical Cyber Assets exist, but has not been approved or reviewed in the last calendar year.

2.3 Level 3: The list of Critical Assets or Critical Cyber Assets does not exist.

2.4 Level 4: The lists of Critical Assets and Critical Cyber Assets do not exist.

E. Regional Differences

None identified.

Version History

Version	Date	Action	Change Tracking
1	01/16/06	R3.2 — Change “Control Center” to “control center”	03/24/06

A. Introduction

1. Title: Cyber Security — Security Management Controls

2. Number: CIP-003-~~1~~2

3. Purpose: Standard CIP-003 requires that Responsible Entities have minimum security management controls in place to protect Critical Cyber Assets. Standard CIP-003 should be read as part of a group of standards numbered Standards CIP-002 through CIP-009. ~~Responsible Entities should interpret and apply Standards CIP-002 through CIP-009 using reasonable business judgment~~.

4. Applicability:

4.1. Within the text of Standard CIP-003, "Responsible Entity" shall mean:

4.1.1 Reliability Coordinator.

4.1.2 Balancing Authority.

4.1.3 Interchange Authority.

4.1.4 Transmission Service Provider.

4.1.5 Transmission Owner.

4.1.6 Transmission Operator.

4.1.7 Generator Owner.

4.1.8 Generator Operator.

4.1.9 Load Serving Entity.

4.1.10 NERC.

4.1.11 Regional Reliability Organizations~~.~~

4.1.12 Regional Entities.

4.2. The following are exempt from Standard CIP-003:

4.2.1 Facilities regulated by the U.S. Nuclear Regulatory Commission or the Canadian Nuclear Safety Commission.

4.2.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.3 Responsible Entities that, in compliance with Standard CIP-002, identify that they have no Critical Cyber Assets.

5. Effective Date: ~~June 1, 2006~~XXXX

B. Requirements

The Responsible Entity shall comply with the following requirements of Standard CIP-003:

R1. Cyber Security Policy — The Responsible Entity shall document and implement a cyber security policy that represents management's commitment and ability to secure its Critical Cyber Assets. The Responsible Entity shall, at minimum, ensure the following:

R1.1. The cyber security policy addresses the requirements in Standards CIP-002 through CIP-009, including provision for emergency situations.

R1.2. The cyber security policy is readily available to all personnel who have access to, or are responsible for, Critical Cyber Assets.

R1.3. Annual review and approval of the cyber security policy by the senior manager assigned pursuant to R2.

R2. Leadership — The Responsible Entity shall assign a senior manager with overall responsibility and authority for leading and managing the entity's implementation of, and adherence to, Standards CIP-002 through CIP-009.

R2.1. The senior manager shall be identified by name, title, ~~business phone, business address,~~ and date of designation.

R2.2. Changes to the senior manager must be documented within thirty calendar days of the effective date.

R2.3. Where allowed by Standards CIP-002 through CIP-009, the senior manager may delegate authority for specific actions to a named delegate. These delegations must be documented in the same manner as R2.1 and R2.2, and approved by the senior manager.

~~**R2.3.**~~**R2.4.** The senior manager or delegate(s), shall authorize and document any exception from the requirements of the cyber security policy.

R3. Exceptions — Instances where the Responsible Entity cannot conform to its cyber security policy must be documented as exceptions and authorized by the senior manager or delegate(s).

R3.1. Exceptions to the Responsible Entity's cyber security policy must be documented within thirty days of being approved by the senior manager or delegate(s).

R3.2. Documented exceptions to the cyber security policy must include an explanation as to why the exception is necessary and any compensating measures, or a statement accepting risk.

R3.3. Authorized exceptions to the cyber security policy must be reviewed and approved annually by the senior manager or delegate(s) to ensure the exceptions are still required and valid. Such review and approval shall be documented.

R4. Information Protection — The Responsible Entity shall implement and document a program to identify, classify, and protect information associated with Critical Cyber Assets.

R4.1. The Critical Cyber Asset information to be protected shall include, at a minimum and regardless of media type, operational procedures, lists as required in Standard CIP-002, network topology or similar diagrams, floor plans of computing centers that contain Critical Cyber Assets, equipment layouts of Critical Cyber Assets, disaster recovery plans, incident response plans, and security configuration information.

R4.2. The Responsible Entity shall classify information to be protected under this program based on the sensitivity of the Critical Cyber Asset information.

R4.3. The Responsible Entity shall, at least annually, assess adherence to its Critical Cyber Asset information protection program, document the assessment results, and implement an action plan to remediate deficiencies identified during the assessment.

R5. Access Control — The Responsible Entity shall document and implement a program for managing access to protected Critical Cyber Asset information.

R5.1. The Responsible Entity shall maintain a list of designated personnel who are responsible for authorizing logical or physical access to protected information.

R5.1.1. Personnel shall be identified by name, title, business phone and the information for which they are responsible for authorizing access.

R5.1.2. The list of personnel responsible for authorizing access to protected information shall be verified at least annually.

R5.2. The Responsible Entity shall review at least annually the access privileges to protected information to confirm that access privileges are correct and that they correspond with the Responsible Entity's needs and appropriate personnel roles and responsibilities.

R5.3. The Responsible Entity shall assess and document at least annually the processes for controlling access privileges to protected information.

R6. Change Control and Configuration Management — The Responsible Entity shall establish and document a process of change control and configuration management for adding, modifying, replacing, or removing Critical Cyber Asset hardware or software, and implement supporting configuration management activities to identify, control and document all entity or vendor-related changes to hardware and software components of Critical Cyber Assets pursuant to the change control process.

C. Measures

The following measures will be used to demonstrate compliance with the requirements of Standard CIP-003:

M1. Documentation of the Responsible Entity's cyber security policy as specified in Requirement R1. Additionally, the Responsible Entity shall demonstrate that the cyber security policy is available as specified in Requirement R1.2.

M2. Documentation of the assignment of, and changes to, the Responsible Entity's leadership as specified in Requirement R2.

M3. Documentation of the Responsible Entity's exceptions, as specified in Requirement R3.

M4. Documentation of the Responsible Entity's information protection program as specified in Requirement R4.

M5. The access control documentation as specified in Requirement R5.

M6. The Responsible Entity's change control and configuration management documentation as specified in Requirement R6.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Monitoring Responsibility

1.1.1 Regional Reliability Organizations for Responsible Entities.

1.1.2 NERC for Regional Reliability Organization.

1.1.3 Third-party monitor without vested interest in the outcome for NERC.

1.2. Compliance Monitoring Period and Reset Time Frame

Annually.

1.3. Data Retention

1.3.1 The Responsible Entity shall keep all documentation and records from the previous full calendar year.

1.3.2 The compliance monitor shall keep audit records for three years.

1.4. Additional Compliance Information

1.4.1 Responsible Entities shall demonstrate compliance through self-certification or audit, as determined by the Compliance Monitor.

1.4.2 Instances where the Responsible Entity cannot conform to its cyber security policy must be documented as exceptions and approved by the designated senior manager or delegate(s). Refer to CIP-003, Requirement R3. Duly authorized exceptions will not result in non-compliance.

2. Levels of Noncompliance

2.1. Level 1:

2.1.1 Changes to the designation of senior manager were not documented in accordance with Requirement R2.2; or,

2.1.2 Exceptions from the cyber security policy have not been documented within thirty calendar days of the approval of the exception; or,

2.1.3 An information protection program to identify and classify information and the processes to protect information associated with Critical Cyber Assets has not been assessed in the previous full calendar year.

2.2. Level 2:

2.2.1 A cyber security policy exists, but has not been reviewed within the previous full calendar year; or,

2.2.2 Exceptions to policy are not documented or authorized by the senior manager or delegate(s); or,

2.2.3 Access privileges to the information related to Critical Cyber Assets have not been reviewed within the previous full calendar year; or,

2.2.4 The list of designated personnel responsible to authorize access to the information related to Critical Cyber Assets has not been reviewed within the previous full calendar year.

2.3. Level 3:

2.3.1 A senior manager has not been identified in accordance with Requirement R2.1; or,

2.3.2 The list of designated personnel responsible to authorize logical or physical access to protected information associated with Critical Cyber Assets does not exist; or,

2.3.3 No changes to hardware and software components of Critical Cyber Assets have been documented in accordance with Requirement R6.

2.4. Level 4:

2.4.1 No cyber security policy exists; or,

2.4.2 No identification and classification program for protecting information associated with Critical Cyber Assets exists; or,

2.4.3 No documented change control and configuration management process exists.

E. Regional Differences

None identified.

Version History

Version	Date	Action	Change Tracking

A. Introduction

1. Title: Cyber Security — Personnel & Training

2. Number: CIP-004-~~1~~2

3. Purpose: Standard CIP-004 requires that personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets, including contractors and service vendors, have an appropriate level of personnel risk assessment, training, and security awareness. Standard CIP-004 should be read as part of a group of standards numbered Standards CIP-002 through CIP-009. ~~Responsible Entities should interpret and apply Standards CIP-002 through CIP-009 using reasonable business judgment.~~

4. Applicability:

4.1. Within the text of Standard CIP-004, "Responsible Entity" shall mean:

4.1.1 Reliability Coordinator.

4.1.2 Balancing Authority.

4.1.3 Interchange Authority.

4.1.4 Transmission Service Provider.

4.1.5 Transmission Owner.

4.1.6 Transmission Operator.

4.1.7 Generator Owner.

4.1.8 Generator Operator.

4.1.9 Load Serving Entity.

4.1.10 NERC.

4.1.11 Regional Reliability Organizations~~.~~

4.1.12 Regional Entities.

4.2. The following are exempt from Standard CIP-004:

4.2.1 Facilities regulated by the U.S. Nuclear Regulatory Commission or the Canadian Nuclear Safety Commission.

4.2.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.3 Responsible Entities that, in compliance with Standard CIP-002, identify that they have no Critical Cyber Assets.

5. Effective Date: ~~June 1, 2006~~XXXX

B. Requirements

The Responsible Entity shall comply with the following requirements of Standard CIP-004:

R1. Awareness — The Responsible Entity shall establish, maintain, ~~and~~ document and implement a security awareness program to ensure personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets receive on-going reinforcement in sound security practices. The program shall include security awareness reinforcement on at least a quarterly basis using mechanisms such as:

- Direct communications (e.g., emails, memos, computer based training, etc.);
- Indirect communications (e.g., posters, intranet, brochures, etc.);

Formatted: Indent: Left: 0.25", Hanging: 0.38", Tab stops: 0.63", Left + Not at 1.8"

- Management support and reinforcement (e.g., presentations, meetings, etc.).

R2. Training — The Responsible Entity shall establish, maintain, ~~and~~ document and implement an annual cyber security training program for personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets, and review the program annually and update as necessary.

Formatted: Indent: Left: 0.25", Hanging: 0.38", Tab stops: 0.63", Left

R2.1. This program will ensure that all personnel having such access to Critical Cyber Assets, including contractors and service vendors, are trained ~~within ninety calendar days of such authorization~~prior to their being granted such access.

R2.2. Training shall cover the policies, access controls, and procedures as developed for the Critical Cyber Assets covered by CIP-004, and include, at a minimum, the following required items appropriate to personnel roles and responsibilities:

R2.2.1. The proper use of Critical Cyber Assets;

R2.2.2. Physical and electronic access controls to Critical Cyber Assets;

R2.2.3. The proper handling of Critical Cyber Asset information; and,

R2.2.4. Action plans and procedures to recover or re-establish Critical Cyber Assets and access thereto following a Cyber Security Incident.

R2.3. The Responsible Entity shall maintain documentation that training is conducted at least annually, including the date the training was completed and attendance records.

R3. Personnel Risk Assessment —The Responsible Entity shall have a documented personnel risk assessment program, in accordance with federal, state, provincial, and local laws, and subject to existing collective bargaining unit agreements, for personnel having authorized cyber or authorized unescorted physical access. A personnel risk assessment shall be conducted pursuant to that program ~~within thirty days of~~prior to such personnel being granted such access. Such program shall at a minimum include:

Formatted: Indent: Left: 0.25", Hanging: 0.38", Tab stops: 0.63", Left + Not at 1.8"

R3.1. The Responsible Entity shall ensure that each assessment conducted include, at least, identity verification (e.g., Social Security Number verification in the U.S.) and seven-year criminal check. The Responsible Entity may conduct more detailed reviews, as permitted by law and subject to existing collective bargaining unit agreements, depending upon the criticality of the position.

R3.2. The Responsible Entity shall update each personnel risk assessment at least every seven years after the initial personnel risk assessment or for cause.

R3.3. The Responsible Entity shall document the results of personnel risk assessments of its personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets, and that personnel risk assessments of contractor and service vendor personnel with such access are conducted pursuant to Standard CIP-004.

R4. Access — The Responsible Entity shall maintain list(s) of personnel with authorized cyber or authorized unescorted physical access to Critical Cyber Assets, including their specific electronic and physical access rights to Critical Cyber Assets.

Formatted: Indent: Left: 0.25", Hanging: 0.38", Tab stops: 0.63", Left + Not at 1.8"

R4.1. The Responsible Entity shall review the list(s) of its personnel who have such access to Critical Cyber Assets quarterly, and update the list(s) within seven calendar days of any change of personnel with such access to Critical Cyber Assets, or any change in the access rights of such personnel. The Responsible Entity shall ensure access list(s) for contractors and service vendors are properly maintained.

R4.2. The Responsible Entity shall revoke such access to Critical Cyber Assets within 24 hours for personnel terminated for cause and within seven calendar days for personnel who no longer require such access to Critical Cyber Assets.

C. Measures

The following measures will be used to demonstrate compliance with the requirements of Standard CIP-004:

M1. Documentation of the Responsible Entity's security awareness and reinforcement program as specified in Requirement R1.

M2. Documentation of the Responsible Entity's cyber security training program, review, and records as specified in Requirement R2.

M3. Documentation of the personnel risk assessment program and that personnel risk assessments have been applied to all personnel who have authorized cyber or authorized unescorted physical access to Critical Cyber Assets, as specified in Requirement R3.

M4. Documentation of the list(s), list review and update, and access revocation as needed as specified in Requirement R4.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Monitoring Responsibility

1.1.1 Regional Reliability Organizations for Responsible Entities.

1.1.2 NERC for Regional Reliability Organization.

1.1.3 Third-party monitor without vested interest in the outcome for NERC.

1.2. Compliance Monitoring Period and Reset Time Frame

Annually.

1.3. Data Retention

1.3.1 The Responsible Entity shall keep personnel risk assessment documents in accordance with federal, state, provincial, and local laws.

1.3.2 The Responsible Entity shall keep all other documentation required by Standard CIP-004 from the previous full calendar year.

1.3.3 The compliance monitor shall keep audit records for three calendar years.

1.4. Additional Compliance Information

1.4.1 Responsible Entities shall demonstrate compliance through self-certification or audit, as determined by the Compliance Monitor.

1.4.2 Instances where the Responsible Entity cannot conform to its cyber security policy must be documented as exceptions and approved by the designated senior manager or delegate(s). Duly authorized exceptions will not result in non-compliance. Refer to CIP-003 Requirement R3.

2. Levels of Noncompliance

2.1. Level 1:

2.1.1 Awareness program exists, but is not conducted within the minimum required period of quarterly reinforcement; or,

2.1.2 Training program exists, but records of training either do not exist or reveal that personnel who have access to Critical Cyber Assets were not trained as required; or,

2.1.3 Personnel risk assessment program exists, but documentation of that program does not exist; or,

2.1.4 List(s) of personnel with their access rights is available, but has not been reviewed and updated as required.

2.1.5 One personnel risk assessment is not updated at least every seven years, or for cause; or,

2.1.6 One instance of personnel (employee, contractor or service provider) change other than for cause in which access to Critical Cyber Assets was no longer needed was not revoked within seven calendar days.

2.2. Level 2:

2.2.1 Awareness program does not exist or is not implemented; or,

2.2.2 Training program exists, but does not address the requirements identified in Standard CIP-004; or,

2.2.3 Personnel risk assessment program exists, but assessments are not conducted as required; or,

2.2.4 One instance of personnel termination for cause (employee, contractor or service provider) in which access to Critical Cyber Assets was not revoked within 24 hours.

2.3. Level 3:

2.3.1 Training program exists, but has not been reviewed and updated at least annually; or,

2.3.2 A personnel risk assessment program exists, but records reveal program does not meet the requirements of Standard CIP-004; or,

2.3.3 List(s) of personnel with their access control rights exists, but does not include service vendors and contractors.

2.4. Level 4:

2.4.1 No documented training program exists; or,

2.4.2 No documented personnel risk assessment program exists; or,

2.4.3 No required documentation created pursuant to the training or personnel risk assessment programs exists.

E. Regional Differences

None identified.

Version History

Version	Date	Action	Change Tracking
1	01/16/06	D.2.2.4 — Insert the phrase "for cause" as intended. "One instance of personnel termination for cause…"	03/24/06
1	06/01/06	D.2.1.4 — Change "access control rights" to "access rights."	06/05/06

A. Introduction

1. Title: Cyber Security — Electronic Security Perimeter(s)

2. Number: CIP-005-~~1~~2

3. Purpose: Standard CIP-005 requires the identification and protection of the Electronic Security Perimeter(s) inside which all Critical Cyber Assets reside, as well as all access points on the perimeter. Standard CIP-005 should be read as part of a group of standards numbered Standards CIP-002 through CIP-009. ~~Responsible Entities should interpret and apply Standards CIP-002 through CIP-009 using reasonable business judgment.~~

4. Applicability

4.1. Within the text of Standard CIP-005, "Responsible Entity" shall mean:

4.1.1 Reliability Coordinator.

4.1.2 Balancing Authority.

4.1.3 Interchange Authority.

4.1.4 Transmission Service Provider.

4.1.5 Transmission Owner.

4.1.6 Transmission Operator.

4.1.7 Generator Owner.

4.1.8 Generator Operator.

4.1.9 Load Serving Entity.

4.1.10 NERC.

4.1.11 Regional Entities

~~4.1.11~~**4.1.12** Regional Reliability Organizations.

4.2. The following are exempt from Standard CIP-005:

4.2.1 Facilities regulated by the U.S. Nuclear Regulatory Commission or the Canadian Nuclear Safety Commission.

4.2.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.3 Responsible Entities that, in compliance with Standard CIP-002, identify that they have no Critical Cyber Assets.

5. Effective Date: ~~June 1, 2006~~XXXX

B. Requirements

The Responsible Entity shall comply with the following requirements of Standard CIP-005:

R1. Electronic Security Perimeter — The Responsible Entity shall ensure that every Critical Cyber Asset resides within an Electronic Security Perimeter. The Responsible Entity shall identify and document the Electronic Security Perimeter(s) and all access points to the perimeter(s).

R1.1. Access points to the Electronic Security Perimeter(s) shall include any externally connected communication end point (for example, dial-up modems) terminating at any device within the Electronic Security Perimeter(s).

R1.2. For a dial-up accessible Critical Cyber Asset that uses a non-routable protocol, the Responsible Entity shall define an Electronic Security Perimeter for that single access point at the dial-up device.

R1.3. Communication links connecting discrete Electronic Security Perimeters shall not be considered part of the Electronic Security Perimeter. However, end points of these communication links within the Electronic Security Perimeter(s) shall be considered access points to the Electronic Security Perimeter(s).

R1.4. Any non-critical Cyber Asset within a defined Electronic Security Perimeter shall be identified and protected pursuant to the requirements of Standard CIP-005.

R1.5. Cyber Assets used in the access control and/or monitoring of the Electronic Security Perimeter(s) shall be afforded the protective measures as a specified in Standard CIP-003~~,~~; Standard CIP-004-1 Requirement R3~~,~~; Standard CIP-005-1 Requirements R2 and R3~~,~~; Standard CIP-006-1 Requirements R2 and R3~~,~~; Standard CIP-007-1, Requirements R1 and R3 through R9~~,~~; Standard CIP-008~~,~~; and Standard CIP-009.

R1.6. The Responsible Entity shall maintain documentation of Electronic Security Perimeter(s), all interconnected Critical and non-critical Cyber Assets within the Electronic Security Perimeter(s), all electronic access points to the Electronic Security Perimeter(s) and the Cyber Assets deployed for the access control and monitoring of these access points.

R2. Electronic Access Controls — The Responsible Entity shall implement and document the organizational processes and technical and procedural mechanisms for control of electronic access at all electronic access points to the Electronic Security Perimeter(s).

R2.1. These processes and mechanisms shall use an access control model that denies access by default, such that explicit access permissions must be specified.

R2.2. At all access points to the Electronic Security Perimeter(s), the Responsible Entity shall enable only ports and services required for operations and for monitoring Cyber Assets within the Electronic Security Perimeter, and shall document, individually or by specified grouping, the configuration of those ports and services.

R2.3. The Responsible Entity shall maintain and implement a procedure for securing dial-up access to the Electronic Security Perimeter(s).

R2.4. Where external interactive access into the Electronic Security Perimeter has been enabled, the Responsible Entity shall implement strong procedural or technical controls at the access points to ensure authenticity of the accessing party, where technically feasible.

R2.5. The required documentation shall, at least, identify and describe:

R2.5.1. The processes for access request and authorization.

R2.5.2. The authentication methods.

R2.5.3. The review process for authorization rights, in accordance with Standard CIP-004-1 Requirement R4.

R2.5.4. The controls used to secure dial-up accessible connections.

R2.6. Appropriate Use Banner — Where technically feasible, electronic access control devices shall display an appropriate use banner on the user screen upon all interactive access attempts. The Responsible Entity shall maintain a document identifying the content of the banner.

R3. Monitoring Electronic Access — The Responsible Entity shall implement and document an electronic or manual process(es) for monitoring and logging access at access points to the Electronic Security Perimeter(s) twenty-four hours a day, seven days a week.

R3.1. For dial-up accessible Critical Cyber Assets that use non-routable protocols, the Responsible Entity shall implement and document monitoring process(es) at each access point to the dial-up device, where technically feasible.

R3.2. Where technically feasible, the security monitoring process(es) shall detect and alert for attempts at or actual unauthorized accesses. These alerts shall provide for appropriate notification to designated response personnel. Where alerting is not technically feasible, the Responsible Entity shall review or otherwise assess access logs for attempts at or actual unauthorized accesses at least every ninety calendar days.

R4. Cyber Vulnerability Assessment — The Responsible Entity shall perform a cyber vulnerability assessment of the electronic access points to the Electronic Security Perimeter(s) at least annually. The vulnerability assessment shall include, at a minimum, the following:

R4.1. A document identifying the vulnerability assessment process;

R4.2. A review to verify that only ports and services required for operations at these access points are enabled;

R4.3. The discovery of all access points to the Electronic Security Perimeter;

R4.4. A review of controls for default accounts, passwords, and network management community strings; and,

R4.5. Documentation of the results of the assessment, the action plan to remediate or mitigate vulnerabilities identified in the assessment, and the execution status of that action plan.

R5. Documentation Review and Maintenance — The Responsible Entity shall review, update, and maintain all documentation to support compliance with the requirements of Standard CIP-005.

R5.1. The Responsible Entity shall ensure that all documentation required by Standard CIP-005 reflect current configurations and processes and shall review the documents and procedures referenced in Standard CIP-005 at least annually.

R5.2. The Responsible Entity shall update the documentation to reflect the modification of the network or controls within ninety calendar days of the change.

R5.3. The Responsible Entity shall retain electronic access logs for at least ninety calendar days. Logs related to reportable incidents shall be kept in accordance with the requirements of Standard CIP-008.

C. Measures

The following measures will be used to demonstrate compliance with the requirements of Standard CIP-005. Responsible entities may document controls either individually or by specified applicable grouping.

M1. Documents about the Electronic Security Perimeter as specified in Requirement R1.

M2. Documentation of the electronic access controls to the Electronic Security Perimeter(s), as specified in Requirement R2.

M3. Documentation of controls implemented to log and monitor access to the Electronic Security Perimeter(s) as specified in Requirement R3.

M4. Documentation of the Responsible Entity's annual vulnerability assessment as specified in Requirement R4.

M5. Access logs and documentation of review, changes, and log retention as specified in Requirement R5.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Monitoring Responsibility

1.1.1 Regional Reliability Organizations for Responsible Entities.

1.1.2 NERC for Regional Reliability Organization.

1.1.3 Third-party monitor without vested interest in the outcome for NERC.

1.2. Compliance Monitoring Period and Reset Time Frame

Annually.

1.3. Data Retention

1.3.1 The Responsible Entity shall keep logs for a minimum of ninety calendar days, unless longer retention is required pursuant to Standard CIP-008, Requirement R2.

1.3.2 The Responsible Entity shall keep other documents and records required by Standard CIP-005 from the previous full calendar year.

1.3.3 The compliance monitor shall keep audit records for three years.

1.4. Additional Compliance Information

1.4.1 Responsible Entities shall demonstrate compliance through self-certification or audit, as determined by the Compliance Monitor.

1.4.2 Instances where the Responsible Entity cannot conform to its cyber security policy must be documented as exceptions and approved by the designated senior manager or delegate(s). Duly authorized exceptions will not result in noncompliance. Refer to CIP-003 Requirement R3.

2. Levels of Noncompliance

2.1. Level 1:

2.1.1 All document(s) identified in CIP-005 exist, but have not been updated within ninety calendar days of any changes as required; or,

2.1.2 Access to less than 15% of electronic security perimeters is not controlled, monitored; and logged;

2.1.3 Document(s) exist confirming that only necessary network ports and services have been enabled, but no record documenting annual reviews exists; or,

2.1.4 At least one, but not all, of the Electronic Security Perimeter vulnerability assessment items has been performed in the last full calendar year.

2.2. Level 2:

2.2.1 All document(s) identified in CIP-005 but have not been updated or reviewed in the previous full calendar year as required; or,

2.2.2 Access to between 15% and 25% of electronic security perimeters is not controlled, monitored; and logged; or,

2.2.3 Documentation and records of vulnerability assessments of the Electronic Security Perimeter(s) exist, but a vulnerability assessment has not been performed in the previous full calendar year.

2.3. Level 3:

2.3.1 A document defining the Electronic Security Perimeter(s) exists, but there are one or more Critical Cyber Assets not within the defined Electronic Security Perimeter(s); or,

2.3.2 One or more identified non-critical Cyber Assets is within the Electronic Security Perimeter(s) but not documented; or,

2.3.3 Electronic access controls document(s) exist, but one or more access points have not been identified; or

2.3.4 Electronic access controls document(s) do not identify or describe access controls for one or more access points; or,

2.3.5 Electronic Access Monitoring:

2.3.5.1 Access to between 26% and 50% of Electronic Security Perimeters is not controlled, monitored; and logged; or,

2.3.5.2 Access logs exist, but have not been reviewed within the past ninety calendar days; or,

2.3.6 Documentation and records of vulnerability assessments of the Electronic Security Perimeter(s) exist, but a vulnerability assessment has not been performed for more than two full calendar years.

2.4. Level 4:

2.4.1 No documented Electronic Security Perimeter exists; or,

2.4.2 No records of access exist; or,

2.4.3 51% or more Electronic Security Perimeters are not controlled, monitored, and logged; or,

2.4.4 Documentation and records of vulnerability assessments of the Electronic Security Perimeter(s) exist, but a vulnerability assessment has not been performed for more than three full calendar years; or,

2.4.5 No documented vulnerability assessment of the Electronic Security Perimeter(s) process exists.

E. Regional Differences

None identified.

Version History

Version	Date	Action	Change Tracking
1	01/16/06	D.2.3.1 — Change “Critical Assets,” to “Critical Cyber Assets” as intended.	03/24/06

A. Introduction

1. Title: Cyber Security — Physical Security of Critical Cyber Assets

2. Number: CIP-006-~~1~~2

3. Purpose: Standard CIP-006 is intended to ensure the implementation of a physical security program for the protection of Critical Cyber Assets. Standard CIP-006 should be read as part of a group of standards numbered Standards CIP-002 through CIP-009. ~~Responsible Entities should apply Standards CIP-002 through CIP-009 using reasonable business judgment.~~

4. Applicability:

4.1. Within the text of Standard CIP-006, "Responsible Entity" shall mean:

4.1.1 Reliability Coordinator.

4.1.2 Balancing Authority.

4.1.3 Interchange Authority.

4.1.4 Transmission Service Provider.

4.1.5 Transmission Owner.

4.1.6 Transmission Operator.

4.1.7 Generator Owner.

4.1.8 Generator Operator.

4.1.9 Load Serving Entity.

4.1.10 NERC.

4.1.11 Regional Entities

~~4.1.11~~**4.1.12** Regional Reliability Organizations.

4.2. The following are exempt from Standard CIP-006:

4.2.1 Facilities regulated by the U.S. Nuclear Regulatory Commission or the Canadian Nuclear Safety Commission.

4.2.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.3 Responsible Entities that, in compliance with Standard CIP-002, identify that they have no Critical Cyber Assets.

5. Effective Date: ~~June 1, 2006~~XXXX

B. Requirements

The Responsible Entity shall comply with the following requirements of Standard CIP-006:

R1. Physical Security Plan — The Responsible Entity shall create ~~and~~ , maintain and implement a physical security plan, approved by ~~a~~ the senior manager or delegate(s) that shall address, at a minimum, the following:

R1.1. Processes to ensure and document that all Cyber Assets within an Electronic Security Perimeter also reside within an identified Physical Security Perimeter. Where a completely enclosed ("six-wall") border cannot be established, the Responsible Entity shall deploy and document alternative measures to control physical access to the Critical Cyber Assets.

R1.2. Processes to identify all access points through each Physical Security Perimeter and implement measures to control entry at those access points.

R1.3. Processes, tools, and procedures to monitor physical access to the perimeter(s).

R1.4. Procedures for and implemention of the appropriate use of physical access controls as described in Requirement R3 including visitor pass management, response to loss, and prohibition of inappropriate use of physical access controls.

R1.5. Procedures for reviewing access authorization requests and revocation of access authorization, in accordance with CIP-004 Requirement R4.

R1.6. Procedures for and implemention of escorted access within the physical security perimeter of personnel not authorized for unescorted access.

R1.7. Process for updating the physical security plan within ~~ninety~~thirty calendar days of implementation of any physical security system redesign or reconfiguration, including, but not limited to, addition or removal of access points through the physical security perimeter, physical access controls, monitoring controls, or logging controls.

R1.8. Cyber Assets used in the access control and/or monitoring of the Physical Security Perimeter(s) shall be afforded the protective measures specified in Standard CIP-003~~,~~-1; Standard CIP-004-1 Requirement R3~~,~~; Standard CIP-005-1 Requirements R2 and R3~~,~~; Standard CIP-006-1 Requirement R2 and R3~~,~~; Standard CIP-007~~,~~-1; Standard CIP-008-1; and Standard CIP-009-1.

R1.9. Process for ensuring that the physical security plan is reviewed at least annually.

R2. Physical Access Controls — The Responsible Entity shall document and implement the operational and procedural controls to manage physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week. The Responsible Entity shall implement one or more of the following physical access methods:

R2.1. Card Key: A means of electronic access where the access rights of the card holder are predefined in a computer database. Access rights may differ from one perimeter to another.

R2.2. Special Locks: These include, but are not limited to, locks with "restricted key" systems, magnetic locks that can be operated remotely, and "man-trap" systems.

R2.3. Security Personnel: Personnel responsible for controlling physical access who may reside on-site or at a monitoring station.

R2.4. Other Authentication Devices: Biometric, keypad, token, or other equivalent devices that control physical access to the Critical Cyber Assets.

R3. Monitoring Physical Access — The Responsible Entity shall document and implement the technical and procedural controls for monitoring physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week. Unauthorized access attempts shall be reviewed immediately and handled in accordance with the procedures specified in Requirement CIP-008. One or more of the following monitoring methods shall be used:

R3.1. Alarm Systems: Systems that alarm to indicate a door, gate or window has been opened without authorization. These alarms must provide for immediate notification to personnel responsible for response.

R3.2. Human Observation of Access Points: Monitoring of physical access points by authorized personnel as specified in Requirement R2.3.

R4. Logging Physical Access — Logging shall record sufficient information to uniquely identify individuals and the time of access twenty-four hours a day, seven days a week. The Responsible Entity shall implement and document the technical and procedural mechanisms for logging physical entry at all access points to the Physical Security Perimeter(s) using one or more of the following logging methods or their equivalent:

R4.1. Computerized Logging: Electronic logs produced by the Responsible Entity's selected access control and monitoring method.

R4.2. Video Recording: Electronic capture of video images of sufficient quality to determine identity.

R4.3. Manual Logging: A log book or sign-in sheet, or other record of physical access maintained by security or other personnel authorized to control and monitor physical access as specified in Requirement R2.3.

R5. Access Log Retention — The responsible entity shall retain physical access logs for at least ninety calendar days. Logs related to reportable incidents shall be kept in accordance with the requirements of Standard CIP-008.

R6. Maintenance and Testing — The Responsible Entity shall implement a maintenance and testing program to ensure that all physical security systems under Requirements R2, R3, and R4 function properly. The program must include, at a minimum, the following:

R6.1. Testing and maintenance of all physical security mechanisms on a cycle no longer than three years.

R6.2. Retention of testing and maintenance records for the cycle determined by the Responsible Entity in Requirement R6.1.

R6.3. Retention of outage records regarding access controls, logging, and monitoring for a minimum of one calendar year.

C. Measures

The following measures will be used to demonstrate compliance with the requirements of Standard CIP-006:

M1. The physical security plan as specified in Requirement R1 and documentation of the review and updating of the plan.

M2. Documentation identifying the methods for controlling physical access to each access point of a Physical Security Perimeter as specified in Requirement R2.

M3. Documentation identifying the methods for monitoring physical access as specified in Requirement R3.

M4. Documentation identifying the methods for logging physical access as specified in Requirement R4.

M5. Access logs as specified in Requirement R5.

M6. Documentation as specified in Requirement R6.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Monitoring Responsibility

1.1.1 Regional Reliability Organizations for Responsible Entities.

1.1.2 NERC for Regional Reliability Organization.

1.1.3 Third-party monitor without vested interest in the outcome for NERC.

1.2. Compliance Monitoring Period and Reset Time Frame

Annually.

1.3. Data Retention

1.3.1 The Responsible Entity shall keep documents other than those specified in Requirements R5 and R6.2 from the previous full calendar year.

1.3.2 The compliance monitor shall keep audit records for three calendar years.

1.4. Additional Compliance Information

1.4.1 Responsible Entities shall demonstrate compliance through self-certification or audit, as determined by the Compliance Monitor.

1.4.2 Instances where the Responsible Entity cannot conform to its cyber security policy must be documented as exceptions and approved by the designated senior manager or delegate(s). Duly authorized exceptions will not result in noncompliance. Refer to Standard CIP-003 Requirement R3.

1.4.3 The Responsible Entity may not make exceptions in its cyber security policy to the creation, documentation, or maintenance of a physical security plan.

1.4.4 For dial-up accessible Critical Cyber Assets that use non-routable protocols, the Responsible Entity shall not be required to comply with Standard CIP-006 for that single access point at the dial-up device.

Comment [th1]: Address SCE&G RFI

2. Levels of Noncompliance

2.1. Level 1:

2.1.1 The physical security plan exists, but has not been updated within ninety calendar days of a modification to the plan or any of its components; or,

2.1.2 Access to less than 15% of a Responsible Entity's total number of physical security perimeters is not controlled, monitored, and logged; or,

2.1.3 Required documentation exists but has not been updated within ninety calendar days of a modification.; or,

2.1.4 Physical access logs are retained for a period shorter than ninety days; or,

2.1.5 A maintenance and testing program for the required physical security systems exists, but not all have been tested within the required cycle; or,

2.1.6 One required document does not exist.

2.2. Level 2:

2.2.1 The physical security plan exists, but has not been updated within six calendar months of a modification to the plan or any of its components; or,

2.2.2 Access to between 15% and 25% of a Responsible Entity's total number of physical security perimeters is not controlled, monitored, and logged; or,

2.2.3 Required documentation exists but has not been updated within six calendar months of a modification; or

2.2.4 More than one required document does not exist.

2.3. Level 3:

2.3.1 The physical security plan exists, but has not been updated or reviewed in the last twelve calendar months of a modification to the physical security plan; or,

2.3.2 Access to between 26% and 50% of a Responsible Entity's total number of physical security perimeters is not controlled, monitored, and logged; or,

2.3.3 No logs of monitored physical access are retained.

2.4. Level 4:

2.4.1 No physical security plan exists; or,

2.4.2 Access to more than 51% of a Responsible Entity's total number of physical security perimeters is not controlled, monitored, and logged; or,

2.4.3 No maintenance or testing program exists.

E. Regional Differences

None identified.

Version History

Version	Date	Action	Change Tracking

A. Introduction

1. Title: Cyber Security — Systems Security Management

2. Number: CIP-007-~~1~~2

3. Purpose: Standard CIP-007 requires Responsible Entities to define methods, processes, and procedures for securing those systems determined to be Critical Cyber Assets, as well as the non-critical Cyber Assets within the Electronic Security Perimeter(s). Standard CIP-007 should be read as part of a group of standards numbered Standards CIP-002 through CIP-009. ~~Responsible Entities should interpret and apply Standards CIP-002 through CIP-009 using reasonable business judgment.~~

4. Applicability:

4.1. Within the text of Standard CIP-007, "Responsible Entity" shall mean:

4.1.1 Reliability Coordinator.

4.1.2 Balancing Authority.

4.1.3 Interchange Authority.

4.1.4 Transmission Service Provider.

4.1.5 Transmission Owner.

4.1.6 Transmission Operator.

4.1.7 Generator Owner.

4.1.8 Generator Operator.

4.1.9 Load Serving Entity.

4.1.10 NERC.

4.1.11 Regional Entities

~~4.1.11~~4.1.12 Regional Reliability Organizations.

4.2. The following are exempt from Standard CIP-007:

4.2.1 Facilities regulated by the U.S. Nuclear Regulatory Commission or the Canadian Nuclear Safety Commission.

4.2.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.3 Responsible Entities that, in compliance with Standard CIP-002, identify that they have no Critical Cyber Assets.

5. Effective Date: ~~June 1, 2006~~XXXX

B. Requirements

The Responsible Entity shall comply with the following requirements of Standard CIP-007 for all Critical Cyber Assets and other Cyber Assets within the Electronic Security Perimeter(s):

R1. Test Procedures — The Responsible Entity shall ensure that new Cyber Assets and significant changes to existing Cyber Assets within the Electronic Security Perimeter do not adversely affect existing cyber security controls. For purposes of Standard CIP-007, a significant change shall, at a minimum, include implementation of security patches, cumulative service packs, vendor releases, and version upgrades of operating systems, applications, database platforms, or other third-party software or firmware.

R1.1. The Responsible Entity shall create, implement, and maintain cyber security test procedures in a manner that minimizes adverse effects on the production system or its operation.

R1.2. The Responsible Entity shall document that testing is performed in a manner that reflects the production environment.

R1.3. The Responsible Entity shall document test results.

R2. Ports and Services — The Responsible Entity shall establish ~~and~~ , document and implement a process to ensure that only those ports and services required for normal and emergency operations are enabled.

R2.1. The Responsible Entity shall enable only those ports and services required for normal and emergency operations.

R2.2. The Responsible Entity shall disable other ports and services, including those used for testing purposes, prior to production use of all Cyber Assets inside the Electronic Security Perimeter(s).

R2.3. In the case where unused ports and services cannot be disabled due to technical limitations, the Responsible Entity shall document compensating measure(s) applied to mitigate risk exposure or an acceptance of risk.

R3. Security Patch Management — The Responsible Entity, either separately or as a component of the documented configuration management process specified in CIP-003-1 Requirement R6, shall establish ~~and~~ , document and implement a security patch management program for tracking, evaluating, testing, and installing applicable cyber security software patches for all Cyber Assets within the Electronic Security Perimeter(s).

R3.1. The Responsible Entity shall document the assessment of security patches and security upgrades for applicability within thirty calendar days of availability of the patches or upgrades.

R3.2. The Responsible Entity shall document the implementation of security patches. In any case where the patch is not installed, the Responsible Entity shall document compensating measure(s) applied to mitigate risk exposure or an acceptance of risk.

R4. Malicious Software Prevention — The Responsible Entity shall use anti-virus software and other malicious software ("malware") prevention tools, where technically feasible, to detect, prevent, deter, and mitigate the introduction, exposure, and propagation of malware on all Cyber Assets within the Electronic Security Perimeter(s).

R4.1. The Responsible Entity shall document and implement anti-virus and malware prevention tools. In the case where anti-virus software and malware prevention tools are not installed, the Responsible Entity shall document compensating measure(s) applied to mitigate risk exposure ~~or an acceptance of risk~~.

R4.2. The Responsible Entity shall document and implement a process for the update of anti-virus and malware prevention "signatures." The process must address testing and installing the signatures.

R5. Account Management — The Responsible Entity shall establish, implement, and document technical and procedural controls that enforce access authentication of, and accountability for, all user activity, and that minimize the risk of unauthorized system access.

R5.1. The Responsible Entity shall ensure that individual and shared system accounts and authorized access permissions are consistent with the concept of "need to know" with respect to work functions performed.

R5.1.1. The Responsible Entity shall ensure that user accounts are implemented as approved by designated personnel. Refer to Standard CIP-003-1 Requirement R5.

R5.1.2. The Responsible Entity shall establish methods, processes, and procedures that generate logs of sufficient detail to create historical audit trails of individual user account access activity for a minimum of ninety days.

R5.1.3. The Responsible Entity shall review, at least annually, user accounts to verify access privileges are in accordance with Standard CIP-003-1 Requirement R5 and Standard CIP-004-1 Requirement R4.

R5.2. The Responsible Entity shall implement a policy to minimize and manage the scope and acceptable use of administrator, shared, and other generic account privileges including factory default accounts.

R5.2.1. The policy shall include the removal, disabling, or renaming of such accounts where possible. For such accounts that must remain enabled, passwords shall be changed prior to putting any system into service.

R5.2.2. The Responsible Entity shall identify those individuals with access to shared accounts.

R5.2.3. Where such accounts must be shared, the Responsible Entity shall have a policy for managing the use of such accounts that limits access to only those with authorization, an audit trail of the account use (automated or manual), and steps for securing the account in the event of personnel changes (for example, change in assignment or termination).

R5.3. At a minimum, the Responsible Entity shall require and use passwords, subject to the following, as technically feasible:

R5.3.1. Each password shall be a minimum of six characters.

R5.3.2. Each password shall consist of a combination of alpha, numeric, and "special" characters.

R5.3.3. Each password shall be changed at least annually, or more frequently based on risk.

R6. Security Status Monitoring — The Responsible Entity shall ensure that all Cyber Assets within the Electronic Security Perimeter, as technically feasible, implement automated tools or organizational process controls to monitor system events that are related to cyber security.

R6.1. The Responsible Entity shall implement and document the organizational processes and technical and procedural mechanisms for monitoring for security events on all Cyber Assets within the Electronic Security Perimeter.

R6.2. The security monitoring controls shall issue automated or manual alerts for detected Cyber Security Incidents.

R6.3. The Responsible Entity shall maintain logs of system events related to cyber security, where technically feasible, to support incident response as required in Standard CIP-008.

R6.4. The Responsible Entity shall retain all logs specified in Requirement R6 for ninety calendar days.

R6.5. The Responsible Entity shall review logs of system events related to cyber security and maintain records documenting review of logs.

R7. Disposal or Redeployment — The Responsible Entity shall establish and implement formal methods, processes, and procedures for disposal or redeployment of Cyber Assets within the Electronic Security Perimeter(s) as identified and documented in Standard CIP-005.

R7.1. Prior to the disposal of such assets, the Responsible Entity shall destroy or erase the data storage media to prevent unauthorized retrieval of sensitive cyber security or reliability data.

R7.2. Prior to redeployment of such assets, the Responsible Entity shall, at a minimum, erase the data storage media to prevent unauthorized retrieval of sensitive cyber security or reliability data.

R7.3. The Responsible Entity shall maintain records that such assets were disposed of or redeployed in accordance with documented procedures.

R8. Cyber Vulnerability Assessment — The Responsible Entity shall perform a cyber vulnerability assessment of all Cyber Assets within the Electronic Security Perimeter at least annually. The vulnerability assessment shall include, at a minimum, the following:

R8.1. A document identifying the vulnerability assessment process;

R8.2. A review to verify that only ports and services required for operation of the Cyber Assets within the Electronic Security Perimeter are enabled;

R8.3. A review of controls for default accounts; and,

R8.4. Documentation of the results of the assessment, the action plan to remediate or mitigate vulnerabilities identified in the assessment, and the execution status of that action plan.

R9. Documentation Review and Maintenance — The Responsible Entity shall review and update the documentation specified in Standard CIP-007 at least annually. Changes resulting from modifications to the systems or controls shall be documented within ~~ninety~~thirty calendar days of the change being completed.

Formatted: Font: 11 pt

Formatted: Font: 11 pt

Formatted: Font: 11 pt

C. Measures

The following measures will be used to demonstrate compliance with the requirements of Standard CIP-007:

M1. Documentation of the Responsible Entity's security test procedures as specified in Requirement R1.

M2. Documentation as specified in Requirement R2.

M3. Documentation and records of the Responsible Entity's security patch management program, as specified in Requirement R3.

M4. Documentation and records of the Responsible Entity's malicious software prevention program as specified in Requirement R4.

M5. Documentation and records of the Responsible Entity's account management program as specified in Requirement R5.

M6. Documentation and records of the Responsible Entity's security status monitoring program as specified in Requirement R6.

M7. Documentation and records of the Responsible Entity's program for the disposal or redeployment of Cyber Assets as specified in Requirement R7.

M8. Documentation and records of the Responsible Entity's annual vulnerability assessment of all Cyber Assets within the Electronic Security Perimeters(s) as specified in Requirement R8.

M9. Documentation and records demonstrating the review and update as specified in Requirement R9.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Monitoring Responsibility

1.1.1 Regional Reliability Organizations for Responsible Entities.

1.1.2 NERC for Regional Reliability Organization.

1.1.3 Third-party monitor without vested interest in the outcome for NERC.

1.2. Compliance Monitoring Period and Reset Time Frame

Annually.

1.3. Data Retention

1.3.1 The Responsible Entity shall keep all documentation and records from the previous full calendar year.

1.3.2 The Responsible Entity shall retain security–related system event logs for ninety calendar days, unless longer retention is required pursuant to Standard CIP-008 Requirement R2.

1.3.3 The compliance monitor shall keep audit records for three calendar years.

1.4. Additional Compliance Information.

1.4.1 Responsible Entities shall demonstrate compliance through self-certification or audit, as determined by the Compliance Monitor.

1.4.2 Instances where the Responsible Entity cannot conform to its cyber security policy must be documented as exceptions and approved by the designated senior manager or delegate(s). Duly authorized exceptions will not result in non-compliance. Refer to Standard CIP-003 Requirement R3.

2. Levels of Noncompliance

2.1. Level 1:

2.1.1 System security controls are in place, but fail to document one of the measures (M1-M9) of Standard CIP-007; or

2.1.2 One of the documents required in Standard CIP-007 has not been reviewed in the previous full calendar year as specified by Requirement R9; or,

2.1.3 One of the documented system security controls has not been updated within ninety calendar days of a change as specified by Requirement R9; or,

2.1.4 Any one of:

- Authorization rights and access privileges have not been reviewed during the previous full calendar year; or,
- A gap exists in any one log of system events related to cyber security of greater than seven calendar days; or,
- Security patches and upgrades have not been assessed for applicability within thirty calendar days of availability.

2.2. Level 2:

2.2.1 System security controls are in place, but fail to document up to two of the measures (M1-M9) of Standard CIP-007; or,

2.2.2 Two occurrences in any combination of those violations enumerated in Noncompliance Level 1, 2.1.4 within the same compliance period.

2.3. Level 3:

2.3.1 System security controls are in place, but fail to document up to three of the measures (M1-M9) of Standard CIP-007; or,

2.3.2 Three occurrences in any combination of those violations enumerated in Noncompliance Level 1, 2.1.4 within the same compliance period.

2.4. Level 4:

2.4.1 System security controls are in place, but fail to document four or more of the measures (M1-M9) of Standard CIP-007; or,

2.4.2 Four occurrences in any combination of those violations enumerated in Noncompliance Level 1, 2.1.4 within the same compliance period.

2.4.3 No logs exist.

E. Regional Differences

None identified.

Version History

Version	Date	Action	Change Tracking

A. Introduction

1. Title: Cyber Security — Incident Reporting and Response Planning

2. Number: CIP-008-~~1~~2

3. Purpose: Standard CIP-008 ensures the identification, classification, response, and reporting of Cyber Security Incidents related to Critical Cyber Assets. Standard CIP-008 should be read as part of a group of standards numbered Standards CIP-002 through CIP-009. ~~Responsible Entities should apply Standards CIP-002 through CIP-009 using reasonable business judgment.~~

4. Applicability

4.1. Within the text of Standard CIP-008, "Responsible Entity" shall mean:

4.1.1 Reliability Coordinator.

4.1.2 Balancing Authority.

4.1.3 Interchange Authority.

4.1.4 Transmission Service Provider.

4.1.5 Transmission Owner.

4.1.6 Transmission Operator.

4.1.7 Generator Owner.

4.1.8 Generator Operator.

4.1.9 Load Serving Entity.

4.1.10 NERC.

4.1.11 Regional Entities

~~4.1.11~~**4.1.12** Regional Reliability Organizations.

4.2. The following are exempt from Standard CIP-008:

4.2.1 Facilities regulated by the U.S. Nuclear Regulatory Commission or the Canadian Nuclear Safety Commission.

4.2.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.3 Responsible Entities that, in compliance with Standard CIP-002, identify that they have no Critical Cyber Assets.

5. Effective Date: ~~June 1, 2006~~XXXX

B. Requirements

The Responsible Entity shall comply with the following requirements of Standard CIP-008:

R1. Cyber Security Incident Response Plan — The Responsible Entity shall develop and maintain a Cyber Security Incident response plan and implement the plan in response to Cyber Security Incidents. The Cyber Security Incident Response plan shall address, at a minimum, the following:

R1.1. Procedures to characterize and classify events as reportable Cyber Security Incidents.

R1.2. Response actions, including roles and responsibilities of incident response teams, incident handling procedures, and communication plans.

R1.3. Process for reporting Cyber Security Incidents to the Electricity Sector Information Sharing and Analysis Center (ES–<u>–</u>ISAC). The Responsible Entity must ensure that all reportable Cyber Security Incidents are reported to the ES–<u>–</u>ISAC either directly or through an intermediary.

R1.4. Process for updating the Cyber Security Incident response plan within ~~ninety~~<u>thirty</u> calendar days of any changes.

R1.5. Process for ensuring that the Cyber Security Incident response plan is reviewed at least annually.

R1.6. Process for ensuring the Cyber Security Incident response plan is tested at least annually. A test of the incident response plan can range from a paper drill, to a full operational exercise, to the response to an actual incident.<u> Testing the Cyber Security Incident response plan does not require removing a component or system from service during the test.</u>

R2. Cyber Security Incident Documentation — The Responsible Entity shall keep relevant documentation related to Cyber Security Incidents reportable per Requirement R1.1 for three calendar years.

C. Measures

The following measures will be used to demonstrate compliance with the requirements of CIP-008:

M1. The Cyber Security Incident response plan as indicated in R1 and documentation of the review, updating, and testing of the plan

M2. All documentation as specified in Requirement R2.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Monitoring Responsibility

1.1.1 Regional Reliability Organizations for Responsible Entities.

1.1.2 NERC for Regional Reliability Organization.

1.1.3 Third-party monitor without vested interest in the outcome for NERC.

1.2. Compliance Monitoring Period and Reset Time Frame

Annually.

1.3. Data Retention

1.3.1 The Responsible Entity shall keep documentation other than that required for reportable Cyber Security Incidents as specified in Standard CIP-008 for the previous full calendar year.

1.3.2 The compliance monitor shall keep audit records for three calendar years.

1.4. Additional Compliance Information

1.4.1 Responsible Entities shall demonstrate compliance through self-certification or audit, as determined by the Compliance Monitor.

1.4.2 Instances where the Responsible Entity cannot conform to its cyber security policy must be documented as exceptions and approved by the designated senior manager or delegate(s). Duly authorized exceptions will not result in non-compliance. Refer to Standard CIP-003 Requirement R3.

1.4.3 The Responsible Entity may not take exception in its cyber security policies to the creation of a Cyber Security Incident response plan.

1.4.4 The Responsible Entity may not take exception in its cyber security policies to reporting Cyber Security Incidents to the ES ISAC.

2. Levels of Noncompliance

2.1. Level 1: A Cyber Security Incident response plan exists, but has not been updated within ninety calendar days of changes.

2.2. Level 2:

2.2.1 A Cyber Security Incident response plan exists, but has not been reviewed in the previous full calendar year; or,

2.2.2 A Cyber Security Incident response plan has not been tested in the previous full calendar year; or,

2.2.3 Records related to reportable Cyber Security Incidents were not retained for three calendar years.

2.3. Level 3:

2.3.1 A Cyber Security Incident response plan exists, but does not include required elements Requirements R1.1, R1.2, and R1.3 of Standard CIP-008; or,

2.3.2 A reportable Cyber Security Incident has occurred but was not reported to the ES ISAC.

2.4. Level 4: A Cyber Security Incident response plan does not exist.

E. Regional Differences

None identified.

Version History

Version	Date	Action	Change Tracking

Style Definition: Requirement: Indent: Left: 0.25", Hanging: 0.38", Tab stops: 0.63", List tab + Not at 0.65"

A. Introduction

1. Title: Cyber Security — Recovery Plans for Critical Cyber Assets

2. Number: CIP-009-~~1~~2

3. Purpose: Standard CIP-009 ensures that recovery plan(s) are put in place for Critical Cyber Assets and that these plans follow established business continuity and disaster recovery techniques and practices. Standard CIP-009 should be read as part of a group of standards numbered Standards CIP-002 through CIP-009. ~~Responsible Entities should apply Standards CIP-002 through CIP-009 using reasonable business judgment.~~

4. Applicability:

4.1. Within the text of Standard CIP-009, "Responsible Entity" shall mean:

4.1.1 Reliability Coordinator

4.1.2 Balancing Authority

4.1.3 Interchange Authority

4.1.4 Transmission Service Provider

4.1.5 Transmission Owner

4.1.6 Transmission Operator

4.1.7 Generator Owner

4.1.8 Generator Operator

4.1.9 Load Serving Entity

4.1.10 NERC

4.1.11 Regional Entities

~~4.1.11~~4.1.12 Regional Reliability Organizations

4.2. The following are exempt from Standard CIP-009:

4.2.1 Facilities regulated by the U.S. Nuclear Regulatory Commission or the Canadian Nuclear Safety Commission.

4.2.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.3 Responsible Entities that, in compliance with Standard CIP-002, identify that they have no Critical Cyber Assets.

5. Effective Date: ~~June 1, 2006~~XXXX

B. Requirements

The Responsible Entity shall comply with the following requirements of Standard CIP-009:

R1. Recovery Plans — The Responsible Entity shall create and annually review recovery plan(s) for Critical Cyber Assets. The recovery plan(s) shall address at a minimum the following:

R1.1. Specify the required actions in response to events or conditions of varying duration and severity that would activate the recovery plan(s).

R1.2. Define the roles and responsibilities of responders.

R2. Exercises — The recovery plan(s) shall be exercised at least annually. An exercise of the recovery plan(s) can range from a paper drill, to a full operational exercise, to recovery from an actual incident.

R3. Change Control — Recovery plan(s) shall be updated to reflect any changes or lessons learned as a result of an exercise or the recovery from an actual incident. Updates shall be communicated to personnel responsible for the activation and implementation of the recovery plan(s) within ~~ninety~~thirty calendar days of the change being completed.

R4. Backup and Restore — The recovery plan(s) shall include processes and procedures for the backup and storage of information required to successfully restore Critical Cyber Assets. For example, backups may include spare electronic components or equipment, written documentation of configuration settings, tape backup, etc.

R5. Testing Backup Media — Information essential to recovery that is stored on backup media shall be tested at least annually to ensure that the information is available. Testing can be completed off site.

C. Measures

The following measures will be used to demonstrate compliance with the requirements of Standard CIP-009:

M1. Recovery plan(s) as specified in Requirement R1.

M2. Records documenting required exercises as specified in Requirement R2.

M3. Documentation of changes to the recovery plan(s), and documentation of all communications, as specified in Requirement R3.

M4. Documentation regarding backup and storage of information as specified in Requirement R4.

M5. Documentation of testing of backup media as specified in Requirement R5.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Monitoring Responsibility

1.1.1 Regional Reliability Organizations for Responsible Entities.

1.1.2 NERC for Regional Reliability Organization.

1.1.3 Third-party monitor without vested interest in the outcome for NERC.

1.2. Compliance Monitoring Period and Reset Time Frame

Annually.

1.3. Data Retention

1.3.1 The Responsible Entity shall keep documentation required by Standard CIP-009 from the previous full calendar year.

1.3.2 The Compliance Monitor shall keep audit records for three calendar years.

1.4. Additional Compliance Information

1.4.1 Responsible Entities shall demonstrate compliance through self-certification or audit (periodic, as part of targeted monitoring or initiated by complaint or event), as determined by the Compliance Monitor.

1.4.2 Instances where the Responsible Entity cannot conform to its cyber security policy must be documented as exceptions and approved by the designated senior manager or delegate(s). Duly authorized exceptions will not result in non-compliance. Refer to Standard CIP-003 Requirement R3.

2. Levels of Noncompliance

2.1. Level 1:

2.1.1 Recovery plan(s) exist and are exercised, but do not contain all elements as specified in Requirement R1; or,

2.1.2 Recovery plan(s) are not updated and personnel are not notified within ninety calendar days of the change.

2.2. Level 2:

2.2.1 Recovery plan(s) exist, but have not been reviewed during the previous full calendar year; or,

2.2.2 Documented processes and procedures for the backup and storage of information required to successfully restore Critical Cyber Assets do not exist.

2.3. Level 3:

2.3.1 Testing of information stored on backup media to ensure that the information is available has not been performed at least annually; or,

2.3.2 Recovery plan(s) exist, but have not been exercised during the previous full calendar year.

2.4. Level 4:

2.4.1 No recovery plan(s) exist; or,

2.4.2 Backup of information required to successfully restore Critical Cyber Assets does not exist.

E. Regional Differences

None identified.

Version History

Version	Date	Action	Change Tracking

Access Control System – a system which provides for Authentication, Authorization and frequently Accounting of access through either a Physical Security Perimeter or an Electronic Security Perimeter. An Access Control System may be a single computer system which performs all three functions, or may be a combination of two or more computer sub-systems which work together to accomplish all three functions.

1. Authentication is the process of verifying a user's or object's identity.

2. Authorization is the process for granting an authenticated user or object, the authority and access to perform a certain operation.

3. Accounting provides an audit trail of access, and includes logging of access by identification and time.

A. Introduction

1. Title: Cyber Security — Critical Cyber Asset Identification

2. Number: CIP-002-~~1~~2

3. Purpose: NERC Standards CIP-002 through CIP-009 provide a cyber security framework for the identification and protection of Critical Cyber Assets to support reliable operation of the Bulk Electric System.

These standards recognize the differing roles of each entity in the operation of the Bulk Electric System, the criticality and vulnerability of the assets needed to manage Bulk Electric System reliability, and the risks to which they are exposed. ~~Responsible Entities should interpret and apply Standards CIP-002 through CIP-009 using reasonable business judgment.~~

Business and operational demands for managing and maintaining a reliable Bulk Electric System increasingly rely on Cyber Assets supporting critical reliability functions and processes to communicate with each other, across functions and organizations, for services and data. This results in increased risks to these Cyber Assets.

Standard CIP-002 requires the identification and documentation of the Critical Cyber Assets associated with the Critical Assets that support the reliable operation of the Bulk Electric System. These Critical Assets are to be identified through the application of a risk-based assessment.

4. Applicability:

4.1. Within the text of Standard CIP-002, "Responsible Entity" shall mean:

4.1.1 Reliability Coordinator.

4.1.2 Balancing Authority.

4.1.3 Interchange Authority.

4.1.4 Transmission Service Provider.

4.1.5 Transmission Owner.

4.1.6 Transmission Operator.

4.1.7 Generator Owner.

4.1.8 Generator Operator.

4.1.9 Load Serving Entity.

4.1.10 NERC.

4.1.11 Regional Reliability Organizations~~.~~

4.1.12 Regional Entities.

4.2. The following are exempt from Standard CIP-002:

4.2.1 Facilities regulated by the U.S. Nuclear Regulatory Commission or the Canadian Nuclear Safety Commission.

4.2.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

5. Effective Date: ~~June 1, 2006~~XXXX

B. Requirements

The Responsible Entity shall comply with the following requirements of Standard CIP-002:

R1. Critical Asset Identification Method — The Responsible Entity shall identify and document a risk-based assessment methodology to use to identify its Critical Assets.

R1.1. The Responsible Entity shall maintain documentation describing its risk-based assessment methodology that includes procedures and evaluation criteria.

R1.2. The risk-based assessment shall consider the following assets:

R1.2.1. Control centers and backup control centers performing the functions of the entities listed in the Applicability section of this standard.

R1.2.2. Transmission substations that support the reliable operation of the Bulk Electric System.

R1.2.3. Generation resources that support the reliable operation of the Bulk Electric System.

R1.2.4. Systems and facilities critical to system restoration, including blackstart generators and substations in the electrical path of transmission lines used for initial system restoration.

R1.2.5. Systems and facilities critical to automatic load shedding under a common control system capable of shedding 300 MW or more.

R1.2.6. Special Protection Systems that support the reliable operation of the Bulk Electric System.

R1.2.7. Any additional assets that support the reliable operation of the Bulk Electric System that the Responsible Entity deems appropriate to include in its assessment.

R2. Critical Asset Identification — The Responsible Entity shall develop a list of its identified Critical Assets determined through an annual application of the risk-based assessment methodology required in R1. The Responsible Entity shall review this list at least annually, and update it as necessary.

R3. Critical Cyber Asset Identification — Using the list of Critical Assets developed pursuant to Requirement R2, the Responsible Entity shall develop a list of associated Critical Cyber Assets essential to the operation of the Critical Asset. Examples at control centers and backup control centers include systems and facilities at master and remote sites that provide monitoring and control, automatic generation control, real-time power system modeling, and real-time inter-utility data exchange. The Responsible Entity shall review this list at least annually, and update it as necessary. For the purpose of Standard CIP-002, Critical Cyber Assets are further qualified to be those having at least one of the following characteristics:

R3.1. The Cyber Asset uses a routable protocol to communicate outside the Electronic Security Perimeter; or,

R3.2. The Cyber Asset uses a routable protocol within a control center; or,

R3.3. The Cyber Asset is dial-up accessible.

R4. Annual Approval — ~~A~~ The senior manager or delegate(s) shall approve annually the risk-based assessment methodology, the list of Critical Assets and the list of Critical Cyber Assets. Based on Requirements R1, R2, and R3 the Responsible Entity may determine that it has no Critical Assets or Critical Cyber Assets. The Responsible Entity shall keep a signed and dated record of the senior manager or delegate(s)'s approval of the risk-based assessment methodology, the list of Critical Assets and the list of Critical Cyber Assets (even if such lists are null.)

C. Measures

The following measures will be used to demonstrate compliance with the requirements of Standard CIP-002:

M1. The risk-based assessment methodology documentation as specified in Requirement R1.

M2. The list of Critical Assets as specified in Requirement R2.

M3. The list of Critical Cyber Assets as specified in Requirement R3.

M4. The records of annual approvals as specified in Requirement R4.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Monitoring Responsibility

1.1.1 Regional Reliability Organizations for Responsible Entities.

1.1.2 NERC for Regional Reliability Organization.

1.1.3 Third-party monitor without vested interest in the outcome for NERC.

1.2. Compliance Monitoring Period and Reset Time Frame

Annually.

1.3. Data Retention

1.3.1 The Responsible Entity shall keep documentation required by Standard CIP-002 from the previous full calendar year

1.3.2 The compliance monitor shall keep audit records for three calendar years.

1.4. Additional Compliance Information

1.4.1 Responsible Entities shall demonstrate compliance through self-certification or audit, as determined by the Compliance Monitor.

2. Levels of Non-Compliance

2.1 Level 1: The risk assessment has not been performed annually.

2.2 Level 2: The list of Critical Assets or Critical Cyber Assets exist, but has not been approved or reviewed in the last calendar year.

2.3 Level 3: The list of Critical Assets or Critical Cyber Assets does not exist.

2.4 Level 4: The lists of Critical Assets and Critical Cyber Assets do not exist.

E. Regional Differences

None identified.

Version History

Version	Date	Action	Change Tracking
1	01/16/06	R3.2 — Change “Control Center” to “control center”	03/24/06

A. Introduction

1. Title: Cyber Security — Security Management Controls

2. Number: CIP-003-~~1~~2

3. Purpose: Standard CIP-003 requires that Responsible Entities have minimum security management controls in place to protect Critical Cyber Assets. Standard CIP-003 should be read as part of a group of standards numbered Standards CIP-002 through CIP-009. ~~Responsible Entities should interpret and apply Standards CIP-002 through CIP-009 using reasonable business judgment~~.

4. Applicability:

4.1. Within the text of Standard CIP-003, "Responsible Entity" shall mean:

4.1.1 Reliability Coordinator.

4.1.2 Balancing Authority.

4.1.3 Interchange Authority.

4.1.4 Transmission Service Provider.

4.1.5 Transmission Owner.

4.1.6 Transmission Operator.

4.1.7 Generator Owner.

4.1.8 Generator Operator.

4.1.9 Load Serving Entity.

4.1.10 NERC.

4.1.11 Regional Reliability Organizations~~.~~

4.1.12 Regional Entities.

4.2. The following are exempt from Standard CIP-003:

4.2.1 Facilities regulated by the U.S. Nuclear Regulatory Commission or the Canadian Nuclear Safety Commission.

4.2.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.3 Responsible Entities that, in compliance with Standard CIP-002, identify that they have no Critical Cyber Assets shall only be required to comply with CIP-003-2 Requirement R2.

5. Effective Date: ~~June 1, 2006~~XXXX

B. Requirements

The Responsible Entity shall comply with the following requirements of Standard CIP-003:

R1. Cyber Security Policy — The Responsible Entity shall document and implement a cyber security policy that represents management's commitment and ability to secure its Critical Cyber Assets. The Responsible Entity shall, at minimum, ensure the following:

R1.1. The cyber security policy addresses the requirements in Standards CIP-002 through CIP-009, including provision for emergency situations.

R1.2. The cyber security policy is readily available to all personnel who have access to, or are responsible for, Critical Cyber Assets.

R1.3. Annual review and approval of the cyber security policy by the senior manager assigned pursuant to R2.

R2. Leadership — The Responsible Entity shall assign a single senior manager with overall responsibility and authority for leading and managing the entity's implementation of, and adherence to, Standards CIP-002 through CIP-009.

R2.1. The senior manager shall be identified by name, title, ~~business phone, business address,~~ and date of designation.

R2.2. Changes to the senior manager must be documented within thirty calendar days of the effective date.

R2.3. Where allowed by Standards CIP-002 through CIP-009, the senior manager may delegate authority for specific actions to a named delegate or delegates. These delegations must be documented in the same manner as R2.1 and R2.2, and approved by the senior manager.

~~R2.3.~~R2.4. The senior manager or delegate(s), shall authorize and document any exception from the requirements of the cyber security policy.

R3. Exceptions — Instances where the Responsible Entity cannot conform to its cyber security policy must be documented as exceptions and authorized by the senior manager or delegate(s).

R3.1. Exceptions to the Responsible Entity's cyber security policy must be documented within thirty days of being approved by the senior manager or delegate(s).

R3.2. Documented exceptions to the cyber security policy must include an explanation as to why the exception is necessary and any compensating measures~~, or a statement accepting risk~~.

R3.3. Authorized exceptions to the cyber security policy must be reviewed and approved annually by the senior manager or delegate(s) to ensure the exceptions are still required and valid. Such review and approval shall be documented.

R4. Information Protection — The Responsible Entity shall implement and document a program to identify, classify, and protect information associated with Critical Cyber Assets.

R4.1. The Critical Cyber Asset information to be protected shall include, at a minimum and regardless of media type, operational procedures, lists as required in Standard CIP-002, network topology or similar diagrams, floor plans of computing centers that contain Critical Cyber Assets, equipment layouts of Critical Cyber Assets, disaster recovery plans, incident response plans, and security configuration information.

R4.2. The Responsible Entity shall classify information to be protected under this program based on the sensitivity of the Critical Cyber Asset information.

R4.3. The Responsible Entity shall, at least annually, assess adherence to its Critical Cyber Asset information protection program, document the assessment results, and implement an action plan to remediate deficiencies identified during the assessment.

R5. Access Control — The Responsible Entity shall document and implement a program for managing access to protected Critical Cyber Asset information.

R5.1. The Responsible Entity shall maintain a list of designated personnel who are responsible for authorizing logical or physical access to protected information.

Formatted: Highlight

R5.1.1. Personnel shall be identified by name, title, business phone and the information for which they are responsible for authorizing access.

R5.1.2. The list of personnel responsible for authorizing access to protected information shall be verified at least annually.

R5.2. The Responsible Entity shall review at least annually the access privileges to protected information to confirm that access privileges are correct and that they correspond with the Responsible Entity's needs and appropriate personnel roles and responsibilities.

R5.3. The Responsible Entity shall assess and document at least annually the processes for controlling access privileges to protected information.

R6. Change Control and Configuration Management — The Responsible Entity shall establish and document a process of change control and configuration management for adding, modifying, replacing, or removing Critical Cyber Asset hardware or software, and implement supporting configuration management activities to identify, control and document all entity or vendor-related changes to hardware and software components of Critical Cyber Assets pursuant to the change control process.

C. Measures

The following measures will be used to demonstrate compliance with the requirements of Standard CIP-003:

M1. Documentation of the Responsible Entity's cyber security policy as specified in Requirement R1. Additionally, the Responsible Entity shall demonstrate that the cyber security policy is available as specified in Requirement R1.2.

M2. Documentation of the assignment of, and changes to, the Responsible Entity's leadership as specified in Requirement R2.

M3. Documentation of the Responsible Entity's exceptions, as specified in Requirement R3.

M4. Documentation of the Responsible Entity's information protection program as specified in Requirement R4.

M5. The access control documentation as specified in Requirement R5.

M6. The Responsible Entity's change control and configuration management documentation as specified in Requirement R6.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Monitoring Responsibility

1.1.1 Regional Reliability Organizations for Responsible Entities.

1.1.2 NERC for Regional Reliability Organization.

1.1.3 Third-party monitor without vested interest in the outcome for NERC.

1.2. Compliance Monitoring Period and Reset Time Frame

Annually.

1.3. Data Retention

1.3.1 The Responsible Entity shall keep all documentation and records from the previous full calendar year.

1.3.2 The compliance monitor shall keep audit records for three years.

1.4. Additional Compliance Information

1.4.1 Responsible Entities shall demonstrate compliance through self-certification or audit, as determined by the Compliance Monitor.

1.4.2 Instances where the Responsible Entity cannot conform to its cyber security policy must be documented as exceptions and approved by the designated senior manager or delegate(s). Refer to CIP-003, Requirement R3. Duly authorized exceptions will not result in non-compliance.

2. Levels of Noncompliance

2.1. Level 1:

2.1.1 Changes to the designation of senior manager were not documented in accordance with Requirement R2.2; or,

2.1.2 Exceptions from the cyber security policy have not been documented within thirty calendar days of the approval of the exception; or,

2.1.3 An information protection program to identify and classify information and the processes to protect information associated with Critical Cyber Assets has not been assessed in the previous full calendar year.

2.2. Level 2:

2.2.1 A cyber security policy exists, but has not been reviewed within the previous full calendar year; or,

2.2.2 Exceptions to policy are not documented or authorized by the senior manager or delegate(s); or,

2.2.3 Access privileges to the information related to Critical Cyber Assets have not been reviewed within the previous full calendar year; or,

2.2.4 The list of designated personnel responsible to authorize access to the information related to Critical Cyber Assets has not been reviewed within the previous full calendar year.

2.3. Level 3:

2.3.1 A senior manager has not been identified in accordance with Requirement R2.1; or,

2.3.2 The list of designated personnel responsible to authorize logical or physical access to protected information associated with Critical Cyber Assets does not exist; or,

2.3.3 No changes to hardware and software components of Critical Cyber Assets have been documented in accordance with Requirement R6.

2.4. Level 4:

2.4.1 No cyber security policy exists; or,

2.4.2 No identification and classification program for protecting information associated with Critical Cyber Assets exists; or,

2.4.3 No documented change control and configuration management process exists.

E. **Regional Differences**

None identified.

Version History

Version	Date	Action	Change Tracking

A. Introduction

1. Title: Cyber Security — Security Management Controls

2. Number: CIP-003-~~1~~2

3. Purpose: Standard CIP-003 requires that Responsible Entities have minimum security management controls in place to protect Critical Cyber Assets. Standard CIP-003 should be read as part of a group of standards numbered Standards CIP-002 through CIP-009. ~~Responsible Entities should interpret and apply Standards CIP-002 through CIP-009 using reasonable business judgment~~.

4. Applicability:

4.1. Within the text of Standard CIP-003, "Responsible Entity" shall mean:

4.1.1 Reliability Coordinator.

4.1.2 Balancing Authority.

4.1.3 Interchange Authority.

4.1.4 Transmission Service Provider.

4.1.5 Transmission Owner.

4.1.6 Transmission Operator.

4.1.7 Generator Owner.

4.1.8 Generator Operator.

4.1.9 Load Serving Entity.

4.1.10 NERC.

4.1.11 Regional Reliability Organizations~~.~~

4.1.12 Regional Entities.

4.2. The following are exempt from Standard CIP-003:

4.2.1 Facilities regulated by the U.S. Nuclear Regulatory Commission or the Canadian Nuclear Safety Commission.

4.2.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.3 Responsible Entities that, in compliance with Standard CIP-002, identify that they have no Critical Cyber Assets shall only be required to comply with CIP-003-2 Requirement R2.

5. Effective Date: ~~June 1, 2006~~XXXX

B. Requirements

The Responsible Entity shall comply with the following requirements of Standard CIP-003:

R1. Cyber Security Policy — The Responsible Entity shall document and implement a cyber security policy that represents management's commitment and ability to secure its Critical Cyber Assets. The Responsible Entity shall, at minimum, ensure the following:

R1.1. The cyber security policy addresses the requirements in Standards CIP-002 through CIP-009, including provision for emergency situations.

R1.2. The cyber security policy is readily available to all personnel who have access to, or are responsible for, Critical Cyber Assets.

R1.3. Annual review and approval of the cyber security policy by the senior manager assigned pursuant to R2.

R2. Leadership — The Responsible Entity shall assign a single senior manager with overall responsibility and authority for leading and managing the~~-~~ entity's implementation of, and adherence to, Standards CIP-002 through CIP-009.

R2.1. The senior manager shall be identified by name, title, ~~business phone, business address,~~ and date of designation.

R2.2. Changes to the senior manager must be documented within thirty calendar days of the effective date.

R2.3. Where allowed by Standards CIP-002 through CIP-009, the senior manager may delegate authority for specific actions to a named delegate or delegates. These delegations must be documented in the same manner as R2.1 and R2.2, and approved by the senior manager.

~~R2.3.~~R2.4. The senior manager or delegate(s), shall authorize and document any exception from the requirements of the cyber security policy.

R3. Exceptions — Instances where the Responsible Entity cannot conform to its cyber security policy must be documented as exceptions and authorized by the senior manager or delegate(s).

R3.1. Exceptions to the Responsible Entity's cyber security policy must be documented within thirty days of being approved by the senior manager or delegate(s).

R3.2. Documented exceptions to the cyber security policy must include an explanation as to why the exception is necessary and any compensating measures~~, or a statement accepting risk~~.

R3.3. Authorized exceptions to the cyber security policy must be reviewed and approved annually by the senior manager or delegate(s) to ensure the exceptions are still required and valid. Such review and approval shall be documented.

R4. Information Protection — The Responsible Entity shall implement and document a program to identify, classify, and protect information associated with Critical Cyber Assets.

R4.1. The Critical Cyber Asset information to be protected shall include, at a minimum and regardless of media type, operational procedures, lists as required in Standard CIP-002, network topology or similar diagrams, floor plans of computing centers that contain Critical Cyber Assets, equipment layouts of Critical Cyber Assets, disaster recovery plans, incident response plans, and security configuration information.

R4.2. The Responsible Entity shall classify information to be protected under this program based on the sensitivity of the Critical Cyber Asset information.

R4.3. The Responsible Entity shall, at least annually, assess adherence to its Critical Cyber Asset information protection program, document the assessment results, and implement an action plan to remediate deficiencies identified during the assessment.

R5. Access Control — The Responsible Entity shall document and implement a program for managing access to protected Critical Cyber Asset information.

R5.1. The Responsible Entity shall maintain a list of designated personnel who are responsible for authorizing logical or physical access to protected information.

R5.1.1. Personnel shall be identified by name, title, business phone and the information for which they are responsible for authorizing access.

R5.1.2. The list of personnel responsible for authorizing access to protected information shall be verified at least annually.

R5.2. The Responsible Entity shall review at least annually the access privileges to protected information to confirm that access privileges are correct and that they correspond with the Responsible Entity's needs and appropriate personnel roles and responsibilities.

R5.3. The Responsible Entity shall assess and document at least annually the processes for controlling access privileges to protected information.

R6. Change Control and Configuration Management — The Responsible Entity shall establish and document a process of change control and configuration management for adding, modifying, replacing, or removing Critical Cyber Asset hardware or software, and implement supporting configuration management activities to identify, control and document all entity or vendor-related changes to hardware and software components of Critical Cyber Assets pursuant to the change control process.

C. Measures

The following measures will be used to demonstrate compliance with the requirements of Standard CIP-003:

M1. Documentation of the Responsible Entity's cyber security policy as specified in Requirement R1. Additionally, the Responsible Entity shall demonstrate that the cyber security policy is available as specified in Requirement R1.2.

M2. Documentation of the assignment of, and changes to, the Responsible Entity's leadership as specified in Requirement R2.

M3. Documentation of the Responsible Entity's exceptions, as specified in Requirement R3.

M4. Documentation of the Responsible Entity's information protection program as specified in Requirement R4.

M5. The access control documentation as specified in Requirement R5.

M6. The Responsible Entity's change control and configuration management documentation as specified in Requirement R6.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Monitoring Responsibility

1.1.1 Regional Reliability Organizations for Responsible Entities.

1.1.2 NERC for Regional Reliability Organization.

1.1.3 Third-party monitor without vested interest in the outcome for NERC.

1.2. Compliance Monitoring Period and Reset Time Frame

Annually.

1.3. Data Retention

1.3.1 The Responsible Entity shall keep all documentation and records from the previous full calendar year.

1.3.2 The compliance monitor shall keep audit records for three years.

1.4. Additional Compliance Information

1.4.1 Responsible Entities shall demonstrate compliance through self-certification or audit, as determined by the Compliance Monitor.

1.4.2 Instances where the Responsible Entity cannot conform to its cyber security policy must be documented as exceptions and approved by the designated senior manager or delegate(s). Refer to CIP-003, Requirement R3. Duly authorized exceptions will not result in non-compliance.

2. Levels of Noncompliance

2.1. Level 1:

2.1.1 Changes to the designation of senior manager were not documented in accordance with Requirement R2.2; or,

2.1.2 Exceptions from the cyber security policy have not been documented within thirty calendar days of the approval of the exception; or,

2.1.3 An information protection program to identify and classify information and the processes to protect information associated with Critical Cyber Assets has not been assessed in the previous full calendar year.

2.2. Level 2:

2.2.1 A cyber security policy exists, but has not been reviewed within the previous full calendar year; or,

2.2.2 Exceptions to policy are not documented or authorized by the senior manager or delegate(s); or,

2.2.3 Access privileges to the information related to Critical Cyber Assets have not been reviewed within the previous full calendar year; or,

2.2.4 The list of designated personnel responsible to authorize access to the information related to Critical Cyber Assets has not been reviewed within the previous full calendar year.

2.3. Level 3:

2.3.1 A senior manager has not been identified in accordance with Requirement R2.1; or,

2.3.2 The list of designated personnel responsible to authorize logical or physical access to protected information associated with Critical Cyber Assets does not exist; or,

2.3.3 No changes to hardware and software components of Critical Cyber Assets have been documented in accordance with Requirement R6.

2.4. Level 4:

2.4.1 No cyber security policy exists; or,

2.4.2 No identification and classification program for protecting information associated with Critical Cyber Assets exists; or,

2.4.3 No documented change control and configuration management process exists.

E. Regional Differences

None identified.

Version History

Version	Date	Action	Change Tracking

A. Introduction

1. Title: Cyber Security — Personnel & Training

2. Number: CIP-004-~~1~~2

3. Purpose: Standard CIP-004 requires that personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets, including contractors and service vendors, have an appropriate level of personnel risk assessment, training, and security awareness. Standard CIP-004 should be read as part of a group of standards numbered Standards CIP-002 through CIP-009. ~~Responsible Entities should interpret and apply Standards CIP-002 through CIP-009 using reasonable business judgment.~~

4. Applicability:

4.1. Within the text of Standard CIP-004, "Responsible Entity" shall mean:

4.1.1 Reliability Coordinator.

4.1.2 Balancing Authority.

4.1.3 Interchange Authority.

4.1.4 Transmission Service Provider.

4.1.5 Transmission Owner.

4.1.6 Transmission Operator.

4.1.7 Generator Owner.

4.1.8 Generator Operator.

4.1.9 Load Serving Entity.

4.1.10 NERC.

4.1.11 Regional Reliability Organizations~~.~~

4.1.12 Regional Entities.

4.2. The following are exempt from Standard CIP-004:

4.2.1 Facilities regulated by the U.S. Nuclear Regulatory Commission or the Canadian Nuclear Safety Commission.

4.2.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.3 Responsible Entities that, in compliance with Standard CIP-002, identify that they have no Critical Cyber Assets.

5. Effective Date: ~~June 1, 2006~~XXXX

B. Requirements

The Responsible Entity shall comply with the following requirements of Standard CIP-004:

R1. Awareness — The Responsible Entity shall establish, maintain, ~~and~~ document and implement a security awareness program to ensure personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets receive on-going reinforcement in sound security practices. The program shall include security awareness reinforcement on at least a quarterly basis using mechanisms such as:

- Direct communications (e.g., emails, memos, computer based training, etc.);
- Indirect communications (e.g., posters, intranet, brochures, etc.);

Formatted: Indent: Left: 0.25", Hanging: 0.38", Tab stops: 0.63", Left + Not at 1.8"

Formatted: French (France)

- Management support and reinforcement (e.g., presentations, meetings, etc.).

R2. Training — The Responsible Entity shall establish, maintain, ~~and~~ document and implement an annual cyber security training program for personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets. The cyber security training program shall be annually ~~, and~~ reviewed ~~the program annually~~ and updated as necessary.

Formatted: Indent: Left: 0.25", Hanging: 0.38", Tab stops: 0.63", Left

R2.1. This program will ensure that all personnel having such access to Critical Cyber Assets, including contractors and service vendors, are trained ~~within ninety calendar days of such authorization~~prior to their being granted such access. Provisions for emergency situations shall be handled in accordance with CIP-003-2 R1.1.

R2.2. Training shall cover the policies, access controls, and procedures as developed for the Critical Cyber Assets covered by CIP-004, and include, at a minimum, the following required items appropriate to personnel roles and responsibilities:

R2.2.1. The proper use of Critical Cyber Assets;

R2.2.2. Physical and electronic access controls to Critical Cyber Assets;

R2.2.3. The proper handling of Critical Cyber Asset information; and,

R2.2.4. Action plans and procedures to recover or re-establish Critical Cyber Assets and access thereto following a Cyber Security Incident.

R2.3. The Responsible Entity shall maintain documentation that training is conducted at least annually, including the date the training was completed and attendance records.

R3. Personnel Risk Assessment —The Responsible Entity shall have a documented personnel risk assessment program, in accordance with federal, state, provincial, and local laws, and subject to existing collective bargaining unit agreements, for personnel having authorized cyber or authorized unescorted physical access. A personnel risk assessment shall be conducted pursuant to that program ~~within thirty days of~~prior to such personnel being granted such access except in specified circumstances such as an emergency. ~~Provisions for emergency situations shall be handled in accordance with CIP-003-2 R1.1.~~

Formatted: Indent: Left: 0.25", Hanging: 0.38", Tab stops: 0.63", Left + Not at 1.8"

~~**R3.**~~ ~~Such~~ The Personnel Risk Assessment program shall at a minimum include:

R3.1. The Responsible Entity shall ensure that each assessment conducted include, at least, identity verification (e.g., Social Security Number verification in the U.S.) and seven-year criminal check. The Responsible Entity may conduct more detailed reviews, as permitted by law and subject to existing collective bargaining unit agreements, depending upon the criticality of the position.

R3.2. The Responsible Entity shall update each personnel risk assessment at least every seven years after the initial personnel risk assessment or for cause.

R3.3. The Responsible Entity shall document the results of personnel risk assessments of its personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets, and that personnel risk assessments of contractor and service vendor personnel with such access are conducted pursuant to Standard CIP-004.

R4. Access — The Responsible Entity shall maintain list(s) of personnel with authorized cyber or authorized unescorted physical access to Critical Cyber Assets, including their specific electronic and physical access rights to Critical Cyber Assets.

Formatted: Indent: Left: 0.25", Hanging: 0.38", Tab stops: 0.63", Left + Not at 1.8"

R4.1. The Responsible Entity shall review the list(s) of its personnel who have such access to Critical Cyber Assets quarterly, and update the list(s) within seven calendar days of any change of personnel with such access to Critical Cyber Assets, or any change in the

access rights of such personnel. The Responsible Entity shall ensure access list(s) for contractors and service vendors are properly maintained.

R4.2. The Responsible Entity shall revoke such access to Critical Cyber Assets within 24 hours for personnel terminated for cause and within seven calendar days for personnel who no longer require such access to Critical Cyber Assets.

C. Measures

The following measures will be used to demonstrate compliance with the requirements of Standard CIP-004:

M1. Documentation of the Responsible Entity's security awareness and reinforcement program as specified in Requirement R1.

M2. Documentation of the Responsible Entity's cyber security training program, review, and records as specified in Requirement R2.

M3. Documentation of the personnel risk assessment program and that personnel risk assessments have been applied to all personnel who have authorized cyber or authorized unescorted physical access to Critical Cyber Assets, as specified in Requirement R3.

M4. Documentation of the list(s), list review and update, and access revocation as needed as specified in Requirement R4.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Monitoring Responsibility

1.1.1 Regional Reliability Organizations for Responsible Entities.

1.1.2 NERC for Regional Reliability Organization.

1.1.3 Third-party monitor without vested interest in the outcome for NERC.

1.2. Compliance Monitoring Period and Reset Time Frame

Annually.

1.3. Data Retention

1.3.1 The Responsible Entity shall keep personnel risk assessment documents in accordance with federal, state, provincial, and local laws.

1.3.2 The Responsible Entity shall keep all other documentation required by Standard CIP-004 from the previous full calendar year.

1.3.3 The compliance monitor shall keep audit records for three calendar years.

1.4. Additional Compliance Information

1.4.1 Responsible Entities shall demonstrate compliance through self-certification or audit, as determined by the Compliance Monitor.

1.4.2 Instances where the Responsible Entity cannot conform to its cyber security policy must be documented as exceptions and approved by the designated senior manager or delegate(s). Duly authorized exceptions will not result in non-compliance. Refer to CIP-003 Requirement R3.

2. Levels of Noncompliance

2.1. Level 1:

2.1.1 Awareness program exists, but is not conducted within the minimum required period of quarterly reinforcement; or,

2.1.2 Training program exists, but records of training either do not exist or reveal that personnel who have access to Critical Cyber Assets were not trained as required; or,

2.1.3 Personnel risk assessment program exists, but documentation of that program does not exist; or,

2.1.4 List(s) of personnel with their access rights is available, but has not been reviewed and updated as required.

2.1.5 One personnel risk assessment is not updated at least every seven years, or for cause; or,

2.1.6 One instance of personnel (employee, contractor or service provider) change other than for cause in which access to Critical Cyber Assets was no longer needed was not revoked within seven calendar days.

2.2. Level 2:

2.2.1 Awareness program does not exist or is not implemented; or,

2.2.2 Training program exists, but does not address the requirements identified in Standard CIP-004; or,

2.2.3 Personnel risk assessment program exists, but assessments are not conducted as required; or,

2.2.4 One instance of personnel termination for cause (employee, contractor or service provider) in which access to Critical Cyber Assets was not revoked within 24 hours.

2.3. Level 3:

2.3.1 Training program exists, but has not been reviewed and updated at least annually; or,

2.3.2 A personnel risk assessment program exists, but records reveal program does not meet the requirements of Standard CIP-004; or,

2.3.3 List(s) of personnel with their access control rights exists, but does not include service vendors and contractors.

2.4. Level 4:

2.4.1 No documented training program exists; or,

2.4.2 No documented personnel risk assessment program exists; or,

2.4.3 No required documentation created pursuant to the training or personnel risk assessment programs exists.

E. Regional Differences

None identified.

Version History

Version	Date	Action	Change Tracking
1	01/16/06	D.2.2.4 — Insert the phrase “for cause” as intended. “One instance of personnel	03/24/06

		termination for cause…"	
1	06/01/06	D.2.1.4 — Change "access control rights" to "access rights."	06/05/06

A. Introduction

1. Title: Cyber Security — Physical Security of Critical Cyber Assets

2. Number: CIP-006-2~~CIP-006-1~~

3. Purpose: Standard CIP-006 is intended to ensure the implementation of a physical security program for the protection of Critical Cyber Assets. Standard CIP-006 should be read as part of a group of standards numbered Standards CIP-002 through CIP-009. ~~Responsible Entities should apply Standards CIP-002 through CIP-009 using reasonable business judgment.~~

4. Applicability:

4.1. Within the text of Standard CIP-006, "Responsible Entity" shall mean:

4.1.1 Reliability Coordinator.

4.1.2 Balancing Authority.

4.1.3 Interchange Authority.

4.1.4 Transmission Service Provider.

4.1.5 Transmission Owner.

4.1.6 Transmission Operator.

4.1.7 Generator Owner.

4.1.8 Generator Operator.

4.1.9 Load Serving Entity.

4.1.10 NERC.

4.1.11 Regional Entities

~~4.1.11~~**4.1.12** Regional Reliability Organizations.

4.2. The following are exempt from Standard CIP-006:

4.2.1 Facilities regulated by the U.S. Nuclear Regulatory Commission or the Canadian Nuclear Safety Commission.

4.2.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.3 Responsible Entities that, in compliance with Standard CIP-002, identify that they have no Critical Cyber Assets.

5. Effective Date: XXXX~~June 1, 2006~~

B. Requirements

The Responsible Entity shall comply with the following requirements of Standard CIP-006:

R1. Physical Security Plan — The Responsible Entity shall ~~create~~document, ~~and~~ maintain, and implement a physical security plan, approved by the~~a~~ senior manager or delegate(s) that shall address, at a minimum, the following:

R1.1. ~~Processes to ensure and document that a~~All Cyber Assets within an Electronic Security Perimeter ~~also~~ shall reside within an identified Physical Security Perimeter. Where a completely enclosed ("six-wall") border cannot be established, the Responsible Entity shall deploy and document alternative measures to control physical access to ~~the~~ such~~Critical~~ Cyber Assets.

R1.2. ~~Processes to identify~~ Identification of all access points through each Physical Security Perimeter and measures to control entry at those access points.

R1.3. Processes, tools, and procedures to monitor physical access to the perimeter(s).

R1.4. ~~Procedures for the a~~Appropriate use of physical access controls as described in Requirement R3 including visitor pass management, response to loss, and prohibition of inappropriate use of physical access controls.

R1.5. ~~Procedures for r~~Review~~ing~~ of access authorization requests and revocation of access authorization, in accordance with CIP-004 Requirement R4.

R1.6. Continuous e~~Procedures for e~~Escorted access within the ~~p~~Physical ~~s~~Security ~~p~~Perimeter of personnel not authorized for unescorted access., ~~including procedures for the active monitoring of escorted persons at all times within the Physical Security Perimeter. Escorts are required to actively monitor escorted person at all times while within the Physical Security Perimeter.~~

R1.7. ~~Process for u~~Updat~~inge~~ of the physical security plan within thirty~~ninety~~ calendar days of the completion of any physical security system redesign or reconfiguration, including, but not limited to, addition or removal of access points through the ~~p~~Physical ~~s~~Security ~~p~~Perimeter, physical access controls, monitoring controls, or logging controls.

R1.8. Annual review of the physical security plan.

R2. Protection of Physical Access Control Systems — Cyber Assets that authorize and/or ~~monitoring~~log ~~used in the~~ access ~~control and monitoring~~ ~~of~~ to the Physical Security Perimeter(s), exclusive of hardware at the Physical Security Perimeter access point such as electronic lock control mechanisms and badge readers, shall:

R2.1. be protected from unauthorized physical access.

R2.2. ~~hardware at the Physical Security Perimeter access point such as and badge readers, systems controlling access to cyber assets shall physically monitored~~ be afforded the protective measures specified in Standard CIP-003-1;~~CIP-003,~~ Standard CIP-004-1 Requirement R3;~~R3,~~ Standard CIP-005-1 Requirements R2 and R3;~~R3,~~ Standard CIP-006-2 Requirements ~~-R4R2~~ and R5;~~R3,~~ Standard CIP-007-1;~~CIP-007,~~ Standard CIP-008-1; and Standard CIP-009-1.~~CIP-009.~~

R3. Protection of Electronic Access Control Systems — Cyber Assets used in the access control and/or monitoring of the Electronic Security Perimeter(s) shall reside within an identified Physical Security Perimeter.

~~**R1.8.**~~

~~**R1.9.** Process for ensuring that the physical security plan is reviewed at least annually.~~

~~**R2.**~~**R4.** Physical Access Controls — The Responsible Entity shall document and implement the operational and procedural controls to manage physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week. The Responsible Entity shall implement one or more of the following physical access methods:

~~**R2.1.a)**~~ Card Key: A means of electronic access where the access rights of the card holder are predefined in a computer database. Access rights may differ from one perimeter to another.

~~**R2.2.b)**~~ Special Locks: These include, but are not limited to, locks with "restricted key" systems, magnetic locks that can be operated remotely, and "man-trap" systems.

Formatted: Highlight

Formatted: Highlight

Comment [KBP1]: Needs some more work.

Comment [SRM2]: definition needed

Formatted

Formatted

Formatted: Outline numbered + Level: 2 + Numbering Style: a, b, c, … + Start at: 1 + Alignment: Left + Aligned at: 0.69" + Tab after: 1.19" + Indent at: 1.19"

~~R2.3.~~c) Security Personnel: Personnel responsible for controlling physical access who may reside on-site or at a monitoring station.

~~R2.4.~~d) Other Authentication Devices: Biometric, keypad, token, or other equivalent devices that control physical access to the Critical Cyber Assets.

~~R3.~~R5. Monitoring Physical Access — The Responsible Entity shall document and implement the technical and procedural controls for monitoring physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week. Unauthorized access attempts shall be reviewed immediately and handled in accordance with the procedures specified in Requirement CIP-008. One or more of the following monitoring methods shall be used:

~~R3.1.~~a) Alarm Systems: Systems that alarm to indicate a door, gate or window has been opened without authorization. These alarms must provide for immediate notification to personnel responsible for response.

~~R3.2.~~b) Human Observation of Access Points: Monitoring of physical access points by authorized personnel as specified in Requirement R~~2~~4.3.

~~R4.~~R6. Logging Physical Access — Logging shall record sufficient information to uniquely identify individuals and the time of access twenty-four hours a day, seven days a week. The Responsible Entity shall implement and document the technical and procedural mechanisms for logging physical entry at all access points to the Physical Security Perimeter(s) using one or more of the following logging methods or their equivalent:

~~R4.1.~~a) Computerized Logging: Electronic logs produced by the Responsible Entity's selected access control and monitoring method.

~~R4.2.~~b) Video Recording: Electronic capture of video images of sufficient quality to determine identity.

~~R4.3.~~c) Manual Logging: A log book or sign-in sheet, or other record of physical access maintained by security or other personnel authorized to control and monitor physical access as specified in Requirement R~~2~~4.3.

~~R5.~~R7. Access Log Retention — The responsible entity shall retain physical access logs for at least ninety calendar days. Logs related to reportable incidents shall be kept in accordance with the requirements of Standard CIP-008.

~~R6.~~R8. Maintenance and Testing — The Responsible Entity shall implement a maintenance and testing program to ensure that all physical security systems under Requirements R~~2~~4, R~~3~~5, and R~~4~~6 function properly. The program must include, at a minimum, the following:

~~R6.1.~~R8.1. Testing and maintenance of all physical security mechanisms on a cycle no longer than three years.

~~R6.2.~~R8.2. Retention of testing and maintenance records for the cycle determined by the Responsible Entity in Requirement ~~R6~~R8.1.

~~R6.3.~~R8.3. Retention of outage records regarding access controls, logging, and monitoring for a minimum of one calendar year.

C. Measures

The following measures will be used to demonstrate compliance with the requirements of Standard CIP-006:

M1. The physical security plan as specified in Requirement R1 and documentation of the implementation, review and updating of the plan.

Formatted: Outline numbered + Level: 2 + Numbering Style: a, b, c, … + Start at: 1 + Alignment: Left + Aligned at: 0.69" + Tab after: 1.19" + Indent at: 1.19"

Formatted: Outline numbered + Level: 2 + Numbering Style: a, b, c, … + Start at: 1 + Alignment: Left + Aligned at: 0.69" + Tab after: 1.19" + Indent at: 1.19"

M2. Documentation that the physical access control systems are protected as specified in Requirement R2.

M3. Documentation that the electronic access control systems are located within an identified Physical Security Perimeter as specified in Requirement R3.

M4. Documentation identifying the methods for controlling physical access to each access point of a Physical Security Perimeter as specified in Requirement R4.

~~**M1.**~~

~~**M2.** Documentation identifying the methods for controlling physical access to each access point of a Physical Security Perimeter as specified in Requirement R2.~~

~~M3.~~M5. Documentation identifying the methods for monitoring physical access as specified in Requirement R~~3~~5.

~~M4.~~M6. Documentation identifying the methods for logging physical access as specified in Requirement R~~4~~6.

~~M5.~~M7. Access logs as specified in Requirement R~~5~~7.

~~M6.~~M8. Documentation as specified in Requirement R~~6~~8.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Monitoring Responsibility

1.1.1 Regional Reliability Organizations for Responsible Entities.

1.1.2 NERC for Regional Reliability Organization.

1.1.3 Third-party monitor without vested interest in the outcome for NERC.

1.2. Compliance Monitoring Period and Reset Time Frame

Annually.

1.3. Data Retention

1.3.1 The Responsible Entity shall keep documents other than those specified in Requirements ~~R5~~ R7 and ~~R6~~R8.2 from the previous full calendar year.

1.3.2 The compliance monitor shall keep audit records for three calendar years.

1.4. Additional Compliance Information

1.4.1 Responsible Entities shall demonstrate compliance through self-certification or audit, as determined by the Compliance Monitor.

1.4.2 Instances where the Responsible Entity cannot conform to its cyber security policy must be documented as exceptions and approved by the designated senior manager or delegate(s). Duly authorized exceptions will not result in noncompliance. Refer to Standard CIP-003 Requirement R3.

1.4.3 The Responsible Entity may not make exceptions in its cyber security policy to the creation, documentation, or maintenance of a physical security plan.

1.4.4 For dial-up accessible Critical Cyber Assets that use non-routable protocols, the Responsible Entity shall not be required to comply with Standard CIP-006 for that single access point at the dial-up device~~.device.~~

2. Levels of Noncompliance

2.1. Level 1:

Formatted: Indent: Left: 0.65", No bullets or numbering

Comment [KBP3]: The SCE&G interpretation is at considerable risk of being rejected by FERC. I strongly recommend it be deferred in order to not put a timely Phase I acceptance in jeopardy.

Comment [th4]: Address SCE&G RFI

Comment [KBP5]: OK to defer to Phase II

2.1.1 The physical security plan exists, but has not been updated within ninety calendar days of a modification to the plan or any of its components; or,

2.1.2 Access to less than 15% of a Responsible Entity's total number of physical security perimeters is not controlled, monitored, and logged; or,

2.1.3 Required documentation exists but has not been updated within ninety calendar days of a modification.; or,

2.1.4 Physical access logs are retained for a period shorter than ninety days; or,

2.1.5 A maintenance and testing program for the required physical security systems exists, but not all have been tested within the required cycle; or,

2.1.6 One required document does not exist.

2.2. Level 2:

2.2.1 The physical security plan exists, but has not been updated within six calendar months of a modification to the plan or any of its components; or,

2.2.2 Access to between 15% and 25% of a Responsible Entity's total number of physical security perimeters is not controlled, monitored, and logged; or,

2.2.3 Required documentation exists but has not been updated within six calendar months of a modification; or

2.2.4 More than one required document does not exist.

2.3. Level 3:

2.3.1 The physical security plan exists, but has not been updated or reviewed in the last twelve calendar months of a modification to the physical security plan; or,

2.3.2 Access to between 26% and 50% of a Responsible Entity's total number of physical security perimeters is not controlled, monitored, and logged; or,

2.3.3 No logs of monitored physical access are retained.

2.4. Level 4:

2.4.1 No physical security plan exists; or,

~~2.4.1~~2.4.2 The physical security plan has not been implemented; or,

~~2.4.2~~2.4.3 Access to more than 51% of a Responsible Entity's total number of physical security perimeters is not controlled, monitored, and logged; or,

~~2.4.3~~2.4.4 No maintenance or testing program exists.

E. **Regional Differences**

None identified.

Version History

Version	Date	Action	Change Tracking

A. Introduction

1. Title: Cyber Security — Systems Security Management

2. Number: CIP-007-~~1~~2

3. Purpose: Standard CIP-007 requires Responsible Entities to define methods, processes, and procedures for securing those systems determined to be Critical Cyber Assets, as well as the ~~non-critical~~other Cyber Assets within the Electronic Security Perimeter(s). Standard CIP-007 should be read as part of a group of standards numbered Standards CIP-002 through CIP-009. ~~Responsible Entities should interpret and apply Standards CIP-002 through CIP-009 using reasonable business judgment.~~

4. Applicability:

4.1. Within the text of Standard CIP-007, "Responsible Entity" shall mean:

4.1.1 Reliability Coordinator.

4.1.2 Balancing Authority.

4.1.3 Interchange Authority.

4.1.4 Transmission Service Provider.

4.1.5 Transmission Owner.

4.1.6 Transmission Operator.

4.1.7 Generator Owner.

4.1.8 Generator Operator.

4.1.9 Load Serving Entity.

4.1.10 NERC.

4.1.11 Regional Entities

~~4.1.11~~4.1.12 Regional Reliability Organizations.

4.2. The following are exempt from Standard CIP-007:

4.2.1 Facilities regulated by the U.S. Nuclear Regulatory Commission or the Canadian Nuclear Safety Commission.

4.2.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.3 Responsible Entities that, in compliance with Standard CIP-002, identify that they have no Critical Cyber Assets.

5. Effective Date: ~~June 1, 2006~~XXXX

B. Requirements

The Responsible Entity shall comply with the following requirements of Standard CIP-007 for all Critical Cyber Assets and other Cyber Assets within the Electronic Security Perimeter(s):

R1. Test Procedures — The Responsible Entity shall ensure that new Cyber Assets and significant changes to existing Cyber Assets within the Electronic Security Perimeter do not adversely affect existing cyber security controls. For purposes of Standard CIP-007, a significant change shall, at a minimum, include implementation of security patches, cumulative service packs, vendor releases, and version upgrades of operating systems, applications, database platforms, or other third-party software or firmware.

R1.1. The Responsible Entity shall create, implement, and maintain cyber security test procedures in a manner that minimizes adverse effects on the production system or its operation.

R1.2. The Responsible Entity shall document that testing is performed in a manner that reflects the production environment.

R1.3. The Responsible Entity shall document test results.

R2. Ports and Services — The Responsible Entity shall establish ~~and~~ , document and implement a process to ensure that only those ports and services required for normal and emergency operations are enabled.

R2.1. The Responsible Entity shall enable only those ports and services required for normal and emergency operations.

R2.2. The Responsible Entity shall disable other ports and services, including those used for testing purposes, prior to production use of all Cyber Assets inside the Electronic Security Perimeter(s).

R2.3. In the case where unused ports and services cannot be disabled due to technical limitations, the Responsible Entity shall document compensating measure(s) applied to mitigate risk exposure or an acceptance of risk.

R3. Security Patch Management — The Responsible Entity, either separately or as a component of the documented configuration management process specified in CIP-003-1 Requirement R6, shall establish ~~and~~ , document and implement a security patch management program for tracking, evaluating, testing, and installing applicable cyber security software patches for all Cyber Assets within the Electronic Security Perimeter(s).

R3.1. The Responsible Entity shall document the assessment of security patches and security upgrades for applicability within thirty calendar days of availability of the patches or upgrades.

R3.2. The Responsible Entity shall document the implementation of security patches. In any case where the patch is not installed, the Responsible Entity shall document compensating measure(s) applied to mitigate risk exposure or an acceptance of risk.

R4. Malicious Software Prevention — The Responsible Entity shall use anti-virus software and other malicious software ("malware") prevention tools, where technically feasible, to detect, prevent, deter, and mitigate the introduction, exposure, and propagation of malware on all Cyber Assets within the Electronic Security Perimeter(s).

R4.1. The Responsible Entity shall document and implement anti-virus and malware prevention tools. In the case where anti-virus software and malware prevention tools are not installed, the Responsible Entity shall document compensating measure(s) applied to mitigate risk exposure ~~or an acceptance of risk~~.

R4.2. The Responsible Entity shall document and implement a process for the update of anti-virus and malware prevention "signatures." The process must address testing and installing the signatures.

R5. Account Management — The Responsible Entity shall establish, implement, and document technical and procedural controls that enforce access authentication of, and accountability for, all user activity, and that minimize the risk of unauthorized system access.

R5.1. The Responsible Entity shall ensure that individual and shared system accounts and authorized access permissions are consistent with the concept of "need to know" with respect to work functions performed.

R5.1.1. The Responsible Entity shall ensure that user accounts are implemented as approved by designated personnel. Refer to Standard CIP-003-1 Requirement R5.

R5.1.2. The Responsible Entity shall establish methods, processes, and procedures that generate logs of sufficient detail to create historical audit trails of individual user account access activity for a minimum of ninety days.

R5.1.3. The Responsible Entity shall review, at least annually, user accounts to verify access privileges are in accordance with Standard CIP-003-1 Requirement R5 and Standard CIP-004-1 Requirement R4.

R5.2. The Responsible Entity shall implement a policy to minimize and manage the scope and acceptable use of administrator, shared, and other generic account privileges including factory default accounts.

R5.2.1. The policy shall include the removal, disabling, or renaming of such accounts where possible. For such accounts that must remain enabled, passwords shall be changed prior to putting any system into service.

R5.2.2. The Responsible Entity shall identify those individuals with access to shared accounts.

R5.2.3. Where such accounts must be shared, the Responsible Entity shall have a policy for managing the use of such accounts that limits access to only those with authorization, an audit trail of the account use (automated or manual), and steps for securing the account in the event of personnel changes (for example, change in assignment or termination).

R5.3. At a minimum, the Responsible Entity shall require and use passwords, subject to the following, as technically feasible:

R5.3.1. Each password shall be a minimum of six characters.

R5.3.2. Each password shall consist of a combination of alpha, numeric, and "special" characters.

R5.3.3. Each password shall be changed at least annually, or more frequently based on risk.

R6. Security Status Monitoring — The Responsible Entity shall ensure that all Cyber Assets within the Electronic Security Perimeter, as technically feasible, implement automated tools or organizational process controls to monitor system events that are related to cyber security.

R6.1. The Responsible Entity shall implement and document the organizational processes and technical and procedural mechanisms for monitoring for security events on all Cyber Assets within the Electronic Security Perimeter.

R6.2. The security monitoring controls shall issue automated or manual alerts for detected Cyber Security Incidents.

R6.3. The Responsible Entity shall maintain logs of system events related to cyber security, where technically feasible, to support incident response as required in Standard CIP-008.

R6.4. The Responsible Entity shall retain all logs specified in Requirement R6 for ninety calendar days.

R6.5. The Responsible Entity shall review logs of system events related to cyber security and maintain records documenting review of logs.

R7. Disposal or Redeployment — The Responsible Entity shall establish and implement formal methods, processes, and procedures for disposal or redeployment of Cyber Assets within the Electronic Security Perimeter(s) as identified and documented in Standard CIP-005.

R7.1. Prior to the disposal of such assets, the Responsible Entity shall destroy or erase the data storage media to prevent unauthorized retrieval of sensitive cyber security or reliability data.

R7.2. Prior to redeployment of such assets, the Responsible Entity shall, at a minimum, erase the data storage media to prevent unauthorized retrieval of sensitive cyber security or reliability data.

R7.3. The Responsible Entity shall maintain records that such assets were disposed of or redeployed in accordance with documented procedures.

R8. Cyber Vulnerability Assessment — The Responsible Entity shall perform a cyber vulnerability assessment of all Cyber Assets within the Electronic Security Perimeter at least annually. The vulnerability assessment shall include, at a minimum, the following:

R8.1. A document identifying the vulnerability assessment process;

R8.2. A review to verify that only ports and services required for operation of the Cyber Assets within the Electronic Security Perimeter are enabled;

R8.3. A review of controls for default accounts; and,

R8.4. Documentation of the results of the assessment, the action plan to remediate or mitigate vulnerabilities identified in the assessment, and the execution status of that action plan.

R9. Documentation Review and Maintenance — The Responsible Entity shall review and update the documentation specified in Standard CIP-007 at least annually. Changes resulting from modifications to the systems or controls shall be documented within ~~ninety~~thirty calendar days of the change being completed.

Formatted: Font: 11 pt

Formatted: Font: 11 pt

Formatted: Font: 11 pt

C. Measures

The following measures will be used to demonstrate compliance with the requirements of Standard CIP-007:

M1. Documentation of the Responsible Entity's security test procedures as specified in Requirement R1.

M2. Documentation as specified in Requirement R2.

M3. Documentation and records of the Responsible Entity's security patch management program, as specified in Requirement R3.

M4. Documentation and records of the Responsible Entity's malicious software prevention program as specified in Requirement R4.

M5. Documentation and records of the Responsible Entity's account management program as specified in Requirement R5.

M6. Documentation and records of the Responsible Entity's security status monitoring program as specified in Requirement R6.

M7. Documentation and records of the Responsible Entity's program for the disposal or redeployment of Cyber Assets as specified in Requirement R7.

M8. Documentation and records of the Responsible Entity's annual vulnerability assessment of all Cyber Assets within the Electronic Security Perimeters(s) as specified in Requirement R8.

M9. Documentation and records demonstrating the review and update as specified in Requirement R9.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Monitoring Responsibility

1.1.1 Regional Reliability Organizations for Responsible Entities.

1.1.2 NERC for Regional Reliability Organization.

1.1.3 Third-party monitor without vested interest in the outcome for NERC.

1.2. Compliance Monitoring Period and Reset Time Frame

Annually.

1.3. Data Retention

1.3.1 The Responsible Entity shall keep all documentation and records from the previous full calendar year.

1.3.2 The Responsible Entity shall retain security–related system event logs for ninety calendar days, unless longer retention is required pursuant to Standard CIP-008 Requirement R2.

1.3.3 The compliance monitor shall keep audit records for three calendar years.

1.4. Additional Compliance Information.

1.4.1 Responsible Entities shall demonstrate compliance through self-certification or audit, as determined by the Compliance Monitor.

1.4.2 Instances where the Responsible Entity cannot conform to its cyber security policy must be documented as exceptions and approved by the designated senior manager or delegate(s). Duly authorized exceptions will not result in non-compliance. Refer to Standard CIP-003 Requirement R3.

2. Levels of Noncompliance

2.1. Level 1:

2.1.1 System security controls are in place, but fail to document one of the measures (M1-M9) of Standard CIP-007; or

2.1.2 One of the documents required in Standard CIP-007 has not been reviewed in the previous full calendar year as specified by Requirement R9; or,

2.1.3 One of the documented system security controls has not been updated within ninety calendar days of a change as specified by Requirement R9; or,

2.1.4 Any one of:

- Authorization rights and access privileges have not been reviewed during the previous full calendar year; or,
- A gap exists in any one log of system events related to cyber security of greater than seven calendar days; or,
- Security patches and upgrades have not been assessed for applicability within thirty calendar days of availability.

2.2. Level 2:

2.2.1 System security controls are in place, but fail to document up to two of the measures (M1-M9) of Standard CIP-007; or,

2.2.2 Two occurrences in any combination of those violations enumerated in Noncompliance Level 1, 2.1.4 within the same compliance period.

2.3. Level 3:

2.3.1 System security controls are in place, but fail to document up to three of the measures (M1-M9) of Standard CIP-007; or,

2.3.2 Three occurrences in any combination of those violations enumerated in Noncompliance Level 1, 2.1.4 within the same compliance period.

2.4. Level 4:

2.4.1 System security controls are in place, but fail to document four or more of the measures (M1-M9) of Standard CIP-007; or,

2.4.2 Four occurrences in any combination of those violations enumerated in Noncompliance Level 1, 2.1.4 within the same compliance period.

2.4.3 No logs exist.

E. Regional Differences

None identified.

Version History

Version	Date	Action	Change Tracking

A. Introduction

1. Title: Cyber Security — Incident Reporting and Response Planning

2. Number: CIP-008-~~1~~2

3. Purpose: Standard CIP-008 ensures the identification, classification, response, and reporting of Cyber Security Incidents related to Critical Cyber Assets. Standard CIP-008 should be read as part of a group of standards numbered Standards CIP-002 through CIP-009. ~~Responsible Entities should apply Standards CIP-002 through CIP-009 using reasonable business judgment.~~

4. Applicability

4.1. Within the text of Standard CIP-008, "Responsible Entity" shall mean:

4.1.1 Reliability Coordinator.

4.1.2 Balancing Authority.

4.1.3 Interchange Authority.

4.1.4 Transmission Service Provider.

4.1.5 Transmission Owner.

4.1.6 Transmission Operator.

4.1.7 Generator Owner.

4.1.8 Generator Operator.

4.1.9 Load Serving Entity.

4.1.10 NERC.

4.1.11 Regional Entities

~~4.1.11~~**4.1.12** Regional Reliability Organizations.

4.2. The following are exempt from Standard CIP-008:

4.2.1 Facilities regulated by the U.S. Nuclear Regulatory Commission or the Canadian Nuclear Safety Commission.

4.2.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.3 Responsible Entities that, in compliance with Standard CIP-002, identify that they have no Critical Cyber Assets.

5. Effective Date: ~~June 1, 2006~~XXXX

B. Requirements

The Responsible Entity shall comply with the following requirements of Standard CIP-008:

R1. Cyber Security Incident Response Plan — The Responsible Entity shall develop and maintain a Cyber Security Incident response plan and implement the plan in response to Cyber Security Incidents. The Cyber Security Incident ~~Response~~ response plan shall address, at a minimum, the following:

R1.1. Procedures to characterize and classify events as reportable Cyber Security Incidents.

R1.2. Response actions, including roles and responsibilities of Cyber Security Incident~~incident~~ response teams, Cyber Security Incident~~incident~~ handling procedures, and communication plans.

R1.3. Process for reporting Cyber Security Incidents to the Electricity Sector Information Sharing and Analysis Center (ES–ISAC). The Responsible Entity must ensure that all reportable Cyber Security Incidents are reported to the ES–ISAC either directly or through an intermediary.

R1.4. Process for updating the Cyber Security Incident response plan within ~~ninety~~thirty calendar days of any changes.

R1.5. Process for ensuring that the Cyber Security Incident response plan is reviewed at least annually.

R1.6. Process for ensuring the Cyber Security Incident response plan is tested at least annually. A test of the Cyber Security Incident ~~incident~~ response plan can range from a paper drill, to a full operational exercise, to the response to an actual incident. Testing the Cyber Security Incident response plan does not require removing a component or system from service during the test.

R2. Cyber Security Incident Documentation — The Responsible Entity shall keep relevant documentation related to Cyber Security Incidents reportable per Requirement R1.1 for three calendar years.

C. Measures

The following measures will be used to demonstrate compliance with the requirements of CIP-008:

M1. The Cyber Security Incident response plan as indicated in R1 and documentation of the review, updating, and testing of the plan

M2. All documentation as specified in Requirement R2.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Monitoring Responsibility

1.1.1 Regional Reliability Organizations for Responsible Entities.

1.1.2 NERC for Regional Reliability Organization.

1.1.3 Third-party monitor without vested interest in the outcome for NERC.

1.2. Compliance Monitoring Period and Reset Time Frame

Annually.

1.3. Data Retention

1.3.1 The Responsible Entity shall keep documentation other than that required for reportable Cyber Security Incidents as specified in Standard CIP-008 for the previous full calendar year.

1.3.2 The compliance monitor shall keep audit records for three calendar years.

1.4. Additional Compliance Information

1.4.1 Responsible Entities shall demonstrate compliance through self-certification or audit, as determined by the Compliance Monitor.

1.4.2 Instances where the Responsible Entity cannot conform to its cyber security policy must be documented as exceptions and approved by the designated senior manager or delegate(s). Duly authorized exceptions will not result in non-compliance. Refer to Standard CIP-003 Requirement R3.

1.4.3 The Responsible Entity may not take exception in its cyber security policies to the creation of a Cyber Security Incident response plan.

1.4.4 The Responsible Entity may not take exception in its cyber security policies to reporting Cyber Security Incidents to the ES ISAC.

2. Levels of Noncompliance

2.1. Level 1: A Cyber Security Incident response plan exists, but has not been updated within ninety calendar days of changes.

2.2. Level 2:

2.2.1 A Cyber Security Incident response plan exists, but has not been reviewed in the previous full calendar year; or,

2.2.2 A Cyber Security Incident response plan has not been tested in the previous full calendar year; or,

2.2.3 Records related to reportable Cyber Security Incidents were not retained for three calendar years.

2.3. Level 3:

2.3.1 A Cyber Security Incident response plan exists, but does not include required elements Requirements R1.1, R1.2, and R1.3 of Standard CIP-008; or,

2.3.2 A reportable Cyber Security Incident has occurred but was not reported to the ES ISAC.

2.4. Level 4: A Cyber Security Incident response plan does not exist.

E. Regional Differences

None identified.

Version History

Version	Date	Action	Change Tracking

NERC

NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Cyber Security Standards: Phase 1 Issues Proposal

SDT Meeting

SMUD

October 21-22, 2008

Scott Mix, CISSP
Manager of Situation Awareness and Infrastructure Security
Scott.Mix@NERC.net
215-853-8204

to ensure the reliability of the bulk power system

Phase 1 Agreed-to Recap

- Remove Reasonable Business Judgment
- Add Regional Entities
- “Implement” procedures
- Approval of Risk-based Assessment Methodology
- Remove business phone & Address from Senior Manager identification requirements
- Document delegations of authority

Phase 1 Agreed-to Recap

- Train prior to access
- PRA prior to access
- Update plans (etc) 30 days after implementation of change
- Remove “acceptance or risk” for malware
- Clarity testing does not require removing an asset from service

Phase 1 To-Do

- CIP-006 Dial-up accessible assets interpretation (SCG&E)
- CIP-006 Cabling Interpretation (Progress Energy)
- Wording changes in CIP-004
- Review Measures with respect to revised requirements
- Implementation Plan – newly identified assets
- Implementation Plan – revised requirements & mapping matrix
- Comment Form

Phase 1 Issues dropped from initial proposal

- CIP-002:
  - Approval of CA list by external entity (i.e., RC, RE, etc)
  - Newly identified assets (as a requirement – working group for implementation plan addendum formed)
- CIP-003:
  - “single” senior manager
  - Escort requirements

Phase 1 Issues dropped from initial proposal

- CIP-004:
  - Training “ensure” language
  - Training “emergency” language, including post-emergency review activities
  - Networking hardware and software included in training
  - Training on escort requirements
  - Training must be appropriate to trainees responsibilities
  - Limited escorted access for new hires or transfers
  - Emergency provision for increased access and approval, including post-emergency review activities

Phase 1 Issues dropped from initial proposal

- CIP-008:
  - Procedures when a documented plan is not followed
  - Requirement to update plan to include response to an event for which there is no documented plan
- CIP-009:
  - Procedures when a documented plan is not followed
  - Requirement to update plan to include recovery to an event for which there is no documented plan

Technical Feasibility Process Strawman

- Constraints:
  - All requirements of a standard must be adhered to
    - No exceptions
  - Self-report of an non-compliance (exception) with Mitigation Plan is allowed
  - FERC Order 706

FERC Order 706 Language

"The Commission continues to view the term 'acceptance of risk' as representing an uncontrolled exception from compliance." (150)

"… any alternative language that provides a similar opportunity for a responsible entity to opt out of compliance would be subject to remand." (151)

"…alternative language that deals with such issues in terms of technical feasibility is preferable." (151)

"… we have adopted the concept of technical feasibility to encompass a broader range of valid justifications." (151)

FERC Order 706 Language

"Expanding the use of the technical feasibility conditions would address the desire for flexibility expressed by some commenters while providing the control that the Commission finds to be necessary." (152)

"…we note that we have found that technical feasibility should not be limited simply to whether something is technically possible but also whether it is technically safe and operationally reasonable." (152)

FERC Order 706 Language

"… we note that a long-established practice of risk acceptance by senior management does not mean that a continuation of this practice is appropriate under a new system of mandatory cyber security Reliability Standards." (153)

"The commission's concern in the CIP NOPR was with the lack of appropriate controls, and eliminating references to acceptance or risk does not imply that all risk can be eliminated." (154)

FERC Order 706 Language

"The Commission … directs the ERO to develop a set of conditions or criteria that a responsible entity must follow when relying on the technical feasibility exception contained in specific Requirements of the CIP Reliability Standards." (178)

"… conditions for invoking technical feasibility exception should allow for operational considerations." (178)

FERC Order 706 Language

"… did not propose to eliminate references to technical feasibility from the CIP Reliability Standards, only that the term be interpreted narrowly…" (178)

"… underlying rationale for a technical feasibility exception … are an acknowledged concern." (178)

"… acknowledge that the possibility of being required to replace equipment before the end of its useful life is a valid concern." (180)

FERC Order 706 Language

"… disagrees … that technical feasibility should be interpreted to apply to future assets also." (181)

"… technical feasibility exceptions may be permitted if appropriate conditions are in place. The term technical feasibility should be interpreted narrowly not to include consideration of business judgment, but we agree … that is should include operational and safety considerations." (186)

FERC Order 706 Language

"… the Commission adopts the CIP NOPR proposal for a three step structure to require accountability when a responsible entity relies on technical feasibility as the basis for exception. We address mitigation and remediation in this section and direct he ERO to develop: (1) a requirement that the responsible entity must develop, document and implement a mitigation plan that achieves a comparable level of security to the requirement; and, (2) a requirement that the use of the technical feasibility exception by a responsible entity must be accompanied by a remediation plan and timeline for elimination of the technical feasibility exemption. … a date certain for remediation may not be possible in some instances." (192)

FERC Order 706 Language

"… technical feasibility exemptions should be reported and justified and subject to approval by the ERO or the relevant Regional Entity." (209)

"… we continue to believe that internal approval is an important component of an overall framework of accountability with regard to use of the technical feasibility exemption. … direct the ERO to include approval of mitigation and remediation steps by the senior manager…" (211)

FERC Order 706 Language

"… Regional Entities should, in the first instance, receive and catalog notices of technical feasibility exceptions that are claimed." (213)

"… actual evaluation and approval of technical feasibility exceptions should be performed in the first instance in the audit process. … include personnel in audit teams with sufficient expertise to judge the need for a technical feasibility exception and the sufficiency of preferred mitigation measures." (214)

FERC Order 706 Language

"… initial audits of technical feasibility exceptions should be expedited, i.e., performed earlier than otherwise, including moving the audit to an earlier year." (215)

"… rather than a pre-approval process, we direct the ERO to design and conduct an approval process through the Regional Entities and the compliance audit process. … the ERO or a Regional Entity to approve any technical feasibility exception, taking into account whether the technical feasibility exception is needed and whether the mitigation and remediation steps are adequate to the circumstance." (218)

FERC Order 706 Language

"… we direct NERC, in developing the accountability structure for the technical feasibility exception, to include appropriate provisions to assure that governmental entities … can safeguard sensitive information." (219)

"… we direct the ERO to develop a set of criteria to provide accountability when a responsible entity relies on the technical feasibility exceptions…" (222)

FERC Order 706 Language

"… framework to include mitigation steps, a remediation plan, a timeline for eliminating the use of the technical feasibility exception unless appropriate justification otherwise is provided, regular review of whether it continues to be necessary to invoke the exception, internal approval by the senior manager, wide-area approval through the ERO's audit process, and cooperation with the ERO to provide the Commission with high-level, wide-area analysis regarding th eeffects of the technical feasibility exception on the reliability of the Bulk-Power System." (222)

FERC Technical Feasibility Process

- Document the exception,
- Document mitigation steps,
- Document a remediation plan,
- Document a timeline for eliminating the use of the technical feasibility exception unless appropriate justification otherwise is provided,
- Provide regular review of whether it continues to be necessary to invoke the exception,
- Document internal approval by the senior manager,
- Document wide-area approval through the ERO's audit process, and
- Provide cooperation with the ERO to provide the Commission with high-level, wide-area analysis regarding the effects of the technical feasibility exception on the reliability of the Bulk-Power System

Current Self-report Process

- Document non-compliance to a specific requirement
- Provide explanation of the non-compliance
- Describe reliability impact
- Describe any external or extraneous factors
- Provide a mitigation plan
- Provide a mitigation schedule
- Senior Officer signature
- Catalog and Approval by Regional Entity
- Catalog and Approval by ERO
- Submit to FERC (US entities)

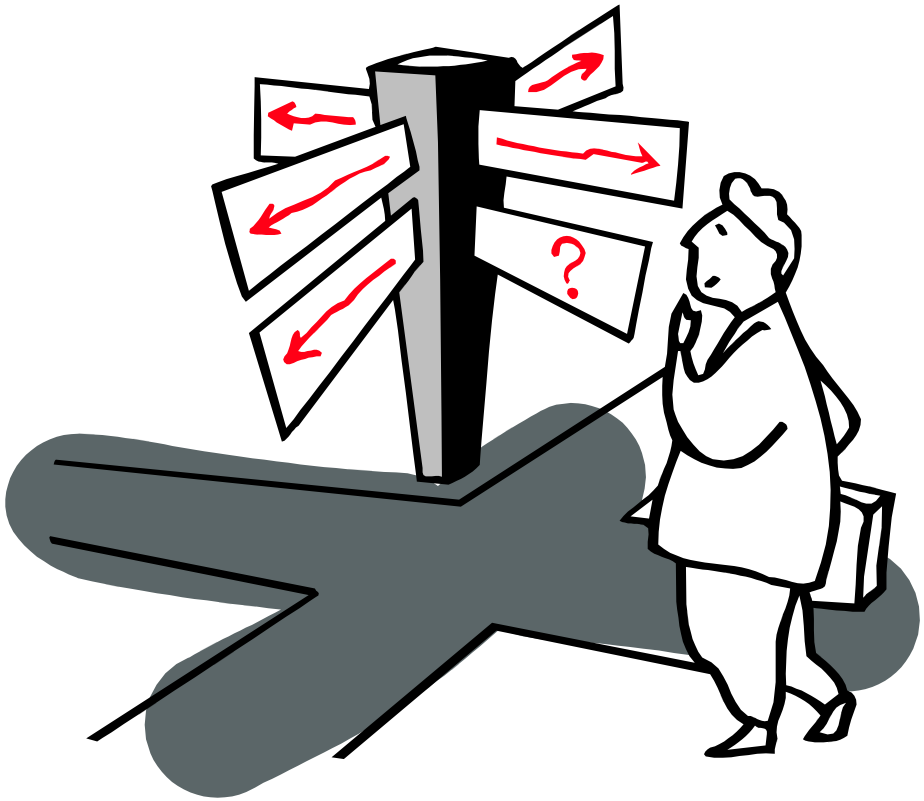
Conclusion

- A Technical Feasibility report becomes a special case Self-report of Non-compliance:
  - New “CIP-003 R4”
    - or is it a Guideline?
  - Discussion of ‘impact to reliability’ if the Technical Feasibility exemption is not taken
    - Also includes statement of technical incompatibility
  - Mandatory compensating / mitigating measures while the Technical Feasibility exemption is in effect
  - Documented justification for not supplying a mitigation plan (i.e., an alternative measure)

Conclusion (cont'd)

- Annual review and re-approval by Responsible Entity, RE, and ERO regardless of mitigation plan status
- ERO to develop separate annual report to FERC
  - Report will contain sensitive information – must be CEII protected
  - Analyzes the combined impact of all Technical Feasibility exemptions
- May trigger accelerated audit schedule

Questions



Scott.Mix@NERC.net
215-853-8204

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Comment Form for Phase I of Project 2008-06

Please use this form to submit comments on the proposed revisions of CIP-002-1 through CIP-009-1, developed by the standard drafting team as part of Project 2008-06 – Cyber Security Order 706. Comments must be submitted by **[December 31, 2008]**. If you have questions please contact Harry Tom at Harry.Tom@nerc.net or by telephone at (609) 452-8060.

Individual Commenter Information **(Complete this page for comments from one organization or individual.)**		
Name:		
Organization:		
Telephone:		
E-mail:		
NERC Region (check all Regions in which your company operates)		**Registered Ballot Body Segment (check all industry segments in which your company is registered)**
☐ **ERCOT**	☐	1 — Transmission Owners
☐ **FRCC**	☐	2 — RTOs and ISOs
☐ **MRO**	☐	3 — Load-serving Entities
☐ **NPCC**	☐	4 — Transmission-dependent Utilities
☐ **RFC**	☐	5 — Electric Generators
☐ **SERC**	☐	6 — Electricity Brokers, Aggregators, and Marketers
☐ **SPP**	☐	7 — Large Electricity End Users
☐ **WECC**	☐	8 — Small Electricity End Users
☐ **NA – Not Applicable**	☐	9 — Federal, State, Provincial Regulatory or other Government Entities
	☐	10 — Regional Reliability Organizations and Regional Entities

Comment Form

Group Comments (Complete this page if comments are from a group.)

Group Name:

Lead Contact:

Contact Organization:

Contact Segment:

Contact Telephone:

Contact E-mail:

Additional Member Name	Additional Member Organization	Region*	Segment*

*If more than one Region or Segment applies, please list all that apply. Regional acronyms and segment numbers are shown on prior page.

Comment Form

Background Information ~~(John Lim)~~

~~The purpose of Project 2008-06 Cyber Security Order 706 is to update and revise the following Cyber Security Standards as scoped out in the Standard Authorization Request and FERC Order 706 to protect the critical cyber assets (including hardware, software, data, and communications networks) essential to the reliable operations of the bulk power system:~~

~~CIP-002-1 Critical Cyber Asset Identification~~
~~CIP-003-1 Security Management Controls~~
~~CIP-004-1 Personnel & Training~~
~~CIP-005-1 Electronic Security Perimeter(s)~~
~~CIP-006-1 Physical Security of Critical Cyber Assets~~
~~CIP-007-1 Systems Security Management~~
~~CIP-008-1 Incident Reporting and Response Planning~~
~~CIP-009-1 Recovery Plans for Critical Cyber Assets~~

~~The SDT is responsible for producing just and reasonable standards that are not unduly discriminatory or preferential and that are in the public interest. The SDT is to consider the scope items in the SAR and FERC Order 706, when revising the CIP Standards, including:~~

- ~~Blackout report recommendations;~~
- ~~Eliminate the phrase "reasonable business judgment" in the standards before the compliance audits commence in July 2009.~~
- ~~How to address acceptance of risk exceptions and accountability.~~
- ~~Develop specific conditions that a reasonable entity must satisfy to invoke the "technical feasibility" exception;~~
- ~~Data as a critical cyber asset and help to defining critical assets - and what external review and procedures may be involved and who should be involved in that process;~~
- ~~Application of a measurable "defense in depth" to create an electronic security perimeter. Different definitions by different world - network view of the world vs. operations.~~
- ~~What strong controls are needed and how much change triggers an "active vulnerability assessment" (change controls).~~
- ~~Modify the standards to conform to the ERO Rules of Procedure as outlined in the Standard Review Guidelines~~
- ~~Multi-phase approach to satisfy what needs to be done in the short term~~

On July 10th, 2008, the NERC Standards Committee approved the Standard A~~cti~~uthorization Request SAR) for developing revisions to Critical Infrastructure Protection Cyber Security Standards (revisions to CIP-002 through CIP-009). A Standards Drafting Team (SDT) was appointed by the Standards Committee on August 7, 2008 to develop these revisions. The overall drafting project requires reviewing each of the standards to ensure that it conforms to the latest version of the ERO Rules of Procedure, including the Reliability Standards Development Procedure as outlined in the Standard Review Guidelines. The revisions will also address all of the directed modifications identified in the FERC Final Order 706.

In addition, the SDT will consider the inclusion of clarifications from Requests for Interpretation to the CIP-002-1 – CIP-009-1 cyber security standards.
~~In addition, the SDT will consider the inclusion of clarifications from Requests for Interpretation to the CIP-002-1 – CIP-009-2 cyber security standards.~~

Comment [JL1]: Corrected typo from -2 to -1

Comment [t2]: SE: John, is it CIP009-2?

The SDT will also consider other Cyber-related standards, guidelines and activities:

- The NIST Security Risk Management Framework (includes GAO, OMB and FIPS)
- Other cyber security related documents such as NIST, ISO 27000 Family, CIPC Risk Assessment Guideline, MITRE corporation technical report, DHS, National Laboratories papers, DOE 417, IEC, ISA, etc.
- Coordination work between FERC, NEI and NRC in regard to the nuclear facility exemption issue with respect to regulatory gaps and modify, as necessary, the standards to reflect current determinations.

Formatted: Bulleted + Level: 1 + Aligned at: 0.25" + Indent at: 0.5"

Revisions will consider the additional issues identified by stakeholders in the SAR comment process:

Industry Education

- Consider what to do with the existing FAQ document e.g., modify, replace.
- Consider how to provide additional guidance in support of these standards, e.g., Technical Reference documents, guidelines, white papers.
- Consider development of a guideline document to address extended LANs over multiple geographically dispersed locations.

Formatted: Bulleted + Level: 1 + Aligned at: 0.25" + Indent at: 0.5"

Balloting and Implementation

- Determine the timing and grouping of revisions to be submitted to industry for comment and ballot, e.g., multi-phase or other approach.
- Determine the optimum implementation plan for revised CIP standards in this project.
- Address when newly identified critical assets or critical cyber assets, newly acquired equipment or assets, etc. must come into compliance with CIP standards.
- Address compliance issue where internal requirements exceed NERC requirements.
- Clarify in view of language contained in FERC Order 706 paragraph 377.

Formatted: Bulleted + Level: 1 + Aligned at: 0.25" + Indent at: 0.5"

Clarify Existing Requirements

- Consider the need for different requirements for different environments e.g., control center, substation and generation plant.
- Clarify how serial and wireless devices are subject to these standards. Refer to pp 278 and 285 of FERC Order 706.

Formatted: Bulleted + Level: 1 + Aligned at: 0.25" + Indent at: 0.5"

Other Issues

- Consider issues surrounding protection of data in motion.
- Consider the issue of hybrid devices that use both serial and routable protocols.
- Consider the issue of data versus information (electronic and/or hardcopy lists, drawings, etc.) protection including transport and transmittal of such information.
- Consider a clearly defined set of risks which can result in a more focused and effective set of compliance expectations.
- With regard to third-party vendors and contractors, provide clarification and additional guidance as to how much a responsible entity may rely on the processes and procedures of contractors and vendors that support the critical infrastructure of that responsible entity under the CIP standards and still be compliant with the standard.

Formatted: Bulleted + Level: 1 + Aligned at: 0.25" + Indent at: 0.5"

Because of the extensive scope and varying complexity of the issues and work in these revisions, the SDT, at its meeting on October 6th-8th, 2008, decided on a multiphase

approach in the development of the revisions. This comment form addresses Phase ~~1~~I of the project. A description of the scope, and criteria and rationale for inclusion in Phase ~~1~~I follow.

Comment [JDB3]: Use SAR description

Summary of Phase I Revisions

Formatted: Not Highlight

Phase I includes necessary modifications to CIP 002 – CIP 009 in order to comply with near term specific directives included in FERC Order 706. Certain modifications directed in Order 706, such as the removal of the term "reasonable business judgment," must be completed before compliance audits begin in 2009. In addition, each of the CIP standards has been modified to ensure that it conforms to the latest version of the ERO Rules of Procedure including applicability to Regional Entities. Additional directives included in FERC Order 706, which apply to specific standards are also addressed in Phase I modifications. More contentious issues listed in the Background Section above will be addressed in a later SDT phase.

Comment [JL4]: I believe this is appropriate, as this document accompanies the output of pase 1.

Phase I of the SDT proposes the following modifications to CIP 002 - CIP 009:

Formatted: Not Highlight

~~**Summary of Phase I Revisions**~~

A. For EACH CIP 002 – 009 Standard the following modifications apply:

Comment [t5]: SE: Each of these changes is based on the published red lined versions discussed at the meeting in Maryland. These changes must be reviewed to assure they are in accordance with the final version that will be sent to NERC for posting.

- As directed in Order 706
  - Purpose Section : Removed 'reasonable business judgment"
- To comply with ERO Rules of Procedure
  - Applicability Section : Added Regional Entity, in addition to Regional Reliability Organization
- Versioning
  - Phase I modifications to the existing version will be reflected as CIP 002-009 – 2
- Dates
  - New version dates will reflect Effective Date of new version and Date Adopted by Board of Trustees

Formatted: Bullets and Numbering

B. In addition to the changes noted above, the following modifications apply to specific CIP Standards:

- **CIP 002 Modifications**
  - As directed in Order 706
    - R4 Annual Approvals: Senior manager shall annually review and approve the risk-based assessment methodology in addition to the list of Critical Assets and Critical Cyber Assets

Formatted: Bullets and Numbering

- **CIP 003 Modifications**
  - As directed in Order 706
    - R2 Leadership: Require the designation of a single manager, who has direct and comprehensive responsibility and accountability for implementation and ongoing compliance with the CIP Reliability Standards. Eliminate the need for business phone and business address designation.

Formatted: Bullets and Numbering

- **CIP 004 Modifications**
  - As directed in Order 706

Formatted: Bullets and Numbering

- R2.1 Training: Personnel having access to Critical Cyber Assets must be trained prior to their being granted such access, rather than allowing 90 days to accomplish the training. Added reference to CIP 003 R1.1. for emergency provisions.
- R3 Personnel Risk Assessment: Personnel risk assessment shall be conducted prior to granting personnel access to Critical Cyber Assets rather than within 30 days of such access. Added reference to CIP 003 R1.1. for emergency provisions.

Comment [t6]: SE: Question: do we want to just list what the requirement was changed to? OR, do we want to indicate both what it is changed to and what it used to be?

- **CIP 005 Modifications**
  - Clarification to assure that requirement must be implemented
    - R2.3 Electronic Access Controls: Responsible Entities must both maintain and implement a procedure for securing dial up access, instead of just maintaining the procedure as stated in the prior CIP version.

Formatted: Bullets and Numbering

- **CIP 006 Modifications**
  - Clarifications to assure that solutions related to requirements must be implemented
    - R1 Physical Security Plan: Responsible entities must create, maintain and implement a physical security plan rather than simply creating and maintaining the plan as stated in prior CIP version.
    - R1.2 Measures to control access to entry points must be implemented as well as identified as stated in the prior CIP version.
    - R1.6 Escorted Access: Added the word implementation to assure that escorted access procedures are both created and implemented.
    - R1.7 Updates to the Physical Security Plan: Added the word implementation to assure that changes to the physical plan occur within thirty calendar days of the implementation of the perimeter change.

Formatted: Bullets and Numbering

Comment [t7]: SE: These were the tweaks related to 'implementation' which were discussed at the meeting. Double check to assure these match the final modifications.

- **CIP 007 Systems Security Management Modifications**
  - As directed in Order 706
    - R2.3 Ports and Services: Removal of the term "or an acceptance of risk."
    - R3.2 Security Patch Management: Removal of the term "or an acceptance of risk."
    - R4.1 Malicious Software Prevention: Removal of the term "or an acceptance of risk."
    - R9 Documentation Review and Maintenance: Modified to assure that changes to systems or controls are documented within thirty calendar days rather than within ninety days as prescribed in the prior CIP version.
  - Clarifications to assure that solutions related to requirements must be implemented
    - R7 Disposal and Redeployment: Added the word "implement" in R7 to assure that formal methods are both established and implemented.
    -

Formatted: Bullets and Numbering

- **CIP 008 Incident Response & Reporting Modifications**
  - As directed in Order 706
    - R1.6 Testing of the Incident Response Plan: Added language to clarify that testing need not require a responsible entity to remove any systems from service.
    - R1.4 Updating the Cyber security Incident Response Plan: Require updates within thirty calendar day so f any changes instead of within 90 days as required in the prior CIP version.
  - Clarifications to assure that solutions related to requirements must be implemented
    - R1 Incident Response Plan: Added the word "implement".

Formatted: Bullets and Numbering

CIP 009 Recovery Plan Modifications

- As directed in Order 706
  - R3 Change Control: Require updates to be communicated within thirty calendar days of the change, instead of within 90 days as required in the prior CIP version.

Formatted: Bullets and Numbering

.

Implementation Plan Changes

- New Critical Assets
  - New Implementation Plan is proposed for newly identified Critical Assets
- Changes in CIP Requirements as a result of Phase I SDT work
  - Modification to CIP Implementation Plan is proposed to address changes noted in Phase I of SDT work

Formatted: Bullets and Numbering

~~To the last point, the SDT adopted the multi-phase approach at its inaugural meeting at NIST headquarters in Gaithersburg, MD. At this meeting, the SDT set out to complete in Phase I, the date certain item to eliminate the phrase "reasonable business judgment" and any other scope items that could be completed within the same Phase I timeframe.~~

~~PUT DESCRIPTIONS OF PHASE I MODIFICATIONS TO CIP-002 TO CIP-009 HERE…~~
~~[list each CIP; summarize changes and rationale]~~

Comment Form

The following questions will assist the SDT in finalizing the Phase I work for CIP-002-2 through CIP-009-2 concerning changes to requirements. ~~For questions where you agree with the SDT, please state that you agree with any explanatory comments and if available, please provide supporting documentation.~~Please indicate whether or not you agree with the change. If you disagree with the SDT, please explain why you disagree and provide ~~data to support your position~~suggestions for improvement. The SDT would appreciate responses to as many of these questions as you can answer.

You do not have to answer all questions. Enter All Comments in Simple Text Format.

Insert a "check" mark in the appropriate boxes by double-clicking the gray areas.

1. The CSO706 SDT ~~modified~~added management approval of the risk-based assessment methodology[1] in CIP-002-1 ~~to remove the phrase "reasonable business judgment", added the Regional Entity as subject to the Standard and _____~~.Requirement R4.

   Do you agree with the change? If not, please explain and ~~explain~~provide specific suggestions for improvement.

   ☐ Yes

   ☐ No

   Comments:

2. The CSO706 SDT ~~modified~~ clarified the intent of the CIP-003-1 Requirement R2 on Leadership ~~to remove the phrase "reasonable business judgment", added the Regional Entity as subject to the Standard and _____~~.that a senior manager be assigned with the overall responsibility and authority for cyber security matters[2]. Requirement R2.3 was added to address senior manager delegation of authority for specific actions to a named delegate. The original R2.3 was renumbered to R2.4.

   Do you agree with the changes? If not, please explain and provide specific suggestions for improvement.

   ☐ Yes

   ☐ No

   Comments:

3. The CSO706 SDT modified CIP-004-1 Requirements R1 and R2 to ~~remove the phrase "reasonable business judgment", added the Regional Entity as subject to the Standard~~

[1] FERC Order 706, paragraph 236

[2] FERC Order 706, paragraph 381

Formatted: Numbered + Level: 1 + Numbering Style: 1, 2, 3, … + Start at: 1 + Alignment: Left + Aligned at: 0" + Tab after: 0.3" + Indent at: 0.3", Don't adjust space between Latin and Asian text

Formatted: Numbered + Level: 1 + Numbering Style: 1, 2, 3, … + Start at: 1 + Alignment: Left + Aligned at: 0" + Tab after: 0.3" + Indent at: 0.3", Don't adjust space between Latin and Asian text

Formatted: Numbered + Level: 1 + Numbering Style: 1, 2, 3, … + Start at: 1 + Alignment: Left + Aligned at: 0" + Tab after: 0.3" + Indent at: 0.3", Don't adjust space between Latin and Asian text

~~and~~ ~~_____~~.include the requirement to implement the Responsible Entity's security awareness and annual cyber security training programs. The requirements to train personnel[3] and complete a personnel risk assessment[4] prior to granting access to Critical Cyber Assets replaced the "within ninety days" language in Requirement R2.1 and R3. For emergency situations, a reference to CIP-003-2 R1.1 was added to Requirements R2 and R3.

Do you agree with the changes? If not, please explain and provide specific suggestions for improvement.

☐ Yes

☐ No

~~Recommended periodicity and reasoning~~Comments:

4. The CSO706 SDT added "implement" to ~~modified~~ CIP-005-1 Requirement R2.3 to clarify that the procedure for securing dial-up access to the Electronic Security Perimeter must be both maintained and implemented. ~~to remove the phrase "reasonable business judgment", added the Regional Entity as subject to the Standard and _____~~.

Formatted: Numbered + Level: 1 + Numbering Style: 1, 2, 3, … + Start at: 1 + Alignment: Left + Aligned at: 0" + Tab after: 0.3" + Indent at: 0.3"

Do you agree with the change? If not, please explain and provide specific suggestions for improvement.

☐ Yes

☐ No

Comments:

5. The CSO706 SDT modified~~modified~~ CIP-006-1 Requirement R1 to ~~remove the phrase "reasonable business judgment", added the Regional Entity as subject to the Standard and _____~~.clarify the requirement to implement the Responsible Entity's physical security plan, monitoring of unauthorized personnel by escorts within the Physical Security Perimeter and update the plan within thirty days of the completion of any changes.

Formatted: Numbered + Level: 1 + Numbering Style: 1, 2, 3, … + Start at: 1 + Alignment: Left + Aligned at: 0" + Tab after: 0.3" + Indent at: 0.3"

Do you agree with the change? If not, please explain and provide specific suggestions for improvement.

☐ Yes

☐ No

Comments:

[3] FERC Order 706, paragraph 431

[4] FERC Order 706, paragraph 443

6. The CSO706 SDT added "implement" to~~modified~~ CIP-007-1 Requirements R2, R3 and R7 to ~~remove the phrase "reasonable business judgment", added the Regional Entity as subject to the Standard and _____~~.clarify that processes and procedures must be implemented as well as documented. Requirement R4.1 was modified to remove "acceptance of risk" language[5]. The SDT revised the timeframe for documenting changes to systems or controls to thirty days in Requirement R9.

   Do you agree with the changes? If not, please explain and provide specific suggestions for improvement.

   ☐ Yes

   ☐ No

   Comments:

7. The CSO706 SDT modified CIP-008-1 Requirement R1 to ~~remove the phrase "reasonable business judgment", added the Regional Entity as subject to the Standard and _____~~.clarify the requirement to implement the plan in response to cyber security incidents, update the plan within thirty days of any changes, and clarify that tests of the plan do not require removing components or systems during the test.

   Do you agree with the changes? If not, please explain and provide specific suggestions for improvement.

   ☐ Yes: ———

   ☐ No

   ~~, instead use this approach~~Comments:

8. The CSO706 SDT revised the timeframe to thirty days for communicating updates of recovery plans to personnel responsible for activating or implementing the plan in~~modified~~ CIP-009-1 Requirement R3~~to remove the phrase "reasonable business judgment", added the Regional Entity as subject to the Standard and _____~~.

   Do you agree with the change? If not, please explain and provide specific suggestions for improvement.

   ☐ Yes

   ☐ No

   Comments: _____

9. The CSO706 SDT revised the CIP implementation plan to address new Critical Assets.

[5] FERC Order 706, paragraph 622

Formatted: Numbered + Level: 1 + Numbering Style: 1, 2, 3, … + Start at: 1 + Alignment: Left + Aligned at: 0" + Tab after: 0.3" + Indent at: 0.3", Don't adjust space between Latin and Asian text

Formatted: Numbered + Level: 1 + Numbering Style: 1, 2, 3, … + Start at: 1 + Alignment: Left + Aligned at: 0" + Tab after: 0.3" + Indent at: 0.3"

Formatted: Numbered + Level: 1 + Numbering Style: 1, 2, 3, … + Start at: 1 + Alignment: Left + Aligned at: 0" + Tab after: 0.3" + Indent at: 0.3"

Formatted: Indent: Left: 0.5", First line: 0"

Formatted: Bullets and Numbering

Do you agree with the change? If not, please explain and provide specific suggestions for improvement.

☐ Yes

☐ No

Comments:

~~9.~~10. Do you have any other Phase I improvements to these standards that have not been addressed? If yes, please explain.

☐ Yes

☐ No

Comments:

Formatted: Numbered + Level: 1 + Numbering Style: 1, 2, 3, … + Start at: 1 + Alignment: Left + Aligned at: 0" + Tab after: 0.3" + Indent at: 0.3"

Formatted: Bullets and Numbering

Meeting Type	Dates	Agenda
~~Webex/Conf call~~	~~Oct 15~~	~~Small group review~~
In person at SMUD (Sacramento, Kevin Sherlin)	October 21-22 Full/Full	
Webex/Conf call for FULL Team	October 29, 2008 1PM to 5PM Eastern Please send completed documents to Harry by COB Monday October 27, 2008.	1. Implementation plan (new CCA) sub team (minus Dave Norton) takes commentary from full team and revises the categories for approval by full team. 2. Comment Form final for approval by full team. 3. Implementation plan (CIP version 2) sub team final for approval by full team. MAPPING document? 4. CIP-004 and CIP-006 final for approval by full team. Submit package to MEL for review and comment.

WebEx/Conference call	November 3, 2008	Develop concept document - TFE sub team (Scott Mix, Keith Stouffer, John Varnell, Jerry Freese, Tom Hofstetter, Compliance staffer). Deliver to full team by Nov. 7 or 10.
WebEx/Conference call	November 5, 2008 - NERC staff feedback	Review and conform drafts per feedback from MEL
In person at Little Rock, Arkansas (confirmed with AECC)	Nov 12-14 Half/Full/Half	1. Finalize Phase I documents. 2. Review and finalize "technical feasibility exception" proposal. 3. One pager "big picture" straw proposal and enumerate some guiding principles.
WebEx/conf call	Nov 18 Webex/Conf call	
In person meeting at FERC offices	December 4-5 Full/Full	
In person at APS (Phoenix, AZ)	January 7-9 Half/Full/Half	Consider Comments to Phase I

Meeting Type	Dates	Agenda
~~Webex/Conf call~~	~~Oct 15~~	~~Small group review~~
In person at SMUD (Sacramento, Kevin Sherlin)	October 21-22 Full/Full	
Webex/Conf call for FULL Team	October 29, 2008 1PM to 5PM Eastern Please send completed documents to Harry by COB Monday October 27, 2008.	1. Implementation plan (new CCA) sub team (minus Dave Norton) takes commentary from full team and revises the categories for approval by full team. 2. Comment Form final for approval by full team. 3. Implementation plan (CIP version 2) sub team final for approval by full team. MAPPING document? 4. CIP-004 and CIP-006 final for approval by full team. Submit package to MEL for review and comment.

WebEx/Conference call	November 3, 2008	Develop concept document - TFE sub team (Scott Mix, Keith Stouffer, John Varnell, Jerry Freese, Tom Hofstetter, Compliance staffer). Deliver to full team by Nov. 7 or 10.
WebEx/Conference call	November 5, 2008 - NERC staff feedback	Review and conform drafts per feedback from MEL
In person at Little Rock, Arkansas (confirmed with AECC)	Nov 12-14 Half/Full/Half	1. Finalize Phase I documents. 2. Review and finalize "technical feasibility exception" proposal. 3. One pager "big picture" straw proposal and enumerate some guiding principles.
WebEx/conf call	Nov 18 Webex/Conf call	
In person meeting at FERC offices	December 4-5 Full/Full	
In person at APS (Phoenix, AZ)	January 7-9 Half/Full/Half	Consider Comments to Phase I

Implementation Plan for Cyber Security Standards
CIP-002-2 through CIP-009-2

Effective Date[i]

The proposed effective date for these standards is the greater of 1) 180 days following approval by the Federal Energy Regulatory Commission, or 2) the number of days following approval by the Federal Energy Regulatory Commission before a Responsible Entity must become Compliant with a requirement according to the associated Compliance Schedule.

Comment [p1]: This section captures the intent of the version 2 implementation schedule. See Implementation Schedule notes at the bottom of this document.

Comment [p2]: Consider Canadian regulatory bodies?

Summary of Modifications

A red line version of each of these standards showing the proposed changes has been posted at the following site:

[Insert URL for Red-Line version]

Modified Part	Modification Description
Purpose statement for all Standards	Removes the allowance of reasonable business judgment for Responsible Entities when applying Standards CIP-002 through CIP-009.
Applicability section for all Standards	Includes Regional Entities in the definition of Responsible Entity.
CIP-002-2 R4	Requires the senior manager or delegate(s) to approve the risk-based assessment methodology in addition to the Critical Asset and Critical Cyber Asset lists.
CIP-003-2 R2	Adds the requirement for the senior manager to have both responsibility and authority for leading and managing the implementation of, and adherence to, the Cyber Security Standards.
CIP-003-2 R2.1	Removes the requirement to identify the senior manager's business phone and address.
CIP-003-2 R2.3	Explicitly permits the assigned senior manager to delegate authority in writing for specified actions, where allowed, throughout the Cyber Security Standards.
CIP-004-2 R1	Explicitly requires the implementation of the documented security awareness program and clarifies that authorized cyber or authorized unescorted physical access is to Critical Cyber Assets.
CIP-004-2 R2	Explicitly requires the implementation of the documented cyber security training program.
CIP-004-2 R2.1	Requires the training of personnel prior to being granted access to Critical Cyber Assets.
CIP-004-2 R3	Requires Responsible Entities to perform a personnel risk assessment prior to such personnel being granted access to Critical Cyber Assets.
CIP-005-2 R1.5	Clarifies the scope of this requirement to include Cyber Assets used in either access control or monitoring of the Electronic Security Perimeter.
CIP-005-2 R2.3	Explicitly requires the implementation of the procedure to secure dial-up access to the Electronic Security Perimeter.
CIP-006-2 R1	Explicitly requires the implementation of a physical security plan. Modifications also include changing "a" senior manager to "the" senior manager.
CIP-006-2	Explicitly requires the implementation of measures to control entry to the Physical

Comment [p3]: We chose not to mention the FERC mandate here since the Implementation Plan is part of the standards. However, we believe the FERC mandate should appear in the comment form.

Comment [p4]: Need to update the FAQ to indicate the reasoning behind some of these changes.

Comment [p5]: MODIFICATION TO REDLINE – Change "a" to "the".

Comment [p6]: MODIFICATION TO REDLINE - Consider changing delegate to plural.

Comment [p7]: Pending review of SDT sub-team

R1.2	Security Perimeter.
CIP-006-2 R1.4	Explicitly requires the implementation of procedures for the appropriate use of physical access controls.
CIP-006-2 R1.6	Explicitly requires the implementation of procedures for escorted access to the Physical Security Perimeter.
CIP-006-2 R1.7	Shortens the timeframe to update the physical security plan from ninety to thirty calendar days upon implementation of a security system redesign or reconfiguration.
CIP-006-2 R1.8	Clarifies the scope of this requirement to include Cyber Assets used in either access control or monitoring of the Physical Security Perimeter.
CIP-007-2 R2	Explicitly requires the implementation of the process to ensure only required ports and services are enabled.
CIP-007-2 R3	Explicitly requires the implementation of a security patch management program.
CIP-007-2 R4.1	Removes the Responsible Entity's option to accept the risk of not implementing malware prevention tools without compensating measure(s) to mitigate risk exposure.
CIP-007-2 R7	Explicitly requires the implementation of Cyber Asset disposal and redeployment procedures.
CIP-007-2 R9	Shortens the timeframe to update CIP-007 documentation in response to a system or control change from ninety to thirty calendar days and further clarifies this timeframe begins after such changes are completed.
CIP-008-2 R1	Explicitly requires the implementation of a Cyber Security Incident response plan.
CIP-008-2 R1.4	Shortens the timeframe to update the Cyber Security Incident response plan from ninety to thirty calendar days.
CIP-008-2 R1.6	Clarifies the testing of Cyber Security Incident response plans does not require the removal of components or systems from service.
CIP-009-2 R3	Shortens the timeframe for communicating updates to Critical Cyber Asset recovery plans from within ninety to thirty calendar days of the change being completed.

Comment [p8]: MODIFICATIONS TO REDLINE – Capitalize physical security perimeter (R1.6 & 1.7)

Comment [p9]: Pending review of SDT sub-team

Comment [p10]: REDLINE NOTE – confusion around the term Cyber Asset and non-critical Cyber Asset globally.

Comment [p11]: REDLINE NOTE - Check for consistency of implementation after changes (e.g. CIP-006 R1.7, CIP-008 R1.4, CIP-009 R3)

Comment [p12]: MODIFICATION TO REDLINE – ensure consistency when capitalizing "Incident" and "Response".

Comment [p13]: REDLINE NOTE – This requirement does not actually require a test to be performed.

[i] **Implementation Schedule Issues**

- Are we 1) modifying, 2) referencing, or 3) completely developing a new Implementation Schedule in revision 2?
- There are issues with the Auditably Compliant phase. If an entity is required to become compliant with phase 2 180 days after approval, they may not have a year's worth of documentation.
- For those in the Substantially Compliant phase upon approval, should we allow additional time before they are required to become Compliant?
- Do the complications of the implementation schedule indicate the need to push all but the "reasonable business judgment" modifications out to Phase 2? Furthermore, is there some phrase we can substitute for "reasonable business judgment" to satisfy FERC in Phase 1?

Implementation Plan Amendment
for Cyber Security Standards
CIP-003 through CIP-009

Implementation Plan for Newly Identified Critical Cyber Assets

This Implementation Plan identifies the schedule for becoming compliant with the requirements of NERC Standards CIP-003 through CIP-009 (current version) for assets determined to be Critical Cyber Assets once the "Compliant" milestone date listed in the existing Implementation Plan has passed.

This Implementation Plan specifies only a Compliant milestone. The Compliant milestone is expressed in this Implementation Plan table as the number of months following the designation of the newly identified asset as a Critical Cyber Asset, following the requirements of NERC Standard CIP-002.

For some requirements, the Responsible Entity is expected to be Compliant immediately upon the designation of the newly identified Critical Cyber Asset. These instances are annotated as "0" herein. For other requirements, the designation of a newly identified Critical Cyber Asset has no bearing on the Compliant date. These are annotated as "—" (a dash).

In all cases where a milestone for compliance is specified (i.e., not annotated as "—"), the Responsible Entity is expected to have all audit records required to demonstrate compliance (i.e., to be Auditably Compliant) one year following the milestone listed in this Implementation Plan. Where the milestone assumes prior compliance (i.e., is annotated as "—"), the Responsible Entity is expected to have all documentation and records showing compliance (i.e., Auditably Compliant) based on other previously defined Implementation Plan milestones.

There are no Implementation Plan milestones specified herein for compliance with NERC Standard CIP-002. All Responsible Entities are required to be compliant with NERC Standard CIP-002 based on the existing Implementation Plan.

Implementation Schedule

There are three milestone categories described in this Implementation Plan. They are briefly:

1. First identified Critical Cyber Asset
2. Reclassification or change-in-status of an ~~E~~existing ~~Critical~~ Cyber Asset to be a Critical Cyber Asset associated with a newly identified Critical Asset~~at a newly identified Critical Asset~~
3. Associated with an existing Critical Asset, any r~~Modification~~ eplacement, reconfiguration, upgrade or addition of a relevant Cyber Asset~~at an existing Critical Asset~~

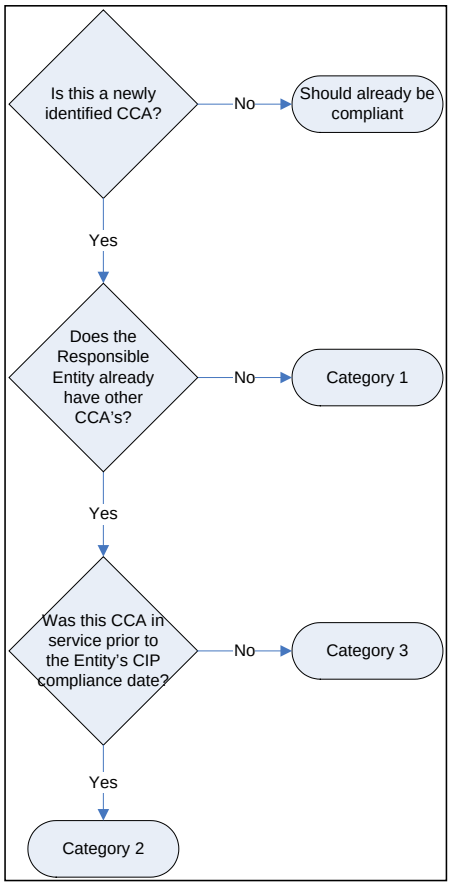


Figure 1

Figure 1 shows an overall process flow for determining which milestone category a Critical Cyber Asset identification scenario must follow. Following the figure is a more detailed description of each category.

The individual categories are distinguished as follows:

1. Category 1: A Responsible Entity that previously has undergone the CIP-002 Critical Asset identification process for at least one annual review and approval period without ever having identified any Critical Cyber Assets at Critical Assets,

but has now identified one or more Critical Asset(s) with associated Critical Cyber Assets. The Compliant milestone specified for this Category shall be the same as Table 4 of the original Implementation Plan for Standards CIP-003 through CIP-009. As such, it is presumed that the Responsible Entity has no previously established cyber security program in force. Table 4 of the original CIP Implementation Plan also shall apply in the event of a Responsible Entity business and system merger or acquisition where previously no Critical Assets had been identified by any of the Entities involved.

2. Category 2: A Responsible Entity has an established CIP Compliance program as required by an existing Implementation Schedule, and now has further identified one or more additional existing Critical Assets with existing associated Critical Cyber Assets. The existing Critical Cyber Assets may remain in service while the relevant requirements of the CIP Standards are implemented. Since the Responsible Entity had previously identified Critical Cyber Assets and had implemented the CIP Standards appropriately for them, it needs only to implement the CIP standards for the newly identified Critical Cyber Asset(s).

   This category applies only when new Critical Cyber Assets or applicable other Cyber Assets are *identified*, not when they are added or modified through construction, upgrade or replacement.

   In the case of business and system merger or asset acquisition, if any of the Responsible Entities involved had previously identified Critical Assets with associated Critical Cyber Assets (and, as appropriate, relevant other Cyber Assets), implementation of the CIP Standards for newly identified Critical Assets and Critical Cyber Assets must be completed per Compliant milestones established herein under Category 2.

   In the case of a merger where all parties already have previously identified Critical Cyber Assets and have existing but different CIP Compliance programs in place, the merged company has one calendar year from the effective date of the merger or acquisition to continue to operate the separate programs and to determine how to create a combined uniform CIP Compliance program. At the conclusion of the one calendar year period, the Category 2 milestones will be used to consolidate the separate CIP Compliance programs into a single uniform CIP Compliance program.

3. Category 3: A Responsible Entity has an established CIP Compliance program as required by an existing Implementation Schedule and implements a new or replacement Critical Cyber Asset associated with a previously identified or newly constructed Critical Asset. This Category shall apply for the following scenarios:

   a. "Greenfield" construction of an asset that will be declared a Critical Asset upon its commissioning or activation (e.g., based on planning or impact studies).

b. Replacement or upgrade of an existing Critical Cyber Asset (and/or other Cyber Asset within an Electronic Security perimeter) associated with a previously identified Critical Asset.
c. Addition of:
    i. a Critical Cyber Asset, or,
    ii. an other Cyber Asset within an established Electronic Security Perimeter.

This Category applies in any case where a Critical Cyber Asset or applicable other Cyber Assets is being added to or modified at an existing or new Critical Asset where that Entity has an established CIP Compliance Program as required by an existing Implementation Schedule.

Category 3 Compliant milestones shall apply for any of the above scenarios where relevant in the event of business and system merger and/or acquisition.

Note that there are no milestones specified for a Responsible Entity that has newly designated a Critical Asset, but no newly designated Critical Cyber Assets. This is because no action is required by the Responsible Entity upon designation of a Critical Asset without associated Critical Cyber Assets. Only upon designation of Critical Cyber Assets does a Responsible Entity need to become compliant with these standards.

Table 1: Implementation milestones for Newly Identified Critical Cyber Assets

Comment [th1]: Consider adding column to give idea what the requirement pertains to...

CIP Standard Requirement	Milestone Category 1	Milestone Category 2	Milestone Category 3
Standard CIP-002-2 – Critical Cyber Asset Identification			
R1	N/A	N/A	N/A
R2	N/A	N/A	N/A
R3	N/A	N/A	N/A
R4	N/A	N/A	N/A
Standard CIP-003-2 – Security Management Controls			
R1	24	—	—
R2	1	—	—
R3	24	—	—
R4	24	—	—
R5	24	—	—
R6	24	—	—
Standard CIP-004-2 – Personnel and Training			
R1	24	—	—
R2	24	2	2
R3	24	6	6
R4	24	6	6

CIP Standard Requirement	Milestone Category 1	Milestone Category 2	Milestone Category 3
Standard CIP-005-2 – Electronic Security Perimeter			
R1	24	12	—
R2	24	12	—
R3	24	12	—
R4	24	12	—
R5	24	12	—
Standard CIP-006-2 – Physical Security			
R1	24	12	—
R2	24	12	—
R3	24	12	—
R4	24	12	—
R5	24	12	—
R6	24	12	—
Standard CIP-007-2 – Systems Security Management			
R1	24	12	3
R2	24	12	3
R3	24	12	0
R4	24	12	3 or 0?
R5	24	12	3
R6	24	12	3
R7	24	12	0
R8	24	12	3
R9	24	12	0
Standard CIP-008-2 – Incident Reporting and Response Planning			
R1	24	3	3
R2	24	0	0
Standard CIP-009-2 – Recovery Plans for Critical Cyber Assets			
R1	24	3	3
R2	24	0	0
R3	24	0	0
R4	24	2	~~2~~3
R5	24	2	~~2~~3

Strawman to address technical feasibility

The Responsible Entity may invoke a technical feasibility exception to a Requirement based on the Responsible Entity's determination that any of the following conditions apply:

- The Requirement poses a risk to the reliability of the Bulk-Power System
- The Requirement creates a significant adverse operational and/or safety impact
- The Requirement specifies mechanisms or functions that are not technically possible for a Cyber Asset to support

The Responsible Entity shall document all technical feasibility exceptions in an Exception Plan provided to the ERO and Regional Entity containing:

- A justification why the technical feasibility exception is necessary
- Compensating controls or mitigation steps to meet the intent of and provide a comparable level of security to the Requirement
- A plan of action, milestones, and schedule for implementing the compensating controls or mitigation steps

The Exception Plan must be approved annually by the Responsibility Entity senior manager.

The Exception Plan must be approved annually by the Regional Entity or the ERO if there is no applicable Regional Entity.

The ERO must annually audit compliance with the Exception Plan and provide FERC with an annual high-level, wide-area analysis regarding the effects of all exceptions on the reliability of the Bulk-Power System.

Possible placement of the language is within the A. Introduction section of each standard – possibly a new 5. Effective Date would then be 6.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Draft Meeting Summary

Cyber Security Order 706 SDT — Project 2008-06

October 21, 2008 | 8 a.m.–5 p.m.
October 22, 2008 | 8 a.m.–noon
Sacramento Municipal Utility District
Sacramento, CA

MEETING SUMMARY CONTENTS

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Appendices

Meeting Facilitation and Draft Report By: Stuart Langton & Hal Beardall
FCRC Consensus Solutions — Florida Conflict Resolution Consortium**, Florida State University**
Thanks to Team members Sharon Edwards and Kevin Perry, and NERC Staff Harry Tom for their meeting notes.
http://www.nerc.com/filez/standards/Project_2008-06_Cyber_Security.html

EXECUTIVE SUMMARY

A. Introductions, Agenda Review, and Welcoming Remarks

The Chair, and Vice Chair welcomed the members and reviewed with the team and participants the proposed meeting agenda *(See appendix #1*). NERC staff Harry Tom conducted a roll call of members and participants in the room and on the conference call *(See appendix #2*). They then and thanked Kevin Sherlin for hosting the meeting at the Sacramento Municipal Utility District offices.

B. Review of NERC Antitrust Compliance Guidelines

Harry Tom reviewed with the team the need to comply with NERC's Antitrust Guidelines (See, Appendix #3). He urged the team and other participants in the process to carefully review the guidelines as they would cover all participants and observers.

C. Acceptance of Organizational Meeting Minutes

Stu Langton and Hal Beardall, with the FCRC Consensus Solutions facilitation team, reviewed the minutes from the first meeting noting corrections. The group agreed to accept the minutes as they were distributed to the group with the minor corrections noted; however the minutes will be open to additions as necessary.

D. Planning Challenges, Purpose Statement, and Consensus Guidelines

Stu Langton provided an overview of organizational issues and planning challenges the drafting team will need to keep in mind such as organization, process, issue identification, progression strategy and schedule.

Mr. Langton suggested some key principles for the group such as the capacity to tolerate ambiguity and patience. This will be an iterative process that will build on previous discussions while flexible enough for the group to revisit earlier issues if needed as a result of subsequent discussions.

Following the challenges and principles, Mr. Langton offered for the group's consideration the following draft purpose statement as a starting point for review and discussion:

> "The overall purpose of the Cyber Security of Order 706 SDT is to work together to build consensus on a package of recommended draft cyber security standards and implementation plan that is responsive to and consistent with the scope of the SAR and the FERC Order 706.
>
> The team's products will seek *to protect the critical cyber assets (including hardware, software, data, and communications networks) essential to the reliable operations of the bulk power system* and will be submitted for consideration by the registered ballot body. *(Italics from the SAR "purpose" statement)"*

Following discussion and suggestions for improvement, the group asked the facilitators work with the chair and staff to reframe the scope based on this discussion and bring a new draft back to the full group for review next time

Mr. Langton provided an overview of how consensus could be defined and used by the drafting team *(See Appendix #6).* He noted that consensus could be understood as having three meanings in a group process: it is an attitude, an outcome or decision rule, and a structured problem solving process. He suggested that the team has some flexibility to define what a 'consensus' decision should mean for the team's process. He suggested that the team review this again at the next meeting with an eye towards adopting a procedure going forward.

Mr. Beardall reviewed a set of ground rules *(See, Appendix #6)* for the meeting including additional items added at the first meeting for phone protocols.

E. Reviewing Sub-team Draft of NERC CIP Standard

Mr. Langton reviewed the drafting sub team assignments (*Appendix #4*). Sub team leader Jackie Collett described the revisions offered for consideration by the CIP 004 sub team. *(See appendix #5 for link to red-line/underline revisions)*

Sub team changes included:

- Improved the wording
- Took out reasonable business judgment
- Training to be completed prior to granting access
- Personnel risk assessment to be completed prior to granting access
- Added provision that emergency provisions should be handled in accordance with CIP 003.R.1.1.

Following team comments regarding proposed changes to CIP 004 the group voted on the following three options for references to emergencies concerning Training and Background Screening Pre-Requisites:

A. A personnel risk assessment shall be conducted pursuant to the program prior to such personnel being granted such access. (No reference to emergency provisions.)
B. A personnel risk assessment shall be conducted pursuant to the program prior to such personnel being granted such access except in specified circumstances such as an emergency. (Note: This option includes language included in FERC 706 language specifically.)
C. A personnel risk assessment shall be conducted pursuant to the program prior to such personnel being granted such access except in specified circumstances such as an emergency. Emergency provisions should be handled in accordance with CIP 003.R1.1. (Note: This option includes reference back to CIP 003 Policy within CIP 004 R.2&3 to deal with Emergency situations.)

Vote on accepting the proposed CIP 004 language

Preferences	Option A Above	Option B Above	Option C Above
Voting Members	0	22	2

The facilitators suggested an initial acceptability rating (using the 4-3-2-1 scale) of the preferred option to guide additional discussion and refinement.

Acceptance of CIP 004 Proposed Changes	4	3	2	1
Voting Members and Observers	16	8	2	0

Following team discussion and suggestions the group came to the following conclusions concerning CIP 004:

- CIP 004 was accepted with the changes to require the Cyber Security training and background screening prior to access and with the inclusion of language concerning emergency provisions in accordance with FERC Order 706 (Option B above).
- CIP 003 Policy language will be reviewed/modified by a work group in Phase II, not Phase I.

F. Technical Feasibility Exception proposal

Michael Assante, NERC Chief Security Officer, addressed the group by phone and asked the team to consider addressing the technical feasibility exception as a priority and possibly as part of Phase I. Mr. Assante pointed to the request from FERC to address this issue and reviewed several of the related issues to be considered.

Following team discussion of the request the Chair offered a motion to table the issue of the Technical Feasibility Exception until after the team agenda is completed. Members voted unanimously in favor of the motion with one abstention.

G. Reviewing Sub team draft of NERC CIP Standard 006

Kevin Perry, as CIP 006 sub team leader, provided an overview of the revisions offered by the sub team in CIP 006 for consideration by the full team: *(See appendix #5 for link to red-line/underline revisions)*

- Removed Reasonable Business judgment;
- Changed dates as appropriate;
- Minor wording changes which did not alter the substance of the requirement
- R1.6 added that procedures for the active monitoring of escorted persons at all times are required;
- R1.8 added that the Physical Security Plan must be reviewed annually;
- R2. (Note: The prior 1.8 requirement becomes R2 in this proposal. The original suggested language follows:

- R2. Protection of Physical Access Control Systems — Cyber Assets authorizing and logging access to the Physical Security Perimeter(s) shall:
    - R2.1. Exclusive of hardware at the Physical Security Perimeter access point such as electronic lock control mechanisms and badge readers, shall reside within an identified Physical Security Perimeter or be physically monitored 24x7 by personnel authorized unescorted access.
    - R2.2. Be afforded the protective measures specified in Standard CIP-003-1; Standard CIP-004-1 Requirement R3; Standard CIP-005-1 Requirements R2 and R3; Standard CIP-006-2 Requirements R4 and R5; Standard CIP-007-1; Standard CIP-008-1; and Standard CIP-009-1.

After an initial team discussion and questions for clarification, the team offered the following initial acceptability rating:

Acceptance of CIP 006 Proposed Changes	4	3	2	1
Voting Members	10	7	2	0

As a result of team discussion of the initial acceptability ratings the following revised CIP 006 language was proposed and tested for acceptability:

- R2. Protection of Physical Access Control systems – Cyber Assets that authorize and/or log access to the Physical Security Perimeters(s), exclusive of hardware at the Physical Security Perimeter access point such as electronic mechanisms and badge readers, shall:
- R2.1 be protected from unauthorized physical access
- R2.2 be afforded the protective measures specified in Standard CIP 003-1; Standard CIP 004-1 Requirement 3; Standard CIP 005-1 Requirements R2 and R3; standard CIP 006-2 Requirement R4 and R5; Standard CIP 007-1; standard CIP 008-1; and Standard CIP 009-1.

Acceptability Rating for CIP 006 with Revised Proposed Language:

Acceptance of CIP 006 Proposed Changes	4	3	2	1
Voting Members	15	8	0	0

H. Review of Sub Team Report on Measures & VRFs

Jerry Freese, leader for the sub team on measures, reported that their team performed a review of the measures, but based on changes prior to today's meeting; they believe there are no changes to the measures in response to proposed changes in CIP requirements.

Todd Thompson reported on behalf of the sub team reviewing VRFs that they believe no changes need to be made at this time.

I. New Implementation Plan for Changes to the Existing Requirements after Phase I Changes

Phillip Huff reported on the progress with the Implementation plan for new or changed Phase I requirements and the accompanying table including the following proposed language: *(See appendix #5 for link to red-line/underline revisions)*

- Proposed language: the original proposed effective date discussed for the modifications contained in these standards is the greater of (1) 180 days following approval by the FERC or (2) the number of days following approval by FERC before a Responsible Entity must become Compliant with a requirement according to the associated Compliance Schedule.

Based on team discussion, the sub team will make additional edits for consistency with changes made in the body of the document and make conforming changes to the standards as identified in review for creating the table.

J. COMMENT FORM REVIEW

Chairman Jeri Domingo-Brewer reviewed the sub team progress on the comment form: *(See appendix #5 for link to red-line/underline revisions)*

- Background information Section uses language out of the SAR to explain what the team had agreed to
- Summary of Phase I Revisions Section summarizes each of the changes
- Requests for Comments/Questions Section requests feedback from commenters

During discussion the team noted that CIP-004, CIP-006 and the Implementation Plan changes need to be updated in the Comment Form. The team also noted the need for education to the industry through a robust communication plan. The team accepted that this draft as a good start on the Comment form.

Members agreed to adjourn for the day.

A. Day Two — Welcome and Agenda Review

Chairperson Jeri Domingo-Brewer thanked the members of the sub teams for their hard work and reviewed the progress made by the group yesterday. She stated that today the team would:

- Review work from the remaining sub teams that were not reviewed yesterday;
- Hanging issue that the group needs to consider pertaining to CIP 006;
- Consider the issue of Technical Feasibility based on the request yesterday from Mike Assante of NERC asking the group to add this issue to the agenda for this meeting.

Stu Langton, with the FCRC Consensus Solutions facilitation team, noted the broad range of expertise members brought to the table and the need to build a common understanding of issues. He asked individuals who raise questions or concerns to also offer a proposed solution or alternatives to help the group move forward.

B. Implementation Plan Amendments

Scott Mix, sub team lead, reviewed the work that has been done so far concerning implementation plans for new assets and other situations that will be covered under CIP standards in the future. The work included a summary, a narrative explanation of each category, and a timetable. *(See appendix #5 for link to red-line/underline revisions)*

He reviewed who and when an entity would need to be compliant. He noted three milestone categories:

- **Category 1** entities starting from scratch. Existing Table 4 will be used.
  - ***The first identified Critical cyber Asset for a Registered Entity***
  - 24 months to become compliant and 36 months to become auditable compliant.
- **Category 2** is for an entity that already has a schedule and is doing things but they have identified a newly identified Critical Asset.
  - ***Reclassification or change in status of an existing Critical Asset to a Critical Cyber asset.***
  - Questions were raised concerning how the proposed tables would work when/if the CIP standards apply to nuclear. There was no answer provided at this time, as there are many variables which still need to be resolved.
  - Mergers
    - For mergers and acquisitions there is a one-year period to bring the two programs of the different companies into harmony.
    - After that one year and after completing the original CIP compliance tables, they would need to comply with the proposed category 2 timetable.

- **Category 3** deals with new assets within an existing Critical Asset. The assumption is that because you are doing something active and that you do not turn on the asset until you have completed the compliance needs within the construction.
    - ***An existing Critical Asset Replacement, reconfiguration, upgrade, or addition of a relevant cyber Asset associated with an existing Critical Asset.***
    - Construction of an asset (substation, etc.) that will be declared Critical upon activation
    - Replacement or upgrade of a Critical Asset
    - Addition of a Critical Cyber Asset at an existing Critical Asset

Scott Mix reviewed the various time thresholds which the sub team is proposing for compliance with the various situations described in the above categories.

As part of the team discussion the Vice Chair offered 6 different scenarios and how each type of scenario could be gamed by entities to gain time for compliance. The Chair asked team members to submit suggested treatments of example scenarios that summarize the categories. The suggestions should ask 3 questions and categorize appropriate events. The sub team will review suggestion during the WebEx on October 29. The Chair also asked that the team to review the comment form and provide related input to the Comment Form Sub Team.

C. CIP 006 Un-resolved Issue

An additional proposed modification to CIP 006 R1.6 language was discussed and accepted by the group as follows:

- Continuous escorted access within the Physical Security Perimeter of personnel not authorized for unescorted access.

D. CIP 003 Changes and Discussion

Proposed changes were offered to CIP 003 as follows: *(See appendix #5 for link to red-line/underline revisions)*

CIP 003 R2: Leadership — The Responsible Entity shall assign a single senior manager with overall responsibility and authority for leading and managing the entity's implementation of, and adherence to, Standards CIP-002 through CIP-009.

a. NERC audit compliance staff clarified that the Responsible Entity may be either the Corporation as a whole or may be the Registered Entity functions (GO, TO, BA, etc.).
b. **CIP 003 R3.2.** Documented exceptions to the cyber security policy must include an explanation as to why the exception is necessary and any compensating measures. ~~taken or a statement accepting risk. and/or any residual risk~~

After reviewing several suggested changes, members were asked to rate the language as revised above striking "or acceptance of risk":

The SDT's first initial rating on acceptance of the proposal:

Scale	4 — Acceptable as it	3 — Acceptable with minor concerns	2 — Not acceptable unless major concerns are addressed	1 — Not acceptable
Voting on the above by SDT	11	7	1	0

Following additional discussion, members were asked to rate the proposal again without the word "any" before "compensating measures":

The SDT's second vote on acceptance of proposed language change:

Scale	4 — Acceptable as it	3 — Acceptable with minor concerns	2 — Not acceptable unless major concerns are addressed	1 — Not acceptable
Voting on the above by SDT	12	6	4	0

Following additional discussion, members agreed to retain the word "any".

There was general agreement around the room that in CIP 007 wherever the phrase "acceptance of risk" appears, it will be removed even though each such instance where the phase appears may not have been discussed at length.

E. Proposal to Substitute "Prudent Judgment" for "Reasonable Business Judgment"

Member John Varnell requested the group consider substituting the term "prudent judgment" in place of the term "reasonable business judgment." Due to a lack of support, the group decided not to move forward with the replacement of the term "reasonable business judgment" with 'prudent judgment."

F. Proposed a Definition of Access Control System

As requested by the drafting team, Scott Mix offered a draft definition of Access Control System as follows:

> A system which provides for Authorization, Authentication, and frequently Accounting of access through either a Physical Security Perimeter or an Electric Security Perimeter. An Access Control System may be a single computer system

which performs all three functions or may be a combination of two or more computer sub systems which work together to accomplish all three functions.

i. Authentication is the process of verifying a users or object's identify.
ii. Authorization is process for granting an authenticated user or object's the authority to perform a certain operation.
iii. Accounting provides an audit trail of access, and includes logging of access by identification and time.

The SDT was asked to submit their comments for the resolution of preferences concerning the definition to Vice Chair, Kevin Perry.

G. Technical Feasibility

The Chair noted that there were two potential proposals (one from Scott Mix and one from Keith Stouffer) for addressing "technical feasibility" exception in Phase 1. She asked the team to listen to each of the proposals, consider the proposals, and decides if one of the alternatives offered could be included within the Phase I work of this team.

Scott Mix reviewed material directed in the FERC Order 706. He noted that FERC wants a framework includes mitigation steps, regular review, justification, internal approval by the senior manager, wide area approval through the ERO audit process, and cooperation with the ERO to provide the Commission with high level impact of the technical feasibility on the reliability of the grid.

Keith Stouffer of NIST provided an alternative proposal on Technical Feasibility noting it is addressed within the NIST framework for risk management and describing what a responsible entity shall document for all Technical Feasibility exceptions in an Exception Plan.

Scott Mix also reviewed the current Self Reporting Process. Based on the similarities between FERC directives and the items required by a self-reporting of non-compliance, Scott suggested that this same process be used for Technical Feasibility Exceptions.

Scott Mix reviewed similarities between the proposals:

Keith Proposal	Scott Proposal
A justification why the Technical Feasibility exception is necessary	Document non compliance to a specific requirement c. Provide explanation d. Describe reliability impact e. Describe any external or extraneous factors
Compensating controls or mitigation steps that provide a comparable level of security	
A plan of action, milestones, and schedule for	Provide mitigation schedule

implementing the compensating controls.	Provide mitigation plan
Obtain approval by the senior manager	Obtain Senior Officer signature
	Catalog and approval by Regional Entity
ERO must annually audit compliance with the Exception plan	Catalog and approval by ERO May trigger accelerated audit schedule Annual review and re-approval by Responsible Entity and ERO
ERO to provide FERC with a high level assessment of the exceptions on reliability of the Bulk Power System	ERO to develop separate annual report to FERC Analyze the combined impact of all Technical Feasibility exemptions
	Report will contain sensitive information — must be CEI protected
	Submit to FERC (US Entities)

As a result of team discussion the following proposal was suggested and tested:

Proposal Prepare a 'conceptual' document to seek stakeholder consideration and feedback that describes a Technical Feasibility Exception process that parallels existing compliance self report process.

Scale	4 — Acceptable as it	3 — Acceptable with minor concerns	2 — Not acceptable unless major concerns are addressed	1 — Not acceptable
1st Poll — Voting SDT	20	2	0	0

As a next step for it was agreed that a sub team of Tom Hofstetter, John Varnell, Keith Stouffer, Scott Mix, Jerry Freese and possibly someone from NERC compliance, would draft a document described above for presentation at the next full team meeting.

H. Assignments and Next Steps for the Next Meeting

The team and staff reviewed the deadlines for revised drafts for review at the WebEx, October 29. In addition the team reviewed the schedule of meetings and possible topics over the next three months as follows:

- WebEx, November 3 — develop concept document for Technical Feasibility. Deliver to full team by November 7 or 10.
- WebEx, November 5 — following NERC Staff feedback, review and conform drafts per feedback.
- November 12–14 — full team meeting in Little Rock, Arkansas to finalize Phase I documents as needed and review proposed roadmap
- December 4 or 5 — In person meeting at FERC Offices in Washington, DC
- January 7–9 — In person meeting at APS in Phoenix, AZ

The Chair suggested that in December the group may begin to hash out the large issues still to be addressed. The Vice Chair offered two alternatives to the "Roadmap" going forward, a multiple phase or single phase approach and proposed the SDT use an incremental approach.

The FCRC Consensus Solutions facilitation team were asked to develop a one page proposal (big picture straw proposal and guiding principles) for addressing the remaining issues following Phase I for review and discussion by the full group at the next meeting in Little Rock, Arkansas. Member discussion today has included several key principles that could guide development and discussion of remaining issues.

The team quickly reviewed the remaining list of "Parking Lot" issues identified at the first SDT 706 meeting in Gaithersburg and not already addressed today.

I. What Did and Did Not Work Well

At the conclusion of the meeting, the facilitators asked the team to offer an evaluation of the process including what worked well during the meeting and what could be improved. Members appreciated the hard work of the sub teams and staff in completing assignment in time for this meeting and the ability of the full team to work toward agreement and respect each other's opinions.

Members suggested an improved phone or speaker system was needed for those who have to call in to participate effectively and that members need to continue to offer suggestions for improvement and avoid getting bogged down in details

Members agreed to adjourn until the next meeting on November 12–14, 2008 in Little Rock, Arkansas.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Cyber Security Order 706 Standard Drafting Team
Draft Second Meeting Summary

A. INTRODUCTIONS, AGENDA REVIEW AND WELCOMING REMARKS

The Chair, and Vice Chair welcomed the members and asked NERC staff Harry Tom to conduct a roll call of members and participants in the room and on the conference call *(See appendix #2*). They then reviewed with the Team and participants the proposed meeting agenda *(See appendix #1*). They also thanked Kevin Sherlin for hosting the meeting at the Sacramento Municipal Utility District offices and for making all of the necessary logistical arrangements.

B. REVIEW OF ANTITRUST GUIDELINES

Harry Tom reviewed with the Team the need to comply with NERC's Antitrust Guidelines (See, Appendix #3). He urged the Team and other participants in the process to carefully review the guidelines as they would cover all participants and observers. He urged all to avoid behaviors or appearance that would be anti-competitive nature and also reminded the group of the sensitive nature of the information under discussion.

C. ACCEPTANCE OF ORGANIZATIONAL MEETING MINUTES

Stu Langton and Hal Beardall, with the FCRC Consensus Solutions facilitation team, reviewed the minutes from the first meeting noting several minor corrections for pagination. It was also noted that Bill Winters should be listed as representing Arizona. The group agreed to accept the minutes as they were distributed to the group with the minor corrections noted; however the minutes will be open to additions as necessary. Harry Tom explained that an announcement will go out that the minutes have been posted to the NERC website. It is the responsibility of the members to download the minutes and review them.

D. Planning challenges, Purpose statement & consensus guidelines

Stu Langton provided an overview of organizational issues including the following planning challenges the drafting team will need to keep in mind:

- Organization — a new team testing how best to work together
- Process — using a consensus building approach or process
- Issue Identification — a huge number of issues to identify and organize effectively
- Progression Strategy — important how you organize and address the issues
- Schedule — what is a realistic pace? In what order do we take up issues?

Mr. Langton suggested there are key principles the group should keep in mind to meet the challenges. He noted the group will need the capacity to tolerate ambiguity and patience since the group cannot do everything well all at once and may at times need to wait for more information. The group's progress may be circular as well as linear due to the practical and political variables that must be considered. This will be an iterative process that will build on previous discussions while flexible enough for the group to revisit earlier issues if needed as a result of subsequent discussions.

Following the challenges and principles, Mr. Langton offered for the group's consideration the following draft purpose statement as a starting point for review and discussion:

> "The overall purpose of the Cyber Security of Order 706 SDT is to work together to build consensus on a package of recommended draft cyber security standards and implementation plan that is responsive to and consistent with the scope of the SAR and the FERC Order 706.
>
> The Team's products will seek *to protect the critical cyber assets (including hardware, software, data, and communications networks) essential to the reliable operations of the bulk power system* and will be submitted for consideration by the registered ballot body. *(Italics from the SAR "purpose" statement)"*

Team Comments and Questions on the Draft Purpose Statement:

- Is this where we look at changing to "bulk power system" from "bulk electric system"? That is the language in the SAR
- "Critical Cyber Assets"? Using that term limits us to that subject. Do we want to limit ourselves to the critical assets?
- Yes, we do want to limit to those issues
- Also concerned about limiting us to those issues
- Critical Cyber Assets – definition includes assets essential to bulk electric system – can strike the word "critical" here
- In the first paragraph consider replacing with "package of recommended modifications to the cyber security standards"
- Remind group that this is part of the SDT process. The SAR sets the scope of this group to look at revising all of the CIP standards based on the order. You have to look at the standards top to bottom. Be careful, this scope can not limit you
- We need to be on the same page but the SAR already sets the scope of this group. We need to cross reference the purpose back to the scope as set by the SAR. We do not want to redefine the SAR
- Who are we serving? NERC, our companies, the public at large? Who are we doing this for? We could be serving more than one, but we are not serving the balloting body
- Expected to serve the public and the industry not the aspirations of our individual companies. Put that into the draft purpose statement.

The group agreed to the suggestion that the facilitators work with the chair and staff to reframe the scope based on this discussion and bring a new draft back to the full group for review next time

Mr. Langton provided an overview of how consensus could be defined and used by the drafting team *(See Appendix #6)*. He noted that consensus could be understood as having three meanings in a group process: it is an attitude of each of the team members, it is an outcome or decision rule for the team and it is a structured problem solving process. He suggested that the team has some

flexibility to define what a 'consensus' decision should mean for the team's process. He noted that among the ballot body, a standard requires at least a 2/3 majority of all of the industry segments to be adopted. The team may want to establish a higher supermajority for agreement (perhaps +75%) to assure 2/3 acceptance of the ballot body. He suggested that this could serve as a default standard and that the process would be designed to seek 100 percent acceptance of the team. He suggested that the team review this again at the next meeting with an eye towards adopting a procedure going forward.

Team Comments on Consensus Guidelines

- Agreement may not be at the same level to all
- These guidelines call for a 75% favorable vote but the standards committee set rules for 2/3's favorable vote – need to make consistent – quorum requires 2/3's present too
- "Dissenting opinion" not in the standards committee rules – how do we document?
- Not a problem to document as a minority report or opinion
- Even if we have consensus of this group, our companies may turn around and say "no" – we are working as a team for the public and the industry
- Know what your CEO wants
- Who in a company provides comments? Depends on the company, usually a lead person responsible for reliability who may get a corporate view, or you can get multiple comments form one company and can be contradictory
- Clarify that members on the phone are counted in any voting or polling
- Members agree to represent and consult their stakeholder interest groups – represent company, sector and self at the table
- What do you mean "seated at the table"? Staff and facilitators are in an advisory role, members are the voting members
- Only team members may participate in discussion? Everyone is invited to participate in discussion, only the votes are limited to members with a caveat to let chair limit discussion if needed
- Clarify that the polling/rating is limited to members and intended to guide discussion but comments are open to observers too
- Want a gentleman's agreement by observers to limit comments to the media
- At the discretion of the Chair or Vice Chair, the straw man polls can be extended to all participants in the meeting and not just be limited to the team members. Need to make sure to gauge the broader consensus by extending the straw poll to all at the discretion of the chair
- Cannot prevent anyone from talking to anyone else – refer to media relations at NERC as needed
- Cannot prohibit you from speaking – give factual updates on what we are doing, but must note personal opinions of the individual and not representing the group
- Group can become very comfortable with what we are doing so knowledgeable of the issues may lose tract of the broader interpretation
- Add phone participants: mute button, indicate name of speaker, use webex button to indicate you want to comment

Mr. Beardall reviewed a set of ground rules *(See, Appendix #6)* for the meeting including additional items added at the first meeting as follows:

- Additional phone protocols include using the mute button when not speaking on the phone. Do Not use the hold button.
- Say your name at the start if you are on the phone — "comment on the phone" with name to get in the queue to speak on an issue or use the feature on the WebEx that indicates you want to speak
- Ask team members on the phone to use the same WebEx feature to "raise their hands" for their acceptability ranking as needed

E. Reviewing Sub team Draft of NERC CIP Standard

Mr. Langton reviewed the drafting sub team assignments (*see Appendix 4*) and asked sub team leader Jackie Collett to describe the revisions offered for consideration by the CIP 004 sub team. *(See appendix #5 for link to red-line/underline revisions)*

Sub team changes included:

- Improved the wording
- Took out reasonable business judgment
- Training to be completed prior to granting access
- Personnel risk assessment to be completed prior to granting access
- Added provision that emergency provisions should be handled in accordance with CIP 003.R.1.1.

Team comments regarding proposed changes to CIP 004

- Some members did not like the reference back to a different standard within CIP 004.
- There were questions as to the intent of CIP 003.R1.1. and the reference to the meaning of 'emergency' as it is used in CIP 003.
- One member suggested that the Responsible Entity should have a mitigation strategy if the pre-requisites for access (Training and Personnel Risk Assessment) will not be enforced in an emergency.
- Vice Chair suggested that the modified language should be changed to: "…granted such access, subject to the emergency provisions of CIP 003-2."

Group voted on the following three options for references to emergencies concerning Training and Background Screening Pre-Requisites:

A. A personnel risk assessment shall be conducted pursuant to the program prior to such personnel being granted such access. (No reference to emergency provisions.)
B. A personnel risk assessment shall be conducted pursuant to the program prior to such personnel being granted such access except in specified circumstances such as an emergency. (Note: This option includes language included in FERC 706 language specifically.)

C. A personnel risk assessment shall be conducted pursuant to the program prior to such personnel being granted such access except in specified circumstances such as an emergency. Emergency provisions should be handled in accordance with CIP 003.R1.1. (Note: This option includes reference back to CIP 003 Policy within CIP 004 R.2&3 to deal with Emergency situations.)

Vote on accepting the proposed CIP 004 language

Preferences	Option A Above	Option B Above	Option C Above
Voting Members	0	22	2

The facilitators suggested an initial acceptability rating (using the 4-3-2-1 scale) of the preferred option to guide additional discussion and refinement.

Acceptance of CIP 004 Proposed Changes	4	3	2	1
Voting Members and Observers	16	8	2	0

Team comments and suggestions:

- 3: Footnote the language to reference CIP-003
- 3: Industry will not know what to document (addressed in CIP-003, R1.1)
- 3: Needs modifications to CIP-003 for completeness – that will be done in Phase 2
- 3: Needs to reference CIP-003 someplace, not necessarily as a footnote. Could be in the FAQ, a Guideline, a NERC definition, or as specific language in the standards themselves.

- There is a definition of "Emergency" or "BES Emergency" that can be used in CIP-003. Need to add some language regarding life and safety issues. Concern that limiting to this combination might be too limiting.
- The term "emergency" is an issue. Perhaps change the language to contingency, exigent, or exceptional.

- **Conclusions concerning CIP 004**
  - CIP 004 was accepted with the changes to require the Cyber Security training and background screening prior to access and with the inclusion of language concerning emergency provisions in accordance with FERC Order 706 (Option B above).
  - **CIP 003** Policy language will be reviewed/modified by a work group in Phase II, not Phase I.

F. Technical Feasibility Exception proposal

Michael Assante, NERC Chief Security Officer, addressed the group by phone and asked the team to consider addressing the technical feasibility exception as a priority and

possibly as part of Phase I. Mr. Assante pointed to the request from FERC to address this issue and reviewed issues to be considered:

- Develop a set of conditions or criteria for invoking technical feasibility exception
- Oversight of its use
- Want operational and safety considerations and not business judgment.
- Want to see a mitigation plan that achieves the same degree of security
- Wants time limitation on the use of the exception
- Senior manager approval of the exception, mitigation, and remediation time line
- Include audits and appeals of the exceptions
- Need to address confidentiality of the exception documentation
- ERO monitoring of the exception
- Accountability

Team discussion:

- Appreciate the importance of the issue but it will take quite a bit of discussion – adding it to the immediate scope may derail the ability to get the phase I products done and the removal of the business judgment language
- This exception should be a priority issue but after we complete the agenda today on the drafting materials for phase I
- Motion:
  - Motion was made by Chairperson to table the issue of the Technical Feasibility Exception until after the team agenda is completed.
  - In favor = 22 members; Against = 0; Abstain = 1; Not present = 1
  - The issue of Technical Feasibility was tabled until completion of the pre-defined agenda

G. Reviewing Sub team draft of NERC CIP Standard 006

Kevin Perry, as CIP 006 sub team leader, provided an overview of the revisions offered by the sub team in CIP 006 for consideration by the full team: *(See appendix #5 for link to red-line/underline revisions)*

- Removed Reasonable Business judgment
- Changed dates as appropriate
- Minor wording changes which did not alter the substance of the requirement
- R1.6 added that procedures for the active monitoring of escorted persons at all times are required.
- R1.8 added that the Physical Security Plan must be reviewed annually.
- R2. (Note: The prior 1.8 requirement becomes R2 in this proposal. The original suggested language follows:
  - R2. Protection of Physical Access Control Systems — Cyber Assets authorizing and logging access to the Physical Security Perimeter(s) shall:
  - R2.1. Exclusive of hardware at the Physical Security Perimeter access point such as electronic lock control mechanisms and badge readers, shall reside

within an identified Physical Security Perimeter or be physically monitored 24x7 by personnel authorized unescorted access.

- R2.2. Be afforded the protective measures specified in Standard CIP-003-1; Standard CIP-004-1 Requirement R3; Standard CIP-005-1 Requirements R2 and R3; Standard CIP-006-2 Requirements R4 and R5; Standard CIP-007-1; Standard CIP-008-1; and Standard CIP-009-1.

Initial Team Discussion and Questions:

- R1.6. How does an entity prove that escorts actively monitored persons at all times?
- Do we need evidence? Or Proof? You want evidence such as a manual sign-in book with the name of the escort associated with the visitor. Auditors need to understand that.
- Training and awareness is an essential part of the process. Make sure the escorts know their responsibilities.
- Order 706, Para 432 discusses the need for qualified escorts.
- Up to the auditor to prove that you did not comply. Needs a way to test the control.
- May need a NERC defined term on what escorted is.
- R2.1: what happens with a situation where the system is in use 8x5 and locked up otherwise. Unattended systems need to be within the PSP, HMI systems need to be secured when not in use.
- Does the system need to be in a PSP when not in use?

Initial Acceptability Rating

Acceptance of CIP 006 Proposed Changes	**4**	**3**	**2**	**1**
Voting Members	**10**	**7**	**2**	**0**

Team Discussion following Initial Acceptability Rating:

- Gave it a 2: R2.1, primarily around the issue surrounding the HMIs. Are we locking people into the card reader systems? One system may control everywhere.
- Gave it a 2: R3 is a new requirement that entities cannot comply with by July 1, 2009. Resolved by inclusion of a requirement-specific implementation plan.
- Whether the word 'remote' belongs in the physical access standard
- Define the Access Control System in the glossary. Address multiple systems that integrate together. [Credentialing, identification, authorization, authentication, accounting]

Revised Proposed CIP 006 language:

- R2. Protection of Physical Access Control systems – Cyber Assets that authorize and/or log access to the Physical Security Perimeters(s), exclusive of hardware at the Physical Security Perimeter access point such as electronic mechanisms and badge readers, shall:
- R2.1 be protected from unauthorized physical access
- R2.2 be afforded the protective measures specified in Standard CIP 003-1; Standard CIP 004-1 Requirement 3; Standard CIP 005-1 Requirements R2 and R3; standard CIP 006-2 Requirement R4 and R5; Standard CIP 007-1; standard CIP 008-1; and Standard CIP 009-1.

Acceptability Rating for CIP 006 with Revised Proposed Language:

Acceptance of CIP 006 Proposed Changes	**4**	**3**	**2**	**1**
Voting Members	**15**	**8**	**0**	**0**

H. Review of Sub Team Report on Measures & VRFs

Jerry Freese, leader for the sub team on measures, reported that their team performed a review of the measures, but based on changes prior to today's meeting, they believe there are no changes to the measures in response to proposed changes in CIP requirements.

Todd Thompson reported on behalf of the sub team reviewing VRFs that they believe no changes need to be made at this time.

I. New Implementation Plan for Changes to the Existing Requirements after Phase I Changes

Phillip Huff reported on the progress with the Implementation plan for new or changed Phase I requirements. *(See appendix #5 for link to red-line/underline revisions)* The original proposal was that the additional implementation plan would be expanded by 180 days to allow participants to comply with changed requirements.

- Proposed language: the original proposed effective date discussed for the modifications contained in these standards is the greater of (1) 180 days following approval by the FERC or (2) the number of days following approval by FERC before a Responsible Entity must become Compliant with a requirement according to the associated Compliance Schedule.

Team comments and suggestions:

- 180 days after regulatory approval unless the initial compliance table is already a later date.
- Comment made that all requirements of the eight standards are affected and thus the revised implementation date affects all requirements. Does not necessarily make sense.
- Does the entity still need to march toward compliance with Version 1 once the Version 2 standards have been approved by FERC?
- We have added the RE – what table applies? Table 4? Do they also get an additional 180 days beyond that?

- Side Note: CIP-003, R2 needs to be required for all entities in the same manner as CIP-002.

Based on team discussion, the sub team will make additional edits for consistency with changes made in the body of the document and make conforming changes to the standards as identified in review for creating the table.

J. COMMENT FORM REVIEW

Chairman Jeri Domingo-Brewer reviewed the sub team progress on the comment form: *(See appendix #5 for link to red-line/underline revisions)*

- Background information Section uses language out of the SAR to explain what the team had agreed to
- Summary of Phase I Revisions Section summarizes each of the changes
- Requests for Comments/Questions Section requests feedback from commenters

Team comments and suggestions:

- CIP-004, CIP-006, and Implementation Plan changes need to be updated in the Comment Form.
- How do we handle an industry response that says they do not care what FERC requires, they will not approve the changes?
- May need an educational WebEx prior to comment and ballot.
- Really need a robust communications plan.
- Need to reach out to the CIPC and possibly the Regional Compliance Managers.
- Group accepted that this is a good start on the Comment form

K. TECHNICAL FEASABILITY QUESTIONS

Having tabled the technical feasibility exemption question until the end of the day, the Chair asked members how and when they wanted to address the issue.

Team comments and suggestions:

- Is it reasonable to try to do this in Phase I?
- It will touch most, if not all standards. That will require us to at least revisit the implementation plan.
- It was agreed to table this discussion until the next day and the end of the review of Phase I items.

Members agreed to adjourn for the day.

A. DAY TWO – WELCOME AND AGENDA REVIEW

Chairperson Jeri Domingo-Brewer thanked the members of the sub teams for their hard work and reviewed the progress made by the group yesterday. She stated that today the team would:

- Review work from the remaining sub teams that were not reviewed yesterday
- Hanging issue that the group needs to consider pertaining to CIP 006
- Consider the issue of Technical Feasibility based on the request yesterday from Mike Assante of NERC asking the group to add this issue to the agenda for this meeting.

Stu Langton, with the FCRC Consensus Solutions facilitation team, recognized the many details the group was trying to address, the broad range of expertise they brought to the table and the need to build a common understanding of issues and how to address those issues. He discussed the need for individuals who raise questions or concerns to also offer a proposed solution or alternatives to help the group move forward.

B. Implementation Plan Amendments

Scott Mix, sub team lead, reviewed the work that has been done so far concerning implementation plans for new assets and other situations that will be covered under CIP standards in the future. The work included a summary, a narrative explanation of each category, and a timetable. *(See appendix #5 for link to red-line/underline revisions)*

He reviewed who and when an entity would need to be compliant. He noted three milestone categories:

- **Category 1** entities starting from scratch. Existing Table 4 will be used.
  - ***The first identified Critical cyber Asset for a Registered Entity***
  - 24 months to become compliant and 36 months to become auditable compliant.
- **Category 2** is for an entity that already has a schedule and is doing things but they have identified a newly identified Critical Asset.
  - ***Reclassification or change in status of an existing Critical Asset to a Critical Cyber asset.***
  - Questions were raised concerning how the proposed tables would work when/if the CIP standards apply to nuclear. There was no answer provided at this time as there are many variables which still need to be resolved.
  - Mergers
    - For mergers and acquisitions there is a one-year period to bring the two programs of the different companies into harmony.
    - After that one year and after completing the original CIP compliance tables, they would need to comply with the proposed category 2 timetable.

- **Category 3** deals with new assets within an existing Critical Asset. The assumption is that because you are doing something active and that you do not turn on the asset until you have completed the compliance needs within the construction.
  - ***An existing Critical Asset Replacement, reconfiguration, upgrade, or addition of a relevant cyber Asset associated with an existing Critical Asset.***
  - Construction of an asset (substation, etc.) that will be declared Critical upon activation
  - Replacement or upgrade of a Critical Asset
  - Addition of a Critical Cyber Asset at an existing Critical Asset

Scott Mix Sub reviewed the various time thresholds which the sub team is proposing for compliance with the various situations described in the above categories.

Team comments and suggestions:

- One SDT member suggested that NERC maintain consistency in the implementation plans across all the NERC standards.
- The assumption is that if an entity is planning and constructing a new Critical Asset, CIP security compliance should be part of the construction. If a cyber asset exists but through a change such as load flow analysis becomes critical, the entity is provided time to come into compliance with the CIP standards.
- Evergreen plan – affects entities already expected to be Compliant under their original implementation table.
- Assumes everyone is fully in compliance with CIP-002. New entities registering for the first time will come under Table 4 in the original plan.
- Table is applicable to each registered entity. If a merged company retains the original registrations, then a merging of the CIP compliance programs might not be necessary.
- What about a purchase of an asset as opposed to a company merger. Falls into Category 2. Section describing this scenario needs some clarification since the remainder of the paragraph speaks to a merger scenario.
- Need to grandfather assets already in construction under Category 2.
- Merging of companies – harmonization of compliance programs spans all reliability standards, not just CIP.
- Upgrades and modifications to existing Cyber Assets that cause them to become Critical Cyber Assets needs to include the necessary compliance steps as part of the upgrade.
- SDT is asked to evaluate the new table against some business cases to determine if there are gaps or inconsistencies.
- Should require the entity to perform the Risk Assessment prior to placing a new asset or Cyber Asset into service.
- Need to address business cases in the implementation plan

- **Implementation Plan Discussion**
  - Dave Norton volunteered to write a white paper explaining scenarios and he asked for written and constructive input from team members.
  - Vice Chairman explained 6 different scenarios and how each type of scenario could be gamed by entities.
  - A SDT member asked if the implementation time frames should distinguish between field assets (substations, etc.) vs. control center assets. Some team members did not believe the implementation plan was the place to deal with the differences. Further team thought this may need to be considered in Phase II.
- **Homework Assignment Concerning Implementation Plan + Proposed Comment Form:**
  - Team members are asked for a treatment of example scenarios that summarize the categories
  - The goal is to ask yourself 3 questions and categorize appropriate events
  - Suggestions from the team should be send to the Sub Team before October 29.
  - Staff will email the team the Implementation Plan for their review.
  - Comments should be sent to Scott.Mix@NERC.net
  - The Chair asked that the SDT also review the Comment form and provide input to the Comment Form Sub Team.

C. CIP 006 Un-resolved Issue

An additional proposed modification to CIP 006 R1.6 language was discussed and accepted by the group as follows:

- Continuous escorted access within the Physical Security Perimeter of personnel not authorized for unescorted access.

D. CIP 003 Changes and Discussion

Proposed changes were offered to CIP 003 as follows: *(See appendix #5 for link to red-line/underline revisions)*

> **CIP 003 R2:** Leadership — The Responsible Entity shall assign a single senior manager with overall responsibility and authority for leading and managing the entity's implementation of, and adherence to, Standards CIP-002 through CIP-009.

f. NERC audit compliance staff clarified that the Responsible Entity may be either the Corporation as a whole or may be the Registered Entity functions (GO, TO, BA, etc.).

~~g.~~ **CIP 003 R3.2.** Documented exceptions to the cyber security policy must include an explanation as to why the exception is necessary and any compensating measures. ~~taken or a statement accepting risk. and/or any residual risk~~

Team comments and suggestions:

Senior Manger:

- Designated by the Registered Entity (registered function)
- Can be the same for multiple registrations (multiple functions)

Exceptions:

- Note that an entity cannot take exception to the regulatory standard, and so the exception would be taken to the entity's own policy. Believe that the flexibility for compensating measures and residual risk was appropriate.
- The NIST technical feasibility material may have language that would be of assistance with the concerns.
- The FERC comment referred more to regulatory compliance rather than compliance with the entity's own policy.
- The reference to acceptance of risk needs to be removed as directed by FERC.
- The issue of removing acceptance of risk is so difficult that it should be moved to Phase II.
- Or the language that provides for acceptance of risk should be removed from the CIP standard.

After reviewing several suggested changes, members were asked to rate the language as revised above striking "or acceptance of risk":

The SDT 1st initial rating on acceptance of the proposal.

Scale	4 – Acceptable as it	3 – Acceptable with minor concerns	2 – Not acceptable unless major concerns are addressed	1 – Not acceptable
Voting on the above by SDT	11	7	1	0

Following additional discussion, members were asked to rate the proposal again without the word "any" before "compensating measures:

The SDT 2nd vote on acceptance of proposed language change.

Scale	4 – Acceptable as it	3 – Acceptable with minor concerns	2 – Not acceptable unless major concerns are addressed	1 – Not acceptable
Voting on the above by SDT	12	6	4	0

Following additional discussion, members agreed to retain the word "any"

There was general agreement around the room that in CIP 007 wherever the phrase "acceptance of risk" appears, it will be removed even though each such instance where the phase appears may not have been discussed at length.

E. Proposal to Substitute "Prudent Judgment" for "Reasonable Business Judgment"

Member John Varnell requested the group consider substituting the term "prudent judgment" in place of the term "reasonable business judgment."

Team comments and suggestions:

- The concern is that the cost to remediate the last few percentages of risk could be cost prohibitive.
- FERC believes, in the order, that "reasonable business judgment" is not required to address that issue
- It was pointed out that Paragraph 132 of FERC order states that there is no recourse needed to substitute another term concerning judgment.

Due to a lack of support, the group decided not to move forward with the replacement of the term "reasonable business judgment" with 'prudent judgment."

F. Proposed a Definition of Access Control System

As requested by the drafting team, Scott Mix offered a draft definition of Access Control System as follows:

> A system which provides for Authorization, Authentication, and frequently Accounting of access through either a Physical Security Perimeter or an Electric Security Perimeter. An Access Control System may be a single computer system which performs all three functions or may be a combination of two or more computer sub systems which work together to accomplish all three functions.
>
> - Authentication is the process of verifying a users or object's identify.
> - Authorization is process for granting an authenticated user or object's the authority to perform a certain operation.
> - Accounting provides an audit trail of access, and includes logging of access by identification and time.

Team comments and suggestions:

- Needed to provide clarity to CIP-005 and CIP-006
- Will help industry understand the concept.
- Does not include a credentialing system.
- Should be a requirement around the credentialing system.
- The SDT was asked to submit their comments for the resolution of preferences concerning the definition to Vice Chair, Kevin Perry.

G. Technical Feasibility

The Chair that there were two potential proposals (one from Scott Mix and one from Keith Stouffer) for addressing "technical feasibility" exception in Phase 1. She asked the team to listen to each of the proposals, consider the proposals, and decide if one of the alternatives offered could be included within the Phase I work of this team.

- **Scott Mix reviewed material directed in the FERC Order 706**
  - All requirements in a NERC standard must be adhered to
    - Implies no exception
  - Self report a non-compliance (exception) with Mitigation Plan is allowed
  - Commission views the term 'acceptance of risk' as an uncontrolled exception
  - Alternative language that deals with such issues in terms of technical feasibility is preferable.
  - Flexibility along with control is the goal.
  - FERC does not support the long established practice of risk acceptance by sr. management
  - FERC wants specific framework for invoking the technical feasibility provisions
  - FERC narrows the application by stating that there are acknowledged concerns (device will not support) compliance with the requirement
  - For future installations the technical feasibility would not carry forward. New equipment should be compliant.
  - FERC steps
    - Comparable level of security to the requirement
    - A remediation plan although a date certain is not required for replacement
  - Exemptions should be reports, justified, and approved by the ERO or relevant Regional Entity
  - Regional entities should catalog notices of technical feasibility
  - Actual evaluation and approval of technical feasibility exceptions should be performed
  - Technical feasibility should be audited
  - NERC must protect such information
  - FERC wants a framework includes mitigation steps, regular review, justification, internal approval by the senior manager, wide area approval through the ERO audit process, and cooperation with the ERO to provide the Commission with high level impact of the technical feasibility on the reliability of the grid.

- **Keith Stouffer of NIST provided an alternative proposal on Technical Feasibility**
  - This is addressed within the NIST framework for risk management
  - The Responsible entity may invoke a technical feasibility exception to a requirement is any of the following conditions apply:
    - The requirement poses a risk to the reliability of the Bulk Power System

- The requirement creates a significant adverse effect on operations and/or safety impact
- The requirement specifies mechanisms or functions that are not technically possible for a cyber asset to support

- The responsible entity shall document all Technical Feasibility exceptions in an Exception Plan containing:
  - A justification why the Technical Feasibility exception is necessary
  - Compensating controls or mitigation steps that provide a comparable level of security
  - A plan of action, milestones, and schedule for implementing the compensating controls.
  - Obtain approval by the senior manager
  - Approval by the Regional Entity or the ERO
  - ERO must annually audit compliance with the Exception plan
  - ERO to provide FERC with a high level assessment of the exceptions on reliability of the Bulk Power System
  - Keith proposed that this section may be included before the effective date

- Scott Mix also reviewed the current Self Reporting Process. Based on the similarities between FERC directives and the items required by a self reporting of non-compliance, Scott suggests that this same process be used for Technical Feasibility Exceptions:
  - Document non compliance to a specific requirement
  - Provide explanation
  - Describe reliability impact
  - Describe any external or extraneous factors
  - Provide mitigation plan
  - Provide mitigation schedule
  - Obtain Senior Officer signature
  - Catalog and approval by ERO
  - Catalog and approval by Regional Entity
  - Submit to FERC (US Entities)

Scott Mix reviewed similarities between the proposals:

Keith Proposal	Scott Proposal
A justification why the Technical Feasibility exception is necessary	Document non compliance to a specific requirement h. Provide explanation i. Describe reliability impact j. Describe any external or extraneous factors

Compensating controls or mitigation steps that provide a comparable level of security	
A plan of action, milestones, and schedule for implementing the compensating controls.	Provide mitigation schedule Provide mitigation plan
Obtain approval by the senior manager	Obtain Senior Officer signature
	Catalog and approval by Regional Entity
ERO must annually audit compliance with the Exception plan	Catalog and approval by ERO May trigger accelerated audit schedule Annual review and re-approval by Responsible Entity and ERO
ERO to provide FERC with a high level assessment of the exceptions on reliability of the Bulk Power System	ERO to develop separate annual report to FERC Analyze the combined impact of all Technical Feasibility exemptions
	Report will contain sensitive information – must be CEI protected
	Submit to FERC (US Entities)

Team comments and suggestions:

- **Information Protection Concerns**
  - Concern was voiced about the controls over protection of the information that would be supplied
  - The specific detail regarding the exception should stay with the asset owner.
  - NERC has not yet addressed the confidentiality issue to any great extent
- **Proposed Whitepaper on Technical Feasibility**: draft and submit to the industry a high level concept document on Technical Feasibility simultaneously, but not as part of a revision to the standard in Phase I. Offer the industry a comment period to react to this as a concept to be folded into a standard later.
  - Allows the regions to review and respond to the proposal.
  - Allows time for NERC to assure protection of the information to be provided.
  - Questions arose concerning whether the technical feasibility exception applied to all requirements or to only certain of the requirements.

- **Proposal** Prepare a 'conceptual' document to seek stakeholder consideration and feedback that describes a Technical Feasibility Exception process that parallels existing compliance self report process.

Scale	4 — Acceptable as it	3 — Acceptable with minor concerns	2 — Not acceptable unless major concerns are addressed	1 — Not acceptable

1st Poll — Voting SDT	20	2	0	0

Additional Team comments and suggestions:

- Need to address issue of information protection in the proposal
- Who will be involved?

Next Steps for Technical Feasibility "White Paper":

- Proposal Sub Team: Tom Hofstetter, John Varnell, Keith Stouffer, Scott Mix, Jerry Freese and possibly someone from NERC compliance.
- Due for the next full team meeting

H. Assignments and Next Steps for the Next Meeting

1. For the next WebEx, October 29:

- NERC staff needs final products by cob Monday, 27th to distribute on Tuesday
- NERC staff will provide progress report on Draft proposal concerning technical feasibility
- Implementation Plan for new CA/CCA — should be done and distributed prior to October 27
- Implementation plan (CIP Version 2)
- Final Comment Form on the 28th
- Final versions of CIP 004 & CIP 006 language

2. Notes on Future Meetings and Proposed Topics

- Webex, November 3 — develop concept document for Technical Feasibility. Deliver to full team by November 7 or 10.
- Webex, November 5 – following NERC Staff feedback, review and conform drafts per feedback.
- November 12–14 — full team meeting in Little Rock, Arkansas to Finalize Phase I documents as needed and review proposed roadmap
- December 4 or 5 — In person meeting at FERC Offices in Washington DC
- January 7–9 — In person meeting at APS in Phoenix, AZ

3. Roadmap Proposals and Discussion

The Chair suggested that in December the group may begin to hash out the large issues still to be addressed. She cautioned members to think outside the box when it comes to all of the work to be done in the future.

The Vice Chair offered two alternatives to the "Roadmap" going forward, a multiple phase or single phase approach.

Multiple Phases:

- Phase I — Issues defined

- Phase II — Technical Feasibility Exception
- Phase III — Risk Assessment framework (18-24 months from end of Phase I). Overhaul CIP-002. Review future phases at that point for CIP-003 through CIP-009. Consider breaking apart the standards into Generation, Transmission, Control Centers, and Special Protection Controls.

Single Phase II:

- Phase II is everything not in Phase I
- Would be continuously communicating with the industry during the development time
- Can choose to post work once majority is completed in the event there are a couple of really difficult issues still on the table.
- Expect to have everything nailed down within 18 months of Phase I.

The Vice Chair made a proposal that the SDT should use an incremental approach.

Team comments and suggestions:

- Nothing sacred about 8 standards.
- If we are going to fundamentally change the standards, we do not want to dribble them out.
- Really intriguing concept to break out the standards functionally rather than one size fits all.
- At some future date we need to have the strategy planning session to determine how we approach the task at hand.
- Does there need to be a training of the industry as part of the strategy?
- Everything is an iterative process – determine next step as you finish up the current step.
- We are concerned with control systems, not information systems. Need to bear that concept in mind as we move forward.
- If we are going to make a revolutionary change, we need to start chewing on that now.
- We are starting to look more and more like traditional IT systems (Off The Shelf solutions are now proliferating).
- The integrated nature of systems is a real issue. We have to figure out how to deal with distribution and home network systems since they interconnect with the transmission-level systems. Also need to consider and handle interdependencies of critical infrastructures.
- Do we have enough representation on the team regarding distributive control systems? Need someone with ISA experience or expertise.
- Probably going to need a couple of days to hash out the strategy. Focus on work plan now and the strategy in January.
- Should address early on the requirement to address the FERC issue of compromised systems (used for malicious control).

- Need to resolve the information protection issues for the required external review of Critical Assets.
- When are we going to address Physical Security of the Critical Assets?
- One of the 17 control families in NIST is physical security controls.
- Pending legislation that will bring distribution systems into the critical infrastructures.
- Do we need a CIP-010 to address emergency actions?
- What are the implications for when the standards apply to the nuclear side of the house?

The FCRC Consensus Solutions facilitation team were asked to develop a one page proposal (big picture straw proposal and guiding principles) for addressing the remaining issues following Phase I for review and discussion by the full group at the next meeting in Little Rock, Arkansas. Member discussion today has included several key principles that could guide development and discussion of remaining issues.

4. Review of Remaining "Parking Lot" Issues Identified at the First SDT 706 Meeting

"Parking Lot" Issue:	
Emergency	Phase II item
Define Cyber Security Incident	Phase II item
006 SCG&E interpretation	Phase II item
Audit against policy question Industry concern regarding CIP 003 language that says the Responsible entity shall document & implement a cyber security. If the policy or sub documents exceed the CIP standards in depth or in scope, there is a desire within the industry for NERC to clarify that if they are in conformance with the CIP standards but fall short of their policy implementation, they should not be held in non-compliance. Auditors are asking the industry to demonstrate that they are in compliance.	NERC compliance staff have stated that they will audit to the standards
Communications Plan	In the future regular updates to regulators, and industry stakeholders will be necessary.

I. What Worked and Did not work

At the conclusion of the meeting, the facilitators asked the Team to offer an evaluation of the process including what worked well during the meeting and what could be improved.

What Worked Well:

- Prep work of the sub teams
- Need to improve the sound on the Web ex's for those who are not attending in person
- Talking about issues in a general way instead of the individuals' corporation perspective
- NERC staff offered feedback that they are pleased with the progress that is being made by the SDT
- Detailed agenda
- Assignments were completed prior to the meeting
- No picking holes – offered improvements
- People left their company hats at the door more often
- Refrained from violent agreement
- Many thanks to Kevin Sherlin and SMUD for hosting the meeting
- While we may have issues, this group has made excellent strides reaching consensus on our issues. Much more productive than most other teams.
- Scott and Harry have done a lot of pre-work and evening work to keep the team making progress.
- We all respect each other and agree to disagree
- External facilitation is essential
- Phase I is NOT a toothless tiger as had been feared.

What Could Be Improved Work

- Phone system is difficult. Hard to hear and follow the meeting
- Need to identify speaker when starting to speak
- Seemed bureaucratic at times
- When offering feedback, speakers should offer improvements not just pick on proposals
- On a couple of occasions the SDT got bogged down in details
- Need to facilitate toward resolution rather than getting bogged down in details.

Members agreed to adjourn until the next meeting on November 12-14, 2008 in Little Rock, Arkansas.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Appendix # 1

Meeting Agenda

Cyber Security Order 706 SDT — Project 2008-06

October 21, 2008 | 8 a.m.–5 p.m.
October 22, 2008 | 8 a.m.–5 p.m.
Sacramento Municipal Utility District
6301 S Street
Sacramento, California

Day 1 Agenda

1. **8 a.m. — Opening Remarks — Jeri Domingo-Brewer, Chair and Kevin Perry, Vice Chair**
   a. SMUD Welcome — announcements, logistics
   b. NERC Antitrust Compliance Guideline
   c. FSU/CRC review of last meeting and adoption of meeting summary
2. **8:15 a.m. — SDT Organizational Issues: Purpose Statement and Adopt Rules of the Road**
3. **9 a.m. — Presentation and Review of Phase I Drafting Group Products**
   a. (Requirements, Measures, Implementation Plan, Comment Form, VRFs)
4. **10:15 a.m. — BREAK**
5. **10:30 a.m. — Phase I presentations and review — continued**
6. **noon Lunch — working (return to meeting at 12:45 p.m. ET)**
7. **12:30 p.m. — Phase I presentations and review — continued**
8. **3 p.m. — BREAK**
9. **3:15 p.m. — Review of Assignments to Finalize Phase I Redline Versions**
10. **4:45 p.m. — Review of Progress and Adjustments, as needed, Day 2 Agenda**
11. **5:00 p.m. — Recess**

Day 2 Agenda

12. **8 a.m. — Opening, Review of Day One Results and Day Two Agenda — Jeri Domingo-Brewer, Chair and Kevin Perry, Vice Chair**
13. **8:15 a.m. — SDT Organizational Issues (TBD)**
14. **8:30 a.m. — Post Phase I (Phase II) Project Roadmap — discussion**
    - Review of CIP 002-009 — Identify Approach, Key Issues from FERC Directive including NIST comparison, etc.
15. **10:30 — BREAK**
16. **10:45 — Continue Review of CIP 002-009 — Approach, Issues from FERC Directive including NIST comparison**
17. **noon — Lunch — working (return to meeting at 12:45 p.m. ET)**
18. **12:45 p.m. — Review of CIP 002-009 — Approach, Issues from FERC Order including NIST comparison.**
19. **2:45 p.m. — BREAK**
20. **3 p.m. — Post Phase I Project Roadmap — discussion, continued**
    - Disposition of RFI from SCE&G and U.S. Army Corps of Engineers
    - Review of Parking lot items from Gaithersburg meeting or Day 1
    - Initial Phase 2 Schedule Structure
21. **4:15 p.m. — Review of short term meeting schedule and Post Phase I drafting assignments**
22. **4:45 p.m. — Next Steps and Evaluation**
23. **5 p.m. Adjourn**

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Appendix # 2

Cyber Security for Order 706 SDT Attendees List
Project 2008-06 — CS 706 SDT
SMUD — Sacramento, CA
October 21, 2008

Attending in Person — Team Members

1. D. Jack Bernhardsen	President/Manager Pacific Northwest Security Coordinator, Inc.
2. Jeri Domingo-Brewer, Chair	U.S. Bureau of Reclamation
3. Sharon Edwards	Project Manager, Duke Energy
4. Scott Fixmer	Senior Security Analyst Exelon Corporate Security, Exelon Corp.
5. Gerald S. Freese	Director, Enterprise Information Security America Electric Power
6. Tom Hoffstetter	Midwest ISO, Inc
7. Philip Huff	Arkansas Electric Cooperative Corporation
8. Richard Kinas	Orlando Utilities Commission
9. John Lim	CISSP, Department Manager, Consolidated Edison Co. of New York
10. David Norton	Policy Consultant, CIPEnergy Coporation
11. Kevin B. Perry, Vice Chair	Director, IT-Infrastructure, Southwest Power Pool
12. Christopher A. Peters	ICF International
13. David S. Revill	Georgia Transmission Corporation
14. Kevin Sherlin	Sacramento Municipal Utility District
15. Jonathan Stanford	Bonneville Power Administration
16. Keith Stouffer	National Institute of Standards & Technology
17. Michael Winters	Arizona Public Service Co.
18. William Winters	Hydro One Networks, Inc.
19. David Taylor	NERC
20. Harry Tom	NERC
21. Roger Lampila	NERC
22. Scott R. Mix	NERC
23. Todd Thompson	NERC
24. Hal Beardall	FSU/FCRC Consensus Center
25. Stuart Langton	FSU/FCRC Consensus Center

SDT Team Members Attending via WebEx

1. Jay S. Cribb	Information Security Analyst, Principal, Southern Company Services, Inc.
2. Joe Doetzl	Manager, Information Security, Kansas City Power & Light Co.
3. Jackie Collett	Manitoba Hydro
4. Scott Rosenberger	Luminant Energy
5. John D. Varnell	Technology Director, Tenaska Power Services Co.

SDT Team Members Unable to Attend or Participate by WebEx

1. Bryan L. Singer	Kenexis

Attending in Person — Participants

1. James Brenton	ERCOT
2. Michael Toecker	Burns & McDonnell Engineering

Attending via WebEx — Participants

1. James Bassett	IPC
2. Marcus Braendle	ABB
3. Steve Brezina	WAPA
4. Jerome Farquharson	Burns & McDonnell Engineering
5. Mike Mertz	Southern California Edison
6. Matt Schnell	Nebraska Public Power District
7. Karen Yoder	First Energy

List of Attendees — Cyber Security Order 706
Standard Drafting Team Meeting
SMUD — Sacramento, CA
October 22, 2008

Attending in Person — Team Members

1. D. Jack Bernhardsen	President/Manager Pacific Northwest Security Coordinator, Inc.
2. Jeri Domingo-Brewer, Chair	U.S. Bureau of Reclamation
3. Sharon Edwards	Project Manager, Duke Energy
4. Scott Fixmer	Senior Security Analyst Exelon Corporate Security, Exelon Corp.
5. Gerald S. Freese	Director, Enterprise Information Security America Electric Power
6. Tom Hoffstetter	Midwest ISO, Inc
7. Philip Huff	Arkansas Electric Cooperative Corporation
8. Richard Kinas	Orlando Utilities Commission
9. John Lim	CISSP, Department Manager, Consolidated Edison Co. of New York
10. David Norton	Policy Consultant, CIPEnergy Coporation
11. Kevin B. Perry, Vice Chair	Director, IT-Infrastructure, Southwest Power Pool
12. Christopher A. Peters	ICF International
13. David S. Revill	Georgia Transmission Corporation
14. Kevin Sherlin	Sacramento Municipal Utility District
15. Jonathan Stanford	Bonneville Power Administration
16. Keith Stouffer	National Institute of Standards & Technology
17. Michael Winters	Arizona Public Service Co.
18. William Winters	Hydro One Networks, Inc.
19. David Taylor	NERC
20. Harry Tom	NERC
21. Roger Lampila	NERC
22. Scott R. Mix	NERC
23. Todd Thompson	NERC
24. Hal Beardall	FSU/FCRC Consensus Center
25. Stuart Langton	FSU/FCRC Consensus Center

SDT Team Members Attending via WebEx

1. Jay S. Cribb	Information Security Analyst, Principal, Southern Company Services, Inc.
2. Joe Doetzl	Manager, Information Security, Kansas City Power & Light Co.
3. Jackie Collett	Manitoba Hydro
4. John D. Varnell	Technology Director, Tenaska Power Services Co.

SDT Team Members Unable to Attend or Participate by WebEx

1. Bryan L. Singer	Kenexis
2. Scott Rosenberger	Luminant Energy

Attending in Person — Participants

1. James Brenton	ERCOT
2. Michael Toecker	Burns & McDonnell Engineering

Attending via Webex — Participants

1. Haung Ngo	Reliant
2. Karen Yoder	First Energy

Appendix # 3

NERC Antitrust Compliance Guidelines

I. General

It is NERC's policy and practice to obey the antitrust laws and to avoid all conduct that unreasonably restrains competition. This policy requires the avoidance of any conduct that violates, or that might appear to violate, the antitrust laws. Among other things, the antitrust laws forbid any agreement between or among competitors regarding prices, availability of service, product design, terms of sale, division of markets, allocation of customers or any other activity that unreasonably restrains competition.

It is the responsibility of every NERC participant and employee who may in any way affect NERC's compliance with the antitrust laws to carry out this commitment.

Antitrust laws are complex and subject to court interpretation that can vary over time and from one court to another. The purpose of these guidelines is to alert NERC participants and employees to potential antitrust problems and to set forth policies to be followed with respect to activities that may involve antitrust considerations. In some instances, the NERC policy contained in these guidelines is stricter than the applicable antitrust laws. Any NERC participant or employee who is uncertain about the legal ramifications of a particular course of conduct or who has doubts or concerns about whether NERC's antitrust compliance policy is implicated in any situation should consult NERC's General Counsel immediately.

II. Prohibited Activities

Participants in NERC activities (including those of its committees and subgroups) should refrain from the following when acting in their capacity as participants in NERC activities (e.g., at NERC meetings, conference calls and in informal discussions):

- Discussions involving pricing information, especially margin (profit) and internal cost information and participants' expectations as to their future prices or internal costs.
- Discussions of a participant's marketing strategies.
- Discussions regarding how customers and geographical areas are to be divided among competitors.
- Discussions concerning the exclusion of competitors from markets.
- Discussions concerning boycotting or group refusals to deal with competitors, vendors or suppliers.

III. Activities That Are Permitted

From time to time decisions or actions of NERC (including those of its committees and subgroups) may have a negative impact on particular entities and thus in that sense adversely impact competition. Decisions and actions by NERC (including its committees and subgroups) should only be undertaken for the purpose of promoting and maintaining the reliability and adequacy of the bulk power system. If you do not have a legitimate

purpose consistent with this objective for discussing a matter, please refrain from discussing the matter during NERC meetings and in other NERC-related communications.

You should also ensure that NERC procedures, including those set forth in NERC's Certificate of Incorporation and Bylaws are followed in conducting NERC business. Other NERC procedures that may be applicable to a particular NERC activity include the following:

- Reliability Standards Process Manual
- Organization and Procedures Manual for the NERC Standing Committees
- System Operator Certification Program

In addition, all discussions in NERC meetings and other NERC-related communications should be within the scope of the mandate for or assignment to the particular NERC committee or subgroup, as well as within the scope of the published agenda for the meeting.

No decisions should be made nor any actions taken in NERC activities for the purpose of giving an industry participant or group of participants a competitive advantage over other participants. In particular, decisions with respect to setting, revising, or assessing compliance with NERC reliability standards should not be influenced by anti-competitive motivations.

Subject to the foregoing restrictions, participants in NERC activities may discuss:

- Reliability matters relating to the bulk power system, including operation and planning matters such as establishing or revising reliability standards, special operating procedures, operating transfer capabilities, and plans for new facilities.
- Matters relating to the impact of reliability standards for the bulk power system on electricity markets, and the impact of electricity market operations on the reliability of the bulk power system.
- Proposed filings or other communications with state or federal regulatory authorities or other governmental entities.
- Matters relating to the internal governance, management and operation of NERC, such as nominations for vacant committee positions, budgeting and assessments, and
  employment matters; and procedural matters such as planning and scheduling meetings.

Any other matters that do not clearly fall within these guidelines should be reviewed with NERC's General Counsel before being discussed.

Appendix # 4

Assignments from First SDT 706 meeting (Gaithersburg, MD)

	Task	Leader	Sub team	Due Date
1	CIP-004 R2 and R3	Jackie Collett	Chris Peters, John Varnell, Sharon Edwards	Straw Proposal due to sub team leader on October 14 in advance of sub team WebEx on October 15
2	CIP-006 R1	Kevin Perry	Joe Doetzl, Scott Fixmer, Thomas Hofstetter	Straw Proposal due to sub team leader on October 14 in advance of sub team WebEx on October 15
3	Review Measures associated with changes in CIP-002 to CIP-009	Jerry Freese	Keith Stouffer, Roger Lampila, Todd Thompson	Straw Proposal due to sub team leader on October 14 in advance of sub team WebEx on October 15
4	Implementation Plan – update to address newly identified CA	Scott Mix	Michael Winters, Dave Norton, Kevin Perry	Straw Proposal due to sub team leader on October 14 in advance of sub team WebEx on October 15
5	Implementation Plan update to address revised Requirements from Phase I and Mapping document – matrix that compares current version of standard with revised version with a comment that explains what changed.	Phil Huff	Kevin Sherlin, Scott Rosenberger, Jon Stanford, Scott Mix	Straw Proposal due to sub team leader on October 14 in advance of sub team WebEx on October 15
6	Comment Form – including an extensive write-up of the background, rationale for revisions, explanatory text.	Jeri Domingo-Brewer	Steve Vandenberg, Harry Tom, Sharon Edwards, John Lim	Straw Proposal due to sub team leader on October 14 in advance of sub team WebEx on October 15
7	Review VRFs associated with changes in CIP-002 to CIP-009	Todd Thompson	Roger Lampila	Straw Proposal due to sub team leader on October 14 in advance of sub team WebEx on October 15

Appendix # 5

Below is a link to the presentations and all of the documents reviewed as part of the SDT 706 Sub Team Reports with red-lined/underlined revisions proposed by Sub Teams and further revisions agreed to during the full Team discussions in Sacramento:

http://www.nerc.com/filez/standards/Project_2008-06_Cyber_Security-RF.html

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Appendix #6

Standard Drafting Team Draft Consensus Guidelines

October 21–22, 2008

CONSENSUS DEFINED

Consensus is a **process**, **an attitude and an outcome**. Consensus processes can produce better quality more informed products.

A. Consensus is a problem solving process in which all members:

1. Jointly distinguish their concerns
2. Educate each other
3. Jointly develop alternatives and then
4. Adopt recommendations everyone can embrace or at least live with.

In a consensus process, members can honestly say:

- I believe that other members understand my point of view
- I believe I understand other members' points of view
- Whether or not I prefer this decision, I support it because it was arrived at openly and fairly and because it is the best solution for us at this time

B. Consensus as an attitude provides that each member commits to work toward agreements that meet their own and other member needs and that all can support the outcome.

C. Consensus as an outcome means that agreement is reached by all members or by a significant majority of members. The level of enthusiasm for the agreement may not be the same among all members on any issue, but on balance all should be able to live with the overall package. **Levels of consensus** can include:

- Participants strongly support the solution
- Participants can "live with" the solution
- Some participants do not support the solution but agree not to veto it.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Draft Consensus Guidelines

The Cyber Security for Order 706 Standard Drafting Team (Team) will seek consensus on its recommendations for any revisions to the CIP standards including assessment of the reliability and market interface impacts.

General consensus is a participatory process whereby, on matters of substance, the members strive for agreements which all of the members can accept, support, live with or agree not to oppose. In instances where, after vigorously exploring possible ways to enhance the members' support for the final package of recommended revisions, and the Team finds that 100% acceptance or support is not achievable, final consensus recommendations will require at least 75% favorable vote of all members present and voting. This super majority decision rule underscores the importance of actively developing consensus throughout the process on substantive issues with the participation of all members. In instances where the Team finds that even 80% acceptance or support is not achievable, the Team's report will include documentation of any differences as well as the options that were considered for which there was greater than 50% support from the Team.

The Team will develop its recommendations using consensus-building techniques with the leadership of the Chair and Vice Chair and the assistance of the facilitators. Techniques such as brainstorming, ranking and prioritizing approaches will be utilized. The Team's consensus process will be conducted as a facilitated consensus-building process. Team members, NERC staff and facilitators will be the only participants seated at the table. Only Team members may participate in discussions and vote on proposals and recommendations. The Chair and Vice Chair may request specific clarification from observers in order to assist the Team in understanding an issue. Observers/members of the public are welcome to speak during a public comment period that will be provided at each meeting, and all written comments submitted on the comment forms will be included in the Team and facilitators' summary reports.

To enhance the possibility of constructive discussions as members educate themselves on the issues and engage in consensus-building, members agree to refrain from public statements that may prejudge the outcome of the Team's consensus process. In discussing the Team process with the media, members agree to be careful to present only their own views and not the views or statements of other participants and/or may direct such inquiries to the Team Chair and Vice Chair. In addition, in order to provide balance to the Team process, members agree to represent and consult with their stakeholder interest group.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Meeting Guidelines for Participants

Participants' Role in Meetings:

- Explore possibilities
- Listen to understand (Respect) (limit sidebar conversations)
- Be focused and concise. (Avoid repetition. No need to offer comments in "strong agreement.")
- Focus on issues, not personalities.
- Offer options to address others' concerns.
- No sidebars.
- If participating by phone, indicate who is speaking.
- If participating by phone, please use the mute button. **Do not** put the phone on hold.

Facilitators/Staff Role in Meetings:

- Assist the Chair and Vice Chair in helping the Team stay on task
- Help the group follow agreed upon ground rules
- Design the meeting and problem solving process in consultation with the Chair and Vice Chair
- Facilitate discussion participation of the Team and other participants
- Prepare agenda packets and reports

Consensus Building Techniques

- **Brainstorming** (green light thinking – not judgmental) At certain points, the facilitator may ask the group to suspend judgment and get ideas onto the table before debating.

- **Name Stacking in Team Discussions**
  - Members in the room should use name tents to be recognized to speak
  - Telephone participants should give their name and indicate desire to speak on the topic

- **Acceptability Consensus Ranking Scale**
  - Use a consensus acceptability scale to help focus discussion and test support in reviewing substantive issues.
  - Use to guide and focus discussion, not used as a voting mechanism. Rather it is a poll to see where folks are.
  - Must be prepared to offer refinements and suggestions to address serious concerns.

  4 = Proposal is acceptable as it is
  3 = Proposal is acceptable; I can live with it but there are minor concerns to address

2 = Proposal is not acceptable. Proposal may be acceptable if the major concerns are addressed

1 = Proposal is not acceptable

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Meeting Agenda

Cyber Security Order 706 SDT — Project 2008-06

October 21, 2008 | 8 a.m.–5 p.m.
October 22, 2008 | 8 a.m.–5 p.m.
Sacramento Municipal Utility District
6301 S Street
Sacramento, California

Cyber Security Order 706 SDT — Day 1 Agenda

1. 8:00 Opening Remarks — Jeri Domingo-Brewer, Chair and Kevin Perry, Vice Chair
   a. SMUD Welcome — announcements, logistics
   b. NERC Antitrust Compliance Guideline
   c. FSU/CRC review of last meeting and adoption of meeting summary
2. 8:15 SDT Organizational Issues: Purpose Statement and Adopt Rules of the Road
3. 9:00 Presentation and Review of Phase I Drafting Group Products
   (Requirements, Measures, Implementation Plan, Comment Form, VRFs)
4. 10:15 BREAK
5. 10:30 Phase I presentations and review — continued
6. 12:00 Lunch — working (return to meeting at 12:45 p.m. ET)
7. 12:30 Phase I presentations and review — *continued*
8. 3:00 BREAK
9. 3:15 Review of Assignments to Finalize Phase I Redline Versions
10. 4:45 Review of Progress and Adjustments, as needed, Day 2 Agenda
11. 5:00 Recess

116-390 Village Blvd.
Princeton, NJ 08540
609.452.8060 | www.nerc.com

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Cyber Security Order 706 SDT — Day 2 Agenda

12. 8:00 Opening, Review of Day One Results and Day Two Agenda — Jeri Domingo-Brewer, Chair and Kevin Perry, Vice Chair
13. 815 SDT Organizational Issues *(TBD)*
14. 8:30 Post Phase I (*Phase II*) Project Roadmap — discussion
    - Review of CIP 002-009 — Identify Approach, Key Issues from FERC Directive including NIST comparison, etc.
15. 10:30 BREAK
16. 10:45 Continue Review of CIP 002-009 — Approach, Issues from FERC Directive including NIST comparison
17. 12:00 Lunch — working (return to meeting at 12:45 p.m. ET)
18. 12:45 Review of CIP 002-009 — Approach, Issues from FERC Order including NIST comparison.
19. 2:45 BREAK
20. 3:00 Post Phase I Project Roadmap — discussion, continued
    - Disposition of RFI from SCE&G and U.S. Army Corps of Engineers
    - Review of Parking lot items from Gaithersburg meeting or Day 1
    - Initial Phase 2 Schedule Structure
21. 4:15 Review of short term meeting schedule and Post Phase I drafting assignments
22. 4:45 Next Steps and Evaluation
23. 5:00 Adjourn

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Draft Meeting Summary

Cyber Security Order 706 SDT — Project 2008-06

November 12, 2008 | 1–5 p.m.
November 13, 2008 | 8 a.m.–5 p.m.
November 14, 2008 | 8 a.m.–noon
Arkansas Electric Cooperative Corporation Offices
Little Rock, Arkansas

Meeting Facilitation and Draft Report By:
Robert Jones, Stuart Langton, and Hal Beardall

FCRC Consensus Solutions, Florida State University

Thanks to Team members Sharon Edwards and Kevin Perry for their meeting notes.

http://www.nerc.com/filez/standards/Project_2008-06_Cyber_Security.html

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

MEETING SUMMARY CONTENTS

EXECUTIVE SUMMARY

The Chair, and Vice Chair welcomed the members reviewed with the team and participants the proposed meeting agenda and thanked Phil Huff for hosting the meeting at the Arkansas Coop offices. Harry Tom reviewed with the team the need to comply with NERC's Antitrust Guidelines. The team accepted the October draft meeting summary but agreed that it will be open to editorial corrections as necessary.

The team reviewed and unanimously adopted the consensus guidelines which had been revised since the Sacramento meeting to address consistency with the NERC Reliability Standards Development Procedure.

Following discussion, the team unanimously adopted the following SDT purpose statement:

> The team is serving the public interest throughout North America to protect the critical cyber assets that include hardware, software, data, and communications networks essential to the reliable operations of the bulk power system.
>
> The team's outcomes will be achieved by working together to build consensus on a technically sound and complete package of recommended draft cyber security standards and realistic implementation plan that is responsive to and consistent with the scope of the SAR, the FERC Order 706 and the ANSI process.

Following an overview and extensive discussion of how to address the proposed edits by the NERC Standards Process Manager, and a review of specific edits in CIP 00 and 003, the SDT decided to accept agreed upon "global changes" discussed in CIP 002-003 review and reject all other changes reverting back to the final Sacramento language version. Team member Jackie Collett presented CIP 002-009 global revisions, including CIP 006 revisions made by Kevin Perry, for consideration by the team. The team also accepted the Implementation section language as revised on November 13 by the sub-team.

In the review of the Newly Identified Assets Implementation plan the team unanimously agreed to go back to the Sacramento agreed-on approach and have the "newly identified asset" CCA implementation plan as a separate document with no changes in the existing CIP standards documents to be posted for industry comment with Phase 1 documents. Based on comments from Phase I industry review and experience in the field, the SDT will consider incorporation into the standards documents in Phase II. The SDT will ask the industry whether they think it should be incorporated into the CIP standards documents as part of the Phase I submission for vote. Following the poll, Scott Mix made conforming changes in the draft language and the SDT then unanimously agreed to move forward this as a separate paper in Phase 1.

Jeri Domingo Brewer reviewed the SDT sub team's revisions to the comment form based on the revisions to the standards adopted by the team and the SDT unanimously agreed to adopt the Comment Form at part of the Phase 1 documents.

On Friday morning, the SDT Phase I package of documents was moved for adoption and submission to the industry for comment (Mover: Kevin Perry, second: Sharon Edwards). The Phase 1 Package was adopted unanimously without discussion.

The SDT reviewed the Phase II options paper drafted by the facilitators with input from the Chair, Vice Chair and some SDT members. The facilitators presented some initial draft assessment criteria and invited the SDT to clarify, revise or add additional criteria. The facilitators suggested the criteria could help provide a frame for each member to assess the acceptability of the various options for how to proceed. Below is the second draft of the assessment criteria:

SECOND DRAFT PHASE 2 OPTIONS ASSESSMENT CRITERIA
(Not Weighted nor Prioritized)

Initial Draft Criteria as Revised by SDT in November 14 Discussions

A. The option is consistent with the SDT purpose statement and is responsive to the FERC 706 directives and the SAR.
B. The option is achievable given the SDT schedule and work plan.
C. The option does most to advance and enhance cyber security.
D. The option helps the SDT address the foundational issues with the current standards.
E. The option is capable of implementation.
F. The option is capable of improving compliance.

New Criteria Identified by SDT in November 14 Review

G. The option helps protect the current investments and wherever possible builds on what has already been done.
H. The option helps to identify and mitigate risk on an ongoing basis.
I. The option balances a systems orientation with a facilities orientation to asset protection approach. The option is capable of being extended into related interests by others (distribution, AMI, Smart Grid, etc.).
J. The option enables the industry provide the appropriate level of security (not over securing nor under securing the cyber assets).
K. The option allows for discrimination among the various types of infrastructure that supports the BES.

The SDT then discussed, refined and reduced the number of optional approaches to four for consideration. The team ranked the acceptability of four identified options for going forward and then directed the Chair, Vice Chair and facilitators to design the December agenda around the approach receiving the greatest support from team members. Below are the results of that exercise:

PHASE II WORK PLAN OPTIONS IN RANK ORDER
(As identified and ranked by SDT November 14, 2008)

1. Address Risk management first then proceed with the rest

Acceptability Ranking Scale	**4** = acceptable, I agree	**3** = acceptable, I agree with minor reservations	**2** = not acceptable unless major reservations addressed	**1** = not acceptable	**Avg.**
11-14 rank	**9**	**5**	**4**	**0**	**3.27 of 4**

2. Adopt/adapt NIST into CIP or Merge NIST into CIP

Acceptability Ranking Scale	**4** = acceptable, I agree	**3** = acceptable, I agree with minor reservations	**2** = not acceptable unless major reservations addressed	**1** = not acceptable	**Avg.**
11-14 rank	**3**	**9**	**4**	**0**	**2.93 of 4**

3. Revise CIP as directed — leave as is and add in only items identified by FERC order

Acceptability Ranking Scale	**4** = acceptable, I agree	**3** = acceptable, I agree with minor reservations	**2** = not acceptable unless major reservations addressed	**1** = not acceptable	**Avg.**
11-14 rank	**5**	**7**	**7**	**0**	**2.89 of 4**

4. Start Over — in terms of a starting point

Acceptability Ranking Scale	**4** = acceptable, I agree	**3** = acceptable, I agree with minor reservations	**2** = not acceptable unless major reservations addressed	**1** = not acceptable	**Avg.**
11-14 rank	**2**	**5**	**7**	**5**	**2.21 of 4**

Scott Mix reviewed the "Technical Feasibility eight page document with two pages included of questions which were reviewed at the Sacramento meeting. This was modeled after self-reporting mechanism to fit into the existing compliance program. He noted that he would go through a red line version for one more round to send to the SDT for review prior to December. He noted the goal would be to post a paper approved by the team for comment soon after the December meeting. The comment period would overlap with the Phase I period but would last longer.

In reviewing next steps, the SDT reviewed the status of the NERC Phase I communication plan and asked for a presentation at the December meeting. They also reviewed the Phase I schedule and evaluated what worked in Little Rock and what could be improved going forward. The proposed December agenda items included:

- Review elements of communication plan for Phase I
- Technical Feasibility review
- Background on NIST and its application
- Continue discussion of Phase II approach

Members agreed to adjourn at 11:30 a.m. on Friday until the next meeting on December 4–5, 2008 in Washington D.C.

Cyber Security Order 706 Standard Drafting Team
Draft Third Meeting Summary

I. Introductions, Agenda Review and Welcoming Remarks

The Chair, and Vice Chair welcomed the members and asked NERC staff Harry Tom to conduct a roll call of members and participants in the room and on the conference call *(See appendix #2*). They then reviewed with the team and participants the proposed meeting agenda *(See appendix #1*). They also thanked Phil Huff for hosting the meeting at the Arkansas Coop. offices and for making all of the necessary logistical arrangements.

II. Review of Antitrust Guidelines

Harry Tom reviewed with the team the need to comply with NERC's Antitrust Guidelines *(See, Appendix #3)*. He urged the team and other participants in the process to carefully review the guidelines as they would cover all participants and observers. He urged all to avoid behaviors or appearance that would be anti-competitive nature and also reminded the group of the sensitive nature of the information under discussion.

III. Acceptance of Second SDT Meeting Summary

On Wednesday the Chair asked members to review the October draft meeting summary and the team would seek to adopt it on Friday. On Friday the Chair reviewed the minutes from the second meeting. The Chair suggested and the team agreed to accept the minutes as they were distributed, however the minutes will be open to editorial corrections as necessary. The Chair noted that an announcement that the minutes have been posted to the NERC Web site will be sent to members and other participants. It is then the responsibility of the members to download the minutes and review them in advance of meetings.

IV. SDT Consensus Guidelines

The team reviewed the consensus guidelines *(Appendix #5)* which had been revised since the Sacramento meeting to address consistency with the NERC Reliability Standards Development Procedure. The facilitator noted that the consensus process and techniques were designed to produce as close to 100 percent support of the team's final products as possible. The team discussed what level of agreement it should establish for making final decisions on substantive proposals. They agreed that it will be essential to seek as much consensus support among the team of its proposals since the products will be scrutinized and tested by the industry, many of whom may not be cyber security subject matter experts. Some noted that the initial adoption of the voluntary CIP standards was a controversial and challenging process and that the passage of mandatory cyber security standards will be at least as challenging. The team agreed to set its threshold for team decision making at least a supermajority of 75 percent of the SDT members. The Chair pointed out this exceeds the two-thirds vote needed to approve a standard by the ballot body.

The team also agreed to adopt a quorum rule of two-thirds of the team's members present in order to make decisions. This is consistent with the quorum set forth in the NERC rules for the ballot body process. Finally the team agreed to provide a statement consistent with the NERC

procedures that voting may take place in the context of formal SDT meetings or may take place through electronic means. The team unanimously adopted the consensus procedures as revised.

V. SDT Purpose Statement

Mr. Langton noted that the Chair and Vice Chair worked with the facilitators to respond to the range of team comments on the first draft purpose statement reviewed at the Sacramento meeting. The following revised purpose statement was offered for the team's consideration:

> **The team is serving the public interest throughout North America to protect the critical cyber assets that include hardware, software, data, and communications networks essential to the reliable operations of the bulk power system.**
>
> **The team's outcomes will be achieved by working together to build consensus on a technically sound and complete package of recommended draft cyber security standards and realistic implementation plan that is responsive to and consistent with the scope of the SAR, the FERC Order 706 and the ANSI process.**

In the discussion that followed, the team acknowledged the issue of communications networks as part of the range of critical cyber assets that need protection. Some emphasized that the team's focus should be on the data that moves over the system and not just on the facilities in the bulk power system. Following the discussion, the team unanimously adopted the SDT purpose statement.

VI. Review and Adoption of Phase One Products

A. Introduction and Overview of NERC Edits

David Taylor reviewed with the team the process for reviewing the team's draft products. He noted that the Standards Process Manager who works on behalf of the Standards Committee. This review as not intended to be a substantive review of the requirements but a fresh review "from the outside looking in" of the proposed SDT language for the standard requirements and other Phase 1 documents, with an eye towards compliance issues. For example, the term "risk based assessment methodology" may need some clarification and perhaps there is an alternative choice of word, better accepted and understood by all who would be reading this. Team members also felt strongly that the SDT's language: "This standard, in conjunction with the other standards in the set CIP-002 through CIP-009, comprise a cyber security framework for the protection of Critical Cyber Assets supporting the reliable operation of the Bulk Electric System," was critical to the draft and should not be removed as suggested by the NERC Standards Process Manager.

B. Team Review of Procedural Approaches to Reviewing Edits

The team discussed how to address NERC's Standards Process Manager proposed edits of the Phase 1 draft documents the team unanimously adopted at the conclusion of its October 21–22 meeting in Sacramento. Due to tight timeframes, an interim WebEx call scheduled to review the proposed NERC editorial changes was canceled. Many of the team members and sub teams did not have a chance to review the proposed edits in

advance of the meeting. After extensive discussion, the team identified and conducted a poll on the preferred approach to finalizing Phase 1 products.

Proposed Approaches	SDT Preference Poll
1. Review 002-009 spending ten minutes on a section. If not resolved, default to final draft as proposed by SDT. If six or more members reject the proposed edit, we reject the proposed edits go and go on to the next requirements.	**11**
2. Reject NERC Standards Process Manager's Changes	**8**
3. Table the discussion of NERC Standards Process Manager's changes. Focus on Requirements first, then Data Retention. We will not be concerned with boiler-plate standards changes made by NIDR.	**1**
4. Leave Alone - Deal with Implementation Plan and other substantive issues. After we do that we consider NERC Standards Process Manager's changes.	**0**
5. Accept NERC Standards Process Manager's changes	**0**
Total	**20**

The team agreed to utilize the approach to go through CIP-002 and touch each change briefly to determine whether to accept or reject, but then to check on its efficacy in moving through the proposed edits and reviewing new language for other products.

C. Initial Review of CIP 002-003

The team's efforts for the rest of the afternoon addressed whether to accept the range of proposed edits by the NERC Standards Process Manager. A chart reflecting the team's day one decisions is displayed in *Appendix #6.*

D. Agreement on Global Edits and Retention of the SDT Requirements and Measures

Following the Team's review of proposed edits to CIP 002, 003 and part of 006, it decided to conduct a ranking of options in going forward with their review. They tested the support for the two proposals noted below.

Proposal	Initial Straw Poll	
1. Accept agreed upon "global changes" discussed in CIP 002 and 003 review — Reject all other changes. Other than global changes, this reverts all standard language back to Sacramento version	20 Y	4 N

2. Accept global changes plus what was already done on CIP 002 and CIP 003. Reject everything else.	Not passed

Team Comments after Poll

- Concern that we are rejecting the changes we made in 002 and 003; which says something about our process?
- Understand the comment but 2 and 3 are really overall governance standards and we are not comfortable accepting the proposed edits without reviewing and reflecting on all the changes to each section.
- Concerned that some changes in 2 and 3 may impact the others without further review.
- This process was not a waste of time; the team had a good and necessary discussion that sets the stage for future work.
- We went through a necessary exercise and valuable team exercise, we then reflected and adjusted based on the experience.

	2nd Poll	
1. Accept all agreed upon global changes — Reject all other changes and edits proposed by NERC Standards Process Manager. Other than the global changes, this reverts all standard language back to the version adopted at the conclusion of the Sacramento meeting.	23	2
2. Accept global changes plus what was already done on CIP 002& CIP 003. Reject everything else.	*Failed to get enough support*	

Review of Global Edits

Team member Jackie Collett presented CIP 002 through CIP-009 global revisions, including CIP-006 revisions made by Kevin Perry, for consideration by the team.

E. Implementation Plan

Phillip Huff reviewed the SDT sub team's suggested revisions and agreed following comments to meet with the Sub team to address suggestions for revisions.

Comments:

- Did compliant date get changed? The "Introduction" makes clear that compliant date is not important.
- If use effective date in the standards then need to include here for consistency.
- Do we need to spell out the "versions" to avoid confusion?
- Also capitalize "Implementation Plan".
- Version 1 is the original 706 standard use "version one" in () to shorten subsequent references, similar description and use of version two.

- The second paragraph was offered by the sub-team for explanation but can dropped if the language is considered too informal.
- What does "Auditable compliant" mean?
- If compliant with standard on day one then do not need years worth of documentation — semantics — agree with having one date and that it does not mean that you will have one years worth of documents on that date.

Following a sub-team meeting over lunch, Mr. Huff reviewed the change proposed for the effective date.

Comments

- Is this to be inserted in place of specific item or as a global item in all the standards? As a global item in all the standards.
- Place it in the effective date for each standard.
- Both options to be included to offer option — not offered here as to which one to include in the standards.
- Why not say 180 days? NERC wants the compliance dates to line up with quarters to make auditing easier.
- The SDT discussed moving the parenthetical but left in as boilerplate already given to the drafting team. The parenthetical is meant as a clarifier not an alternative — remove the "or" in the parenthetical to clarify?
- Change to capital "Compliant Date"? That means it needs to be in the glossary — leave in lower case.
- Is this the effective date that appears in the footer of the document (XXXX)? No that footer addresses when FERC ultimately approves.
- It would have to be read multiple times to understand.
- The later of: i); or, ii) ….
- Remove "applicable"? Leave in to cover different Canadian jurisdictions.

	Poll of SDT Members	
Accept the Implementation section language as revised on Nov. 13	19	1

Comments following the Poll

- Still confused as to when this could become effective to investor owned utility in the U.S.?
- Possibly the end of next year.
- Note this is not the newly identified asset "implementation" plan.

F. Newly Identified Assets — Implementation Plan

Scott Mix reviewed the suggested revisions noting the new requirement R3.1.

Comments on Proposal

- Is this something we need to move here — identify senior manager — We agreed in Sacramento to include senior manager?
- Should say first calendar "day" of the first quarter.
- If categorization of an asset is now required is it subject to audits? As a requirement the answer is yes but how? Need to give compliance a chance to review.
- Should we be wrapping into the standards as a requirement in Phase 1 as opposed to a white paper for comment? We discussed in Sacramento and agreed to the white paper approach.
- Categorizing the equipment support reliable operation? This is about compliance first, not operations.
- CIP-002 has a new requirement CIP-003 through 009 do not
- Are we asking for a world of hurt by adding additional verbiage? This would add a lot of text to the standards here. Yes, but this is really salient concern in the industry asking us to fix this.
- Suggestion is not to not include it but address it as a separate document rather than embed in the standards
- Give ourselves a waiver under the applicability standard; avoids complications under implementing, and it is still auditable, but allows equipment to avoid compliance for longer period of time.
- How does it get implemented without embedding it? It gets a two-year test run as a separate document and in phase 2 we use the comments and practice and adjust as needed into the standards.
- Separate document makes it clearer what the concept is that is being presented to the industry.
- Give a 180-day waiver to critical and 30-day waiver for non-critical? Time could be adjusted, but it gives industry time to adjust to the concept before implementation.
- Simplicity is appealing but could be wrong — this is a complex issue that needs a complex answer to address multiple permutations — industry will tell us which ones are wrong.

The SDT used a straw proposal acceptability ranking to test support on how to proceed:

Consensus Ranking on options for how to present the "Newly Identified Assets" Implementation plan	**Acceptability Rank**			
A Go back to the Sacramento agreed on approach and have the "newly identified asset" CCA implementation plan as a separate document with no changes in the existing CIP standards documents to be posted for industry comment with Phase 1 documents. Based on comments from Phase I industry review and experience in the field, the SDT considers	**4**	**3**	**2**	**1**

incorporation into the standards documents in Phase II. Ask the industry whether they think it should be incorporated into the CIP standards documents as part of the Phase I submission for vote.	**19**	**2**	**0**	**0**
B. Instead of option A above, address the new assets within the applicability section	**3**	**9**	**8**	**1**
Poll on Support for Proposal A	**Poll**			
Who accepts Proposal A?	21-0			

Comments after the Poll:

- Need to strive for consistency where ever possible; have to look at different parts of the document to understand how to comply.
- We are talking about a phased in implementation.
- Putting into applicability section will lock into format and be more confusing.
- Elegance in simplicity but separate document will offer clearer path to receive and interpret comments.
- Do not think we can boil this issue down to key bullets and be comprehensive enough.
- This is too complex to put into the applicability section; compliance and other issues that do not fit in the applicability section. Review as one document now and then disperse into the standards as needed in Phase II; premature to place it in one place or another until we get comments back.
- Believe it is consistent to put in a separate document for implementation.

Following the poll, Scott Mix made some conforming changes in the draft language for "newly identified assets" white paper and presented to the SDT:

- Reviewed the three categories
- Category 3 is not called out directly in the flow chart
- Category 3 is covered by "compliant upon commissioning"
- Auditable Compliant always follows one-year after compliance
- Added storm restoration to the table — unplanned to get service back up for customers
- The dates are linked to quarters

Comments:

- Do we need to add verbiage to explain intent of this section and its applicability?
- The last sentence in adopted proposal frames the question to be asked in the comment form.
- Might include explanation for the time frames used in the table.

- Concerned about how we deal with constructive ambiguity in a large company formed from multiple former companies — each still operates parts of their grid separately.
- If separate delegated authority then should not have to combine and you may not have a single program but need a common governance program
- Three month time frames may not be enough for a large corporation realistically — change all of the 3's to 6's? Or wait for industry comments? Wait for industry comments.
- Can we use "senior management" for consistency?

The SDT then unanimously agreed to move forward this as a separate paper in phase 1.

G. Comment Form

Jeri Domingo Brewer reviewed the SDT sub team's revisions to the comment form based on the revisions to the standards adopted by the team.

SDT Comments on the Comment Form

- No changes have been made by the sub team — following a review comments from NERC.
- Include list of standards and titles in background to be sure industry understands what is being reviewed.
- Editorial changes included deletion of material from the SAR — trying not to confuse industry on what we are doing in phase I, so the sub team is suggesting deleting material that appears to be related to phase II
- Suggest removing the Requirements section that was added by the sub team
- Under Implementation Plan — make clear what the two different implementation plans are trying to do.
- Added to question about what they do not like the request for suggestions to address the concern — may adopt in other standards comment forms too.
- Keep language about intent to educate the industry on what we mean now and in future phases
- Clarify whether the implementation plan only in play during the transition from version 1 to version 2?
- Since we got rid of the second implementation plan, then related language here is no longer needed.
- Footnotes here are helpful in explaining the intent. Check whether the Footnotes work in the new "checkbox" software? May have to use (parenthetical) form.
- Ask Scott Mix and Phillip Huff to come up with questions for the critical asset identification and the effective date respectfully.

The sub-team agreed to review and present a proposal a revised version of the Comment Form before the vote on the Phase 1 package and products. On Friday, Jeri reviewed with the SDT the minor corrections to clarify language on the comment form that included key questions from the Implementation Plan document and from the "newly

identified assets document." The SDT unanimously agreed to adopt the Comment Form at part of the Phase 1 documents.

H. Adoption of Phase 1 Package

On Friday morning, the SDT Phase I package of documents was moved for adoption and submission to the industry for comment (Mover: Kevin Perry, second: Sharon Edwards). The Phase 1 Package was adopted unanimously without discussion.

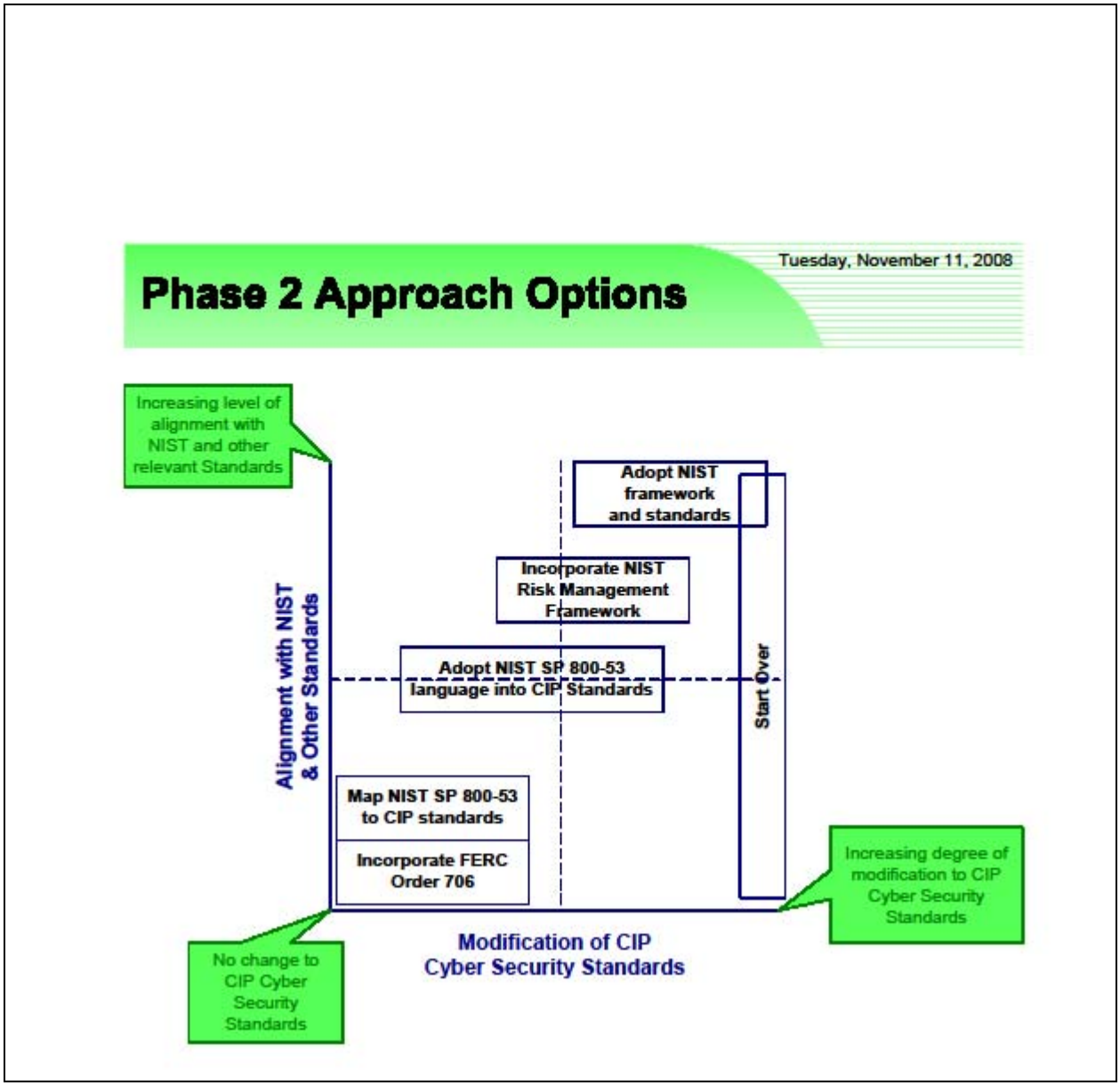
Phase 1 Package of Documents	Adoption Vote	
Phase I Document Motion to Adopt *(Mover, Kevin Perry, Second, Sharon Edwards)*.	21	0

VII. INITIAL REVIEW OF PHASE II APPROACH

A. Review of the Facilitators' Phase II Options Paper

The SDT at its first two meetings discussed how to develop a clear roadmap for how it would engage on the issues and products in Phase II. At the conclusion of the Sacramento meeting, the Chair asked the facilitator to develop an options paper for review at the Little Rock meeting following the adoption of the Phase I package. During an interim WebEx call, the Chair invited any member to send any thoughts on the options to the facilitators. The facilitators received comments and suggestions on approaches and options from John Varnell, Bryan Singer and William Winters and worked closely with the Chair and the Vice Chair in producing the options white paper *(See Appendix # 7)*.

The paper suggested there is a foundational issue concerning the relative merits of the CIP and NIST (and other) cyber security standards that should be addressed for several reasons. One reason is the attention that FERC Order 706 gives to this issue (*See Appendix # 9)*; second it raises questions about the basic paradigm that NERC uses in standards development and oversight; and third, how this matter is addressed by the SDT will influence how it may address many other issues raised in FERC Order 706. For these reasons, the paper suggested the next item on the SDT agenda at the conclusion of submitting the Phase I document will be a review of the CIP cyber security standards in relation to relevant standards developed by NIST and others. A diagram was offered to graphically describe a way to chart the options presented for Phase II.



SDT Initial Comments on the Phase II Options Paper:

- Option E is probably not acceptable under the NERC standards development process.
- We are on risky ground adopting a NIST risk management framework because it allows the entity to accept risk. FERC has stated that is not acceptable.
- NIST has a process for identifying risks that are very difficult to contain and a process to gradually work your way out of that situation. We need to have that discussion with FERC.

- Problem with current standards is that the acceptance of risk was decoupled from risk assessment.
- The FERC order is regulatory law and we cannot decide to ignore and go another direction.
- Missing link: FERC said to look at FISMA/NIST. FIPS 199/200 looks at risk profile. Things are different between the datacenter and the field sites. What is missing is "how much do I really need to worry about this?"
- We have got to do something about the cherry-pick approach to security found in the current standards.
- Need to group of all the issues to best determine the best approach for tackling them. Perhaps putting together multiple spreadsheets and sources of those issues.
- Note there are many suggestions in the SAR for process development aimed at NERC rather than the drafting team.
- For the SDT Scope, are we relying here only SAR 706? Are we only focusing on the FERC 706 order for our decision?
- Our charge is to consider all of the options from doing nothing to complete adoption of the NIST framework — the strawman is to test multiple options for responding to FERC
- The last two options (E and F) mention discarding — that is probably too harsh
- Also not adopting but will be adapting NIST into CIP?
- SAR notes the SDT can and perhaps should reassess everything
- E — Adopting NIST framework — does not meet the NERC process and is not allowed — adapting it may be a severe form of option C.
- F may be where FERC directive asks us to go but keep in mind that the original 15799 was the framework for the 1200 standard the industry started with and long since moved past.
- Has FERC told us the direction but also indicated that the direction is not acceptable — need to manage expectations based on risk assessment directions in the SAR
- Last two options have problems for adopting them in terms of responding to FERC.
- Acceptance of Risk — 706 language developed by lawyers and substance people may not be happy — we have to make it happen practically — process for easing our way out of the problem — FERC may be trying to "have their cake and eat it too"
- This would require a massive funding of a new system — need to practically work toward a more acceptable method of getting out of the problem developed over the past 100 years — FERC can not have it both ways
- Do not assume FERC is adverse to risk acceptance if we can show a practical way of addressing the issue.
- We have no choice to follow what is in the order regarding the CIP standards unless a contravening order is issued — it is the current law.

- Can comment within the law — just setting foundation for addressing additional issues beyond phase I
- Several of the options presented seem to overlap and say some of the same things — need not to bog down in discussing this and need to move on to meatier matters of substance.
- Look to NIST to see if there is anything we can approve — one issue is the residual risk — figure out your risk profile or impact — need levels of gradation of risk as a target — same goes for facilities, some more vulnerable or have a bigger impact — NIST framework helps address these two sets of gradation
- Commend facilitators for capturing the essence of the issue in the options to get us through the discussion to set the framework for dealing with the issues
- Today we "cherry pick" the issues in cyber security with a focus on what should not be covered — we have to figure out how to deal with this under any of the options offered.
- Not identifying new standards but to look at cyber security as it relates to bulk power production, not try to do everything
- We may not have a good concurrence on the scope of what we are being asked to do — the criteria help us focus on what needs to be considered — is there any support for throwing out the system and starting over?

B. Review of Draft Assessment Criteria

The facilitators presented some initial draft assessment criteria (*See Appendix #8)* and invited the SDT to clarify, revise or add additional criteria. The facilitators suggested the criteria could help provide a frame for each member to assess the acceptability of the various options for how to proceed. The criteria also offer an initial opportunity for the SDT to discuss key issues related to how to proceed. The facilitators noted that the mechanics of the proposed review process will include looking at each option to identify the pros/cons of each on its merit *(see Appendix # 8),* then ranking each option for acceptability and ending up with list ranked from top to bottom in terms of acceptability. The SDT could look at lower ranked options and see if anything is worth retaining or incorporating into the most acceptable framework option.

SDT Comments on Draft Criteria

- Suggest decoupling E between implementation and compliance and making this two criteria.
- Are these weighted for relative importance between the criteria? No. Enhancing cyber security should be given a higher weighting
- Goes to how we use these criteria — intended for guiding discussion not a formal formula for scoring each option
- Corollary to D — does the option do the most for advancing the reliability of the bulk power system? That is the object of ensuring cyber security
- Does it protect the investment we have already made in adhering to the CIP standards? — dollars or economic question — builds on what we have already done

- Which option best addresses the foundational issues? Foundational issues includes risk assessment is never done in the current system; also everything such as people and facilities are seen from a box — brainstorm a list of the key foundational issues — something is either critical or not, no gradation
- How does the option identify and mitigate the risk? Option that does the most to identify and mitigates risk.
- Which approach allows to extend into related issues — smart grid with new standards, distribution automation, etc. — from electronic systems view, being able to hack into system versus physical access to a facility — we are the most central system, other systems are looking to us for a model
- Possible criteria: "Does not drive industry to overly secure"
- This is not a one size fits all approach to assessing and securing risk, E.g. the impact on rural farm areas is different than impact on key urban facilities. This requires different assessments and levels of attention.
- Trying to protect bulk power system not the distribution (if not with in the production system)
- Will help if we move FAQs out as guidance to get them the attention they need for clarifying issues.
- Different types of bulk system production requires different levels of protection — vary in types of risk to be addressed
- C in CIP is not "cyber" but "critical" infrastructure protection. Need to stick with cyber security — it is in the Team's title.
- We are looking at the strategy for addressing issues in phase II, not the scope — that was developed by the SAR team, with flexibility for how to address the issues
- Drop off options that are not designed to significantly address issues identified in SAR
- F — double weights other criteria — "If expensive then it would not be supported by ballot,."
- Need to use a risk analysis process — that would help us to focus.
- "Support at ballot" is not a good criteria — no changes at all would be the most supportable at the ballot — need to keep in mind that we are protecting the bulk electric system and the focus is on cyber security
- To move forward there may be too many options and criteria for weighing and judging among them — also some of the answers to the criteria questions may be too subjective.

SECOND DRAFT PHASE II OPTIONS ASSESSMENT CRITERIA
(Not Weighted nor Prioritized)

Initial Draft Criteria as Revised by SDT in November 14 Discussion

D. The option is consistent with the SDT purpose statement and is responsive to the FERC 706 directives and the SAR.
E. The option is achievable given the SDT schedule and work plan.

F. The option does most to advance and enhance cyber security.
L. The option helps the SDT address the foundational issues with the current standards.
M. The option is capable of implementation.
N. The option is capable of improving compliance.

New Criteria Identified by SDT in November 14 Review

O. The option helps protect the current investments and wherever possible builds on what has already been done.
P. The option helps to identify and mitigate risk on an ongoing basis
Q. The option balances a systems orientation with a facilities orientation to asset protection approach. The option is capable of being extended into related interests by others (distribution, AMI, Smart Grid, etc.).
R. The option enables the industry provide the appropriate level of security (not over securing nor under securing the cyber assets).
S. The option allows for discrimination among the various types of infrastructure that supports the BES

C. Review and Ranking of Optional Phase II Approaches

The SDT then discussed refining and reducing the number of optional approaches to consider and rank:

SDT Comments on Approaches

- We need to tackle risk assessment first — everything else follows CIP 002 — that will drive the rest of the options — CIP 2 is not cyber security but is risk assessment
- Options: A is a must do, FERC will use as a check list and if not addressed then will shot us down and say start over; but other options may follow question on CIP 2 — look at NIST to see what it says about each issue, NIST stuff is not copyrighted and we can steal as needed
- A, B, C and some of D — the right approach is an amalgam of the options with A as the lead or preliminary discussion
- How much alignment do we have to start with? The groupings can be realigned — are we to fill the worksheet out for the next meeting? Group into three options and see where we fall as group — are we aligned or not — where on the graphic do we fall as a team?
- The question is where to start? The industry is about producing electricity — we are different — is it a facilities oriented framework or a systems oriented framework? - is it a physical asset protection or information system protection? Do we start with NIST framework and ask what is the right thing to do, checking with the 706 spreadsheet of issues? Or do we continue to cherry pick with current standards? Start with NIST mindset or CIP mindset?
- CIP has a huge acceptability in the industry to start with. What percentage of the CIP standards are acceptable to FERC? Offers a head start over the NIST standards.

- Do we need a broader discussion of risk assessment before discussing the framework?
- Is everyone familiar enough with NIST to assess its value as a starting framework?
- Concerned with setting to narrow a solution for guiding the discussion — need to look at the overall risk to be addressed first — previously we found a solution and fit the problem to it
- We need to look at the FERC order — want us to fix the standards, not replace them or start over — identified the things we need to fix — can look to NIST to see if it fixes particular problems
- Question on process — living with CIP standards and only read NIST standards in one day — need to take a deeper dive into NIST before deciding — utilize experience at the table as to how both are applied

The Chair suggested and SDT agreed to "test the team's pulse" by ranking the acceptability of four identified options for going forward and then to design the December agenda around the approach receiving the greatest support from team members. Below are the results of that exercise:

PHASE II WORK PLAN OPTIONS IN RANK ORDER
(As identified and ranked by SDT November 14, 2008)

1. Address Risk management first then proceed with the rest

Acceptability Ranking Scale	*4 = acceptable, I agree*	*3 = acceptable, I agree with minor reservations*	*2 = not acceptable unless major reservations addressed*	*1 = not acceptable*	*Avg.*
11-14 rank	**9**	**5**	**4**	**0**	**3.27 of 4**

2. Adopt/adapt NIST into CIP or Merge NIST into CIP

Acceptability Ranking Scale	*4 = acceptable, I agree*	*3 = acceptable, I agree with minor reservations*	*2 = not acceptable unless major reservations addressed*	*1 = not acceptable*	*Avg.*
11-14 rank	**3**	**9**	**4**	**0**	**2.93 of 4**

3. Revise CIP as directed — leave as is and add in only items identified by FERC order

Acceptability Ranking Scale	*4 = acceptable, I agree*	*3 = acceptable, I agree with minor reservations*	*2 = not acceptable unless major reservations addressed*	*1 = not acceptable*	*Avg.*
11-14 rank	**5**	**7**	**7**	**0**	**2.89 of 4**

4. Start Over — in terms of a starting point

Acceptability Ranking Scale	*4 = acceptable, I agree*	*3 = acceptable, I agree with minor reservations*	*2 = not acceptable unless major reservations addressed*	*1 = not acceptable*	*Avg.*
11-14 rank	**2**	**5**	**7**	**5**	**2.21 of 4**

The Chair agreed to plan for the December agenda with this in mind.

VIII. TECHNICAL FEASIBILITY

Scott Mix reviewed the "Technical Feasibility" eight page document with two pages included of questions which were reviewed at the Sacramento meeting. This was modeled after self-reporting mechanism to fit into the existing compliance program. He noted that he would go through a red line version for one more round to send to the SDT for review prior to December. He noted the goal would be to post a paper approved by the team for comment soon after the December meeting. The comment period would overlap with the Phase I period but would last longer.

SDT Comments on Technical Feasibility

- Purpose is because "reasonable business" not stricken yet and this is set for audits after June 1

IX. NEXT STEPS AND EVALUATION

A. NERC Phase One Communication Plan

The Chair asked whether NERC was developing a communication strategy for supporting this project. Dave Taylor noted he was still working with Gerry Adamski to develop the strategy and that they hope to have something ready to present at the December meeting. The Chair noted she prefers to have a session with the industry as soon after posting the package as possible to ensure they have the information they need before commenting. Mr. Taylor agreed to have a NERC presentation on the plan at the December SDT meeting.

B. Review of Phase I Schedule

Dave Taylor reviewed the potential schedule to complete the Phase I process by the end of June 2009. He noted the concerns that times are tight but noted the schedule provides very limited flexibility to extend the comment time — if we do so it extends the end of the time line into the middle of July.

SDT Comments:

- Changing the time frame will not help much — extending the time will not change how people vote.
- Important from a perception point to get this in on time to FERC — getting in after date may show too little concern for their directives— NERC and industry are under the gun.
- To do a realistic quality job and seriously respond to comments the schedule proposed gives us a defensible position that this is complicated and needs more than eighteen months — The Phase I experience will show FERC why it takes more time.
- Is this the fast track process promised by NERC CEO or is this the same process trying to go faster? No, this is not the fast track process.
- Holidays leaves people the first weeks of December to comment and we will offer WebEx explanation after first week? The comment period ends in early January just before the scheduled Phoenix SDT meeting.
- Credibility with FERC is important — need to meet the deadline is important
- Need to do the best we can to get the message out and input back but within the time deadline — set a conference call to discuss the communication plan
- Schedule offered, with three comment periods, Phase II ends April 2011 — draft subject to discussion to follow on proposals for concept approach to Phase II

C. December Meeting Agenda Review

NERC announced that the next meeting will take place in law office in downtown Washington, D.C. downtown and will be a two day format from 8 a.m.–5 p.m. on day one and from 8 a.m.–3 p.m. on day two to allow for travel out on a Friday.

The proposed agenda items include:

- Review elements of communication plan for Phase I,
- Technical Feasibility review,
- Background on NIST and its application, and

- Continue discussion of Phase II approach.

D. SDT Meeting Evaluation — What Worked and What Could Be Improved?
At the conclusion of the meeting, the facilitators asked the team to offer an evaluation of the process including what worked well during the meeting and what could be improved.

What worked?

- AECC is a GREAT meeting facility (Thanks to Phillip)
- Quick polls
- Attitude of the group as a whole very good and productive
- Like idea of breaking into sub-teams for editing documents
- Best meeting so far to participate in by WebEx
- Learned from SDT mis-direction and bounced back
- Came up with an edit rejection method for use while editing text
- Building arsenal of processes and when to use them
- Several team members stepped up and did a lot of extra effort
- Rich distinguished between "its" and "the" — the devil is in the detail and haste makes waste
- Everyone is not bashful about speaking up
- Devil is in the details — got to get it right — avoided temptation to rush to quickly past the details that make a huge impact.

What could be improved?

- Need a UBS for meeting rooms in the future
- Take opportunity to take straw polls sooner to keep us moving
- Bogged down
- Veered from time table
- Confusion over consensus procedures and use of parliamentary procedures and Robert's Rules
- Need tighter oversight from the facilitators. Facilitators could help us more avoid unintended discussions and detours
- Did not get a draft of the Communications Plan from NERC in advance as promised
- Need to have drafts available before meetings
- WebEx master needs to have all documents ahead of time

Other Comments

- Assumed NERC review would be tech-writing format only
- Need pre-review opportunity for NERC edited documents
- Frustration over the process but it is a good thing to realize decisions are hard but need to deal with issue
- Did not get a draft of communications plan as promised
- Making sure long edits are available prior to the meeting
- Help if WebEx has documents ahead of time

- Pre agreement for the process to deal with documents is helpful
- Gap in process — assumed NERC review would be a limited review — turned out to be much more extensive — would have been helpful to have an opportunity to review ahead of time — lack of opportunity to see and address ahead of time
- Appreciate the efforts of Scott and Jackie and others who committed extra time to help us move forward
- Sub teams stepped up and efforts were appreciated
- Important for everyone to speak up and we need to stop and pay attention when needed
- What matters are the words that make it onto the paper not just what we think they mean — others outside the room will read without the underlying discussion — need words to accurately communicate what we mean
- Thank you to Phillip again for hosting

Members agreed to adjourn at 11:30 a.m. on Friday until the next meeting on December 4–5, 2008 in Washington D.C.

Appendix # 1
Meeting Agenda
Cyber Security Order 706 SDT — Project 2008-06

November 12, 2008 — 1–5 p.m. EST
November 13, 2008 — 8 a.m.–5 p.m. EST
November 14, 2008 — 8 a.m.–noon EST
Little Rock, AK

Wednesday	**November 12, 2008**
1:00 p.m.	Welcome and Opening Remarks- Jeri Domingo-Brewer and Kevin Perry
1:05	Roll Call — Harry Tom
1:10	Review NERC Antitrust Compliance Guidelines — Harry Tom
1:15	Adopt October 22 Meeting Summary and Review of Meeting Objectives — Bob Jones
1:20	Organizational Issues — Stuart Langton ▪ Review of Work-plan ▪ Adopting the SRT Consensus Guidelines ▪ SRT Purpose Statement
2:00	Phase I Products Review and Refinement
3:00	Break
3:15	Phase I Products- Review and Refinement
5:00	Observer Comments and Suggestions
5:15	Summary of Day One Outcomes and Review of Day Two Agenda
5:30	Recess
Thursday November 13, 2008	
8:00	Welcome and Agenda Review
8:10	Phase I Products — Refinements and Straw Polls
10:00	Break
10:15	Phase I Produces — Refinements and Straw Polls
12:00	Working Lunch
1:00	Phase I Products — Refinements and Straw Polls
3:00	Break
3:15	Phase I Products Refinements and Straw Polls
5:00	Adoption of Phase I Products
5:15	Summary of Day Two Outcomes and Review of Day Three Agenda
5:30	Recess
Friday November 14, 2008	
8:00	Welcome and Agenda Review
8:10	Phase II Work-plan Review and Discussion — Review of Concept(s) Submitted and Straw-man
9:00	Phase II Discussion of Foundational Assumptions, Approach and Expectations
10:00	Break
10:15	Phase II Ranking and Discussion of Optional Approaches
11:30	Assignments, Next Steps, and Review of Work plan
12:00	Adjourn

Appendix # 2

Cyber Security for Order 706 Standard Drafting Team and Attendees List
Project 2008-06 — CS 706 SDT

Little Rock, Arkansas
November 12–14, 2008

Attending in Person — Team Members

1 **Jeri Domingo-Brewer, Chair**	U.S. Bureau of Reclamation
2. Jackie Collett	Manitoba Hydro
3. Jay S. Cribb	Information Security Analyst, Principal, Southern Company Services, Inc.
4. Sharon Edwards	Project Manager, Duke Energy
5. Scott Fixmer	Senior Security Analyst Exelon Corporate Security, Exelon Corp.
6. Gerald S. Freese	Director, Enterprise Information Security America Electric Power
7. Philip Huff	Arkansas Electric Cooperative Corporation
8. Richard Kinas	Orlando Utilities Commission
9. John Lim	CISSP, Department Manager, Consolidated Edison Co. of New York
10. David Norton	Policy Consultant, CIPEnergy Corporation
11. **Kevin B. Perry, Vice Chair**	Director, IT-Infrastructure, Southwest Power Pool
12. David S. Revill	Georgia Transmission Corporation
13. Scott Rosenberger	Luminant Energy
14. Kevin Sherlin	Sacramento Municipal Utility District
15. Michael Winters	Arizona Public Service Co.
1. David Taylor	NERC
2. Harry Tom	NERC
4. Scott R. Mix	NERC
5. Todd Thompson	NERC
6. Hal Beardall	FSU/FCRC Consensus Center (November 13 & 14)
7. Robert Jones	
8. Stuart Langton	FSU/FCRC Consensus Center

SDT Team Members Attending via WebEx/Phone

1. Joe Doetzl	Manager, Information Security, Kansas City Power & Light Co.
2. Tom Hoffstetter	Midwest ISO, Inc *(November 13 and 14 only)*
3. Christopher A. Peters	ICF International *(November 12 and 14 only)*
4. Jonathan Stanford	Bonneville Power Administration
5. John D. Varnell	Technology Director, Tenaska Power Services Co.
6. William Winters	Hydro One Networks, Inc.

SDT Team Members Unable to Attend or Participate by WebEx

1. Bryan L. Singer	Kenexis
2. Keith Stouffer	National Institute of Standards & Technology

Attending in Person — Participants

1. John McGlynn	PJM
2.	Arkansas?

Attending via WebEx — Participants

6. Matt Schnell	Nebraska Public Power District
7. Karen Yoder	First Energy

Appendix # 3
NERC Antitrust Compliance Guidelines

I. General

It is NERC's policy and practice to obey the antitrust laws and to avoid all conduct that unreasonably restrains competition. This policy requires the avoidance of any conduct that violates, or that might appear to violate, the antitrust laws. Among other things, the antitrust laws forbid any agreement between or among competitors regarding prices, availability of service, product design, terms of sale, division of markets, allocation of customers or any other activity that unreasonably restrains competition.

It is the responsibility of every NERC participant and employee who may in any way affect NERC's compliance with the antitrust laws to carry out this commitment.

Antitrust laws are complex and subject to court interpretation that can vary over time and from one court to another. The purpose of these guidelines is to alert NERC participants and employees to potential antitrust problems and to set forth policies to be followed with respect to activities that may involve antitrust considerations. In some instances, the NERC policy contained in these guidelines is stricter than the applicable antitrust laws. Any NERC participant or employee who is uncertain about the legal ramifications of a particular course of conduct or who has doubts or concerns about whether NERC's antitrust compliance policy is implicated in any situation should consult NERC's General Counsel immediately.

II. Prohibited Activities

Participants in NERC activities (including those of its committees and subgroups) should refrain from the following when acting in their capacity as participants in NERC activities (e.g., at NERC meetings, conference calls and in informal discussions):

- Discussions involving pricing information, especially margin (profit) and internal cost information and participants' expectations as to their future prices or internal costs.
- Discussions of a participant's marketing strategies.
- Discussions regarding how customers and geographical areas are to be divided among competitors.
- Discussions concerning the exclusion of competitors from markets.
- Discussions concerning boycotting or group refusals to deal with competitors, vendors or suppliers.

III. Activities That Are Permitted

From time to time decisions or actions of NERC (including those of its committees and subgroups) may have a negative impact on particular entities and thus in that sense adversely impact competition. Decisions and actions by NERC (including its committees and subgroups) should only be undertaken for the purpose of promoting and maintaining the reliability and adequacy of the bulk power system. If you do not have a legitimate purpose consistent with this objective for discussing a matter, please refrain from discussing the matter during NERC

meetings and in other NERC-related communications.

You should also ensure that NERC procedures, including those set forth in NERC's Certificate of Incorporation and Bylaws are followed in conducting NERC business. Other NERC procedures that may be applicable to a particular NERC activity include the following:

- Reliability Standards Process Manual
- Organization and Procedures Manual for the NERC Standing Committees
- System Operator Certification Program

In addition, all discussions in NERC meetings and other NERC-related communications should be within the scope of the mandate for or assignment to the particular NERC committee or subgroup, as well as within the scope of the published agenda for the meeting.

No decisions should be made nor any actions taken in NERC activities for the purpose of giving an industry participant or group of participants a competitive advantage over other participants. In particular, decisions with respect to setting, revising, or assessing compliance with NERC reliability standards should not be influenced by anti-competitive motivations.

Subject to the foregoing restrictions, participants in NERC activities may discuss:

- Reliability matters relating to the bulk power system, including operation and planning matters such as establishing or revising reliability standards, special operating procedures, operating transfer capabilities, and plans for new facilities.
- Matters relating to the impact of reliability standards for the bulk power system on electricity markets, and the impact of electricity market operations on the reliability of the bulk power system.
- Proposed filings or other communications with state or federal regulatory authorities or other governmental entities.
- Matters relating to the internal governance, management and operation of NERC, such as nominations for vacant committee positions, budgeting and assessments, and employment matters; and procedural matters such as planning and scheduling meetings.

Any other matters that do not clearly fall within these guidelines should be reviewed with NERC's General Counsel before being discussed.

Appendix # 4 Phase I Products

Below is a link to all of the documents reviewed by the SDT including final Phase I products with both clean and red-lined versions agreed to during the full Team discussions in Little Rock:

http://www.nerc.com/filez/standards/Project_2008-06_Cyber_Security-RF.html

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Appendix # 5 SDT Consensus Guidelines

Adopted Unanimously, November 13, 2008

Cyber Security for Order 706 Standard Drafting Team

Draft Consensus Guidelines

CONSENSUS DEFINED

Consensus is a **process**, **an attitude and an outcome**. Consensus processes can produce better quality more informed products.

A. Consensus is a problem solving process in which all members:

1. Jointly distinguish their concerns
2. Educate each other
3. Jointly develop alternatives and then
4. Adopt recommendations everyone can embrace or at least live with.

In a consensus process, members can honestly say:

- I believe that other members understand my point of view
- I believe I understand other members' points of view
- Whether or not I prefer this decision, I support it because it was arrived at openly and fairly and because it is the best solution for us at this time

B. Consensus as an attitude provides that each member commits to work toward agreements that meet their own and other member needs and that all can support the outcome.

C. Consensus as an outcome means that agreement is reached by all members or by a significant majority of members. The level of enthusiasm for the agreement may not be the same among all members on any issue, but on balance all should be able to live with the overall package. **Levels of consensus** can include:

- Participants strongly support the solution
- Participants can "live with" the solution
- Some participants do not support the solution but agree not to veto it.

DRAFT CONSENSUS GUIDELINES

The Cyber Security for Order 706 Standard Drafting Team (Team) will seek consensus on its recommendations for any revisions to the CIP standards.

General consensus is a participatory process whereby, on matters of substance, the members strive for agreements which all of the members can accept, support, live with or agree not to oppose. In instances where, after vigorously exploring possible ways to enhance the members' support for the final package of recommended revisions, and the Team finds that 100% acceptance or support of the members present is not achievable, final consensus recommendations will require at least 75% favorable vote of all members present and voting. This super majority decision rule underscores the importance of actively developing consensus throughout the process on substantive issues with the participation of all members. In instances where the Team finds that even 75% acceptance or support is not achievable, the Team's report will include documentation of any differences as well as the options that were considered for which there was greater than 50% support from the Team.

The Team will develop its recommendations using consensus-building techniques with the leadership of the Chair and Vice Chair and the assistance of the facilitators. Techniques such as brainstorming, ranking and prioritizing approaches will be utilized. The Team's consensus process will be conducted as a facilitated consensus-building process. Team members, NERC staff and facilitators will be the only participants seated at the table. Only Team members may participate in consensus ranking or vote on proposals and recommendations. Observers/members of the public are welcome to speak when recognized by the Facilitator and all written comments submitted on the comment forms will be included in the Team and facilitators' summary reports.

The Team will make decisions only when a quorum is present. A quorum shall be constituted by at least 51% of the appointed members being present (simple majority). The Team will utilize Robert's Rules of Order *(as per the NERC Reliability Standards Development Procedure),* as modified by the Team's adopted procedural guidelines, to make and approve motions; however, the 75% supermajority voting requirement will supersede the normal voting requirements used in Robert's Rules of Order for decision making on substantive motions and amendments to motions. In addition, the Council will utilize their adopted meeting guidelines for conduct during meetings. The Council will make substantive recommendations using their adopted facilitated consensus-building procedures, and will use Robert's Rules of Order only for formal motions once a facilitated discussion is completed.

The presiding chair and/or Facilitator of the SDT, in general, should use parliamentary procedures set forth in Robert's Rules of Order, as modified by Council's adopted procedural guidelines.

To enhance the possibility of constructive discussions as members educate themselves on the issues and engage in consensus-building, members agree to refrain from public statements that may prejudge the outcome of the Team's consensus process. In discussing the Team process with the media, members agree to be careful to present only their own views and not the views or statements of other participants and/or may direct such inquiries to the Team Chair and Vice Chair. In addition, in order to provide balance to the Team process, members agree to represent and consult with their stakeholder interest group.

MEETING GUIDELINES FOR PARTICIPANTS

Participants' role in meetings:

- Explore possibilities
- Listen to understand (Respect) (limit sidebar conversations)
- Be focused and concise. (Avoid repetition. No need to offer comments in "strong agreement.")
- Focus on issues, not personalities.
- Offer options to address others' concerns.
- No sidebars.
- If participating by phone, indicate who is speaking.
- If participating by phone, please use the mute button. **Do not** put the phone on hold.

Facilitators and Staff role in meetings:

- Assist the Chair and Vice Chair in helping the Team stay on task
- Help the group follow agreed upon ground rules
- Design the meeting and problem solving process in consultation with the Chair and Vice Chair
- Facilitate discussion participation of the Team and other participants
- Prepare agenda packets and reports

CONSENSUS BUILDING TECHNIQUES

- **Brainstorming** (green light thinking — not judgmental) At certain points, the facilitator may ask the group to suspend judgment and get ideas onto the table before debating.

- **Name Stacking in Team Discussions** (use of name tents to seek attention)

- **Acceptability Consensus Ranking Scale**
  - Use a consensus acceptability scale to help focus discussion and test support in reviewing substantive issues.
  - Use to guide and focus discussion and as a poll to see where the Team stands, not used as a voting mechanism.
  - Must be prepared to offer refinements and suggestions to address serious concerns.

  4 = Proposal is acceptable as it is
  3 = Proposal is acceptable; I can live with it but there are minor concerns to address
  2 = Proposal is not acceptable. Proposal may be acceptable if the major concerns are addressed
  1 = Proposal is not acceptable

- **Consensus Ranking Scale**
  4. Comfortable — I support proposal as is ♥♥♥♥
  3. Minor Reservations — I can live with this; but would like to see changes as follows♥♥♥ Be prepared to offer specific refinements or changes to address your

concerns.

2. Major Reservations — I can't support this unless following changes are addressed to meet my serious concerns ♥♥ Be prepared to offer specific refinements or changes to address your concerns.
1. Fatal Flaws — I can't support this ♥ Be prepared to offer alternatives and options that would address your own as well as other's concerns.

- **Robert's Rules of Order and Facilitated Consensus Building Procedures**
  The Council will make substantive recommendations using their adopted facilitated consensus-building procedures, and will use Robert's Rules of Order only for formal motions once a facilitated discussion is completed.

Appendix # 6
Day One NERC Edit Review

CIP-002 November 13	# of Members Not Accepting NERC Edits (6 o more= reject edit)	Accept/Reject
Introduction A.3 Purpose Edits	**20** (16/4 ph)	Reject
A.4 Regional Entit~~ies~~y	**20** (16/4 ph)	Reject but make "Entity"
B. Requirements Delete Preamble	**1** (1/0 ph)	Accept
R1 Edits	**7** (5/2 ph)	Reject
R1-4 Edits - Delete Titles	**6** (5/1 ph)	Reject
R2 Edits	**10** (8/2 ph)	Reject
R3 Edits, delete ~~the~~, substitute its	**2** (2/0 ph)	Accept
R3 Edits- delete examples	**2** (2/0 ph)	Accept
R3 other edits	**12** (12/0 ph)	Reject
R4 Edits- including deletions and footnote	**10** (8/2 ph)	Reject
R4 Delegate~~'s~~ Delete 's	**2** (2/0 ph)	Accept
C. Measures - Delete preamble/intro	**2** (1/1 ph)	Accept
M1 Edits	**2** (2/0 ph)	Accept
M2 Edits	**2** (2/0 ph)	Accept
M3 Edits	**1** (1/0 ph)	Accept
M4 Edits including delete "of annual"	**1** (0/1 ph)	Accept
D. Compliance		
1.1-1.3 Edits *Global to all CIP requirements*	**0 (**0/0)	Accept
1.4.1 Edits	**0 (**0/0)	Accept
1.4.2 Edits	**14(**13/1 ph)	Reject
1.5.1 Edits *Global to all CIP requirements*	**0 (**0/0 ph)	Accept
D.2. Delete/add "violation severity levels"	**1** (1/0 ph)	Accept
Version History- NERC to revise consistent with changes above		Accept

CIP-003 November 13	# of Members Not Accepting NERC Edits (6 or more= reject edit)	Accept/Reject
Introduction A.3 Purpose Edits GLOBAL	**20** (16/4 ph)	Reject
A.4 Regional Entit~~ies~~y GLOBAL	**20** (16/4 ph)	Reject but make "Entity"
B. Requirements Delete Preamble	**1** (1/0 ph)	Accept
R1, Delete "Identifies" add "represents"	**7** (7/0 ph)	Reject
R1-6 Edits- Delete Titles	**6** (5/1 ph)	Reject
R3 Edits,	**10** (10/0 ph)	Reject
R3.1	**7** (7/0 ph)	Reject
R3.2	**7** (7/0 ph)	Reject
R3.3	**8** (8/0 ph)	Reject
R4 Edits	**20** (16/4 ph)	Reject
CIP- 003	# of Members Not Accepting NERC Edits (6 or more= reject edit)	Accept/Reject

R4 Edit, delete ~~the~~, substitute its	**2** (2/0 ph)	Accept
R5 Edits, delete ~~the~~, substitute its	**2** (2/0 ph)	Accept
R5.1	**2** (2/0 ph)	Accept
R5.1.1	**0** (0/0 ph)	Accept
R51.2	**0** (0/0 ph)	Accept
R5.3 Edit, delete ~~the~~, substitute its	**0**(0/0 ph)	Accept
C. Measures- Delete preamble/intro	**2** (1/1 ph)	Accept
M1-6 Edits	**1** (1/0 ph)	Accept
M4 Edits including delete "of annual"	**1** (0/1 ph)	Accept
D. Compliance		
1.1-1.3 Edits *Global to all CIP requirements*	**0 (**0/0)	Accept
1.4.1 Edits	**0 (**0/0)	Accept
1.4.2 Edits	**14(**13/1 ph)	Reject
D.2. Delete/add "violation severity levels"	**1** (1/0 ph)	Accept
Version History- NERC to revise consistent with changes above		Accept

CIP-006	***# of Members Not Accepting NERC Edits*** *(6 or more= reject edit)*	***Accept/Reject***
Introduction A.3 Purpose Edits GLOBAL	**20** (16/4 ph)	Reject
A.4 Regional Entiti~~esy~~ GLOBAL	**20** (16/4 ph)	Reject but make "Entity"
B. Requirements Delete Preamble	**1** (1/0 ph)	Accept

TABLED, November 13

Appendix #7
Options Paper—Phase II

OPTIONS FOR REVISING THE CIP CYBER SECURITY STANDARD(S)

As the SDT completes its phase I work, it needs to determine what issues it will next address and in what order. However, prior to so doing, there is a foundational issue concerning the relative merits of the CIP and NIST (and other) cyber security standards that should be addressed for several reasons. One reason is the attention that FERC Order 706 gives to this issue; second it raises questions about the basic paradigm that NERC uses in standards development and oversight; and third, how this matter is addressed by the SDT will influence how it may address many other issues raised in FERC Order 706. For these reasons, it is proposed that the next item on the SDT agenda at the conclusion of submitting the Phase I document will be a review of the CIP cyber security standards in relation to relevant standards developed by NIST and others.

Among the points that FERC makes regarding the NERC Cyber Security Standards and those developed by NIST and others, the following seem particularly relevant for the SDT to consider:

1. FERC "believes" that NIST standards "may" provide valuable guidance in developing "future" iterations of CIP standards (sec. 25).
2. FERC "directs" NERC to review revisions in the CIP standards "considering applicable features of the NIST framework." (sec. 25).
3. FERC states it will not delay the "effectiveness" of CIP standards by "directing replacement" of the CIP standards "with others based on the NIST framework." (sec. 25)
4. FERC says it, "will not at this time direct NERC to incorporate specific provisions of the NIST standards," and adds, "that immediate adoption of the NIST standards would result in unacceptable delays (sec.232).
5. FERC says it "believes" NERC "should monitor" the development of NIST standards to see if they contain provisions that may be better than the CIP standards (sec.233).
6. FERC "directs" NERC to "consult with federal agencies" that use both CIP and NIST standards regarding effectiveness and implementation issues concerning NIST and to, "report these findings to the Commission.," (sec. 233).
7. FERC says it "may" revisit this issue in future proceedings as part of their evaluation and assessment of NERC (sec. 233).

Given the above comments, and others from FERC, the NERC Standards Committee has included the following in its directions to the SDT.

"Revisions should consider other Cyber-related standards, guidelines and activities:

- Consider adopting the NIST Security Risk Management Framework (includes GAO, OMB and FIPS)
- Consider other cyber security related documents such as NIST, ISO 27000 Family,
- CIPC WG Risk Assessment Guideline, MITRE Corporation technical report, DHS,

- National Laboratoires papers, DOE 417, IEC, ISA, etc.
- Stay apprised of coordination work between FERC, NEI and NRC in regard to the nuclear facility exemption issue with respect to regulatory gaps. As necessary modify the standards to reflect current determinations."

FERC Order 706 and the directions provided by the NERC Standards Committee suggest a degree of latitude for the SDT in what they may conclude regarding consideration of the NIST Security Risk Management Framework, applicable features, or elements of other security related documents. In regard to the challenge this presents to the SDT, several members have offered suggestions. John Varnell, for example, points out the compatibility of CIP and NIST standards and suggests, "each CIP requirement can be mapped to a NIST 800-53 requirement." This is consistent with the NIST briefings the SDT was given at its first meeting. John goes on to suggest that the SDT develop a guide that will show how NIST requirements can comply with each CIP requirement. Bryan Singer supports this and suggests other relevant standards need to be considered and that attention needs to be given to whether any optional standards meet the intent of a compliance requirement. William Winters suggests that the SDT should first identify its foundational assumptions, of which he offers some examples and alternatives such as: "…adopt the NIST framework and proceed with a roadmap on that basis," "The team should dump the whole standard and start over," and ,"read each FERC concern and adjust current standard as little as necessary to address the concerns."

In keeping with the above suggestions, it is proposed that the SDT consider six options, which, as Phase II Approach Options graphic and the list below illustrate, range from more modest to more sweeping alternatives:

A. Incorporate FERC Order 706. Modify the CIP standards to incorporate the requirements of FERC Order 706. Modify the CIP standards as necessary to address the other requirements of the SAR. Evaluate splitting industrial control systems (ICS) into own set of standards.

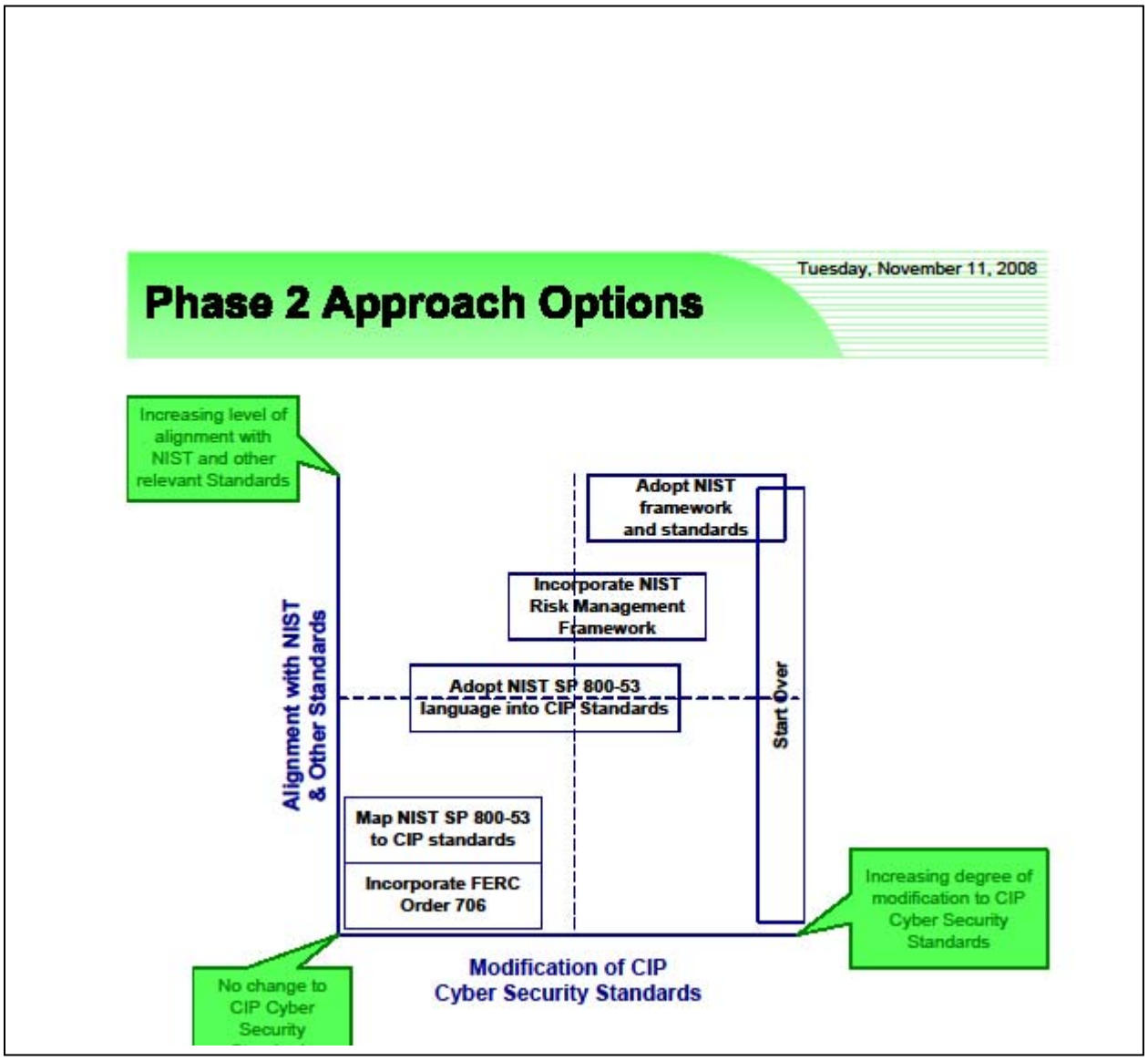
B. Map NIST SP 800-53 to CIP standards: Map similarities and differences between the CIP standards and NIST 800-53 requirements, and provide guidance as to how they can be managed separately but in concert with each other.

C. Adopt NIST SP 800-53 language into CIP standards. In addition to incorporating Option A, provide specific mapping between the CIP standards and the requirements of NIST SP 800-53. Evaluate and modify the language of CIP standards requirements and measures in light of NIST SP 800-53.

D. Incorporate NIST Risk Management Framework. In addition to incorporating options A and C, evaluate and incorporate the NIST Risk Management Framework into the CIP standards. This would predominately impact Critical Cyber Asset identification and technical feasibility/risk mitigation.

E. Adopt NIST framework and standards: Replace CIP Standards with NIST Risk Management Framework and SP 800-53/SP 800-82. This approach represents the wholesale adoption of the NIST framework and discards the existing CIP standards.

F. Start over. Evaluate all available security/risk management frameworks, including ISO



17799/27001, ISA 99, and NIST/FISMA. Select a framework and adopt it fully in place of the existing CIP standards.

It is proposed that the SDT assess these options, identify others that may be as appropriate, and consider modifications or combinations of them. To do this, it may be helpful for the SDT to select assessment criteria, identify the pros and cons of each option, and to rate the various options in regard to levels of acceptability.

Appendix #8 — Phase II Options Review Worksheet

This worksheet was developed by the Facilitators for use on November 14 to guide the STD discussion on approaches and options to Phase II on November 14

SDT PURPOSE STATEMENT

CYBER SECURITY FOR ORDER 706 STANARD DRAFTING TEAM
(adopted unanimously by the SDT, November 13)

The Cyber Security Order 706 Standards Drafting Team (SDT) is serving in the public interest throughout North America to protect the critical cyber assets (including hardware, software, data, and communications networks) essential to the reliable operations of the bulk power system.

The overall purpose of the SDT is to work together to build consensus on a technically sound and complete package of recommended cyber security standards and a realistic implementation plan that is responsive to and consistent with the scope of the Standard Authorization Request (SAR), the FERC Order 706 and the ANSI process.

DRAFT STRAWMAN OPTIONS ASSESSMENT CRITERIA

Review the draft strawman assessment criteria below. If you have an additional criterion you would like to propose, we will solicit those. We will rank, discuss and refine all proposed criteria. Members can utilize these criteria in the evaluation and assessment of each of the Phase II Options:

A. **The option most parallels the SDT purpose statement**

Acceptability Ranking Scale	***4** = acceptable, I agree*	***3** = acceptable, I agree with minor reservations*	***2** = not acceptable unless major reservations addressed*	***1** = not acceptable*
11-14 initial rank				

B. **The option is responsive to the FERC 706 directives and the SAR.**

Acceptability Ranking Scale	***4** = acceptable, I agree*	***3** = acceptable, I agree with minor reservations*	***2** = not acceptable unless major reservations addressed*	***1** = not acceptable*
11-14 initial rank				

C. **The option is achievable in time-- in terms of the SDT developing the proposed standards.**

Acceptability Ranking Scale	***4** = acceptable, I agree*	***3** = acceptable, I agree with minor reservations*	***2** = not acceptable unless major reservations addressed*	***1** = not acceptable*
11-14 initial rank				

D. **The option does most to advance and enhance cyber security**

Acceptability Ranking Scale	***4** = acceptable, I agree*	***3** = acceptable, I agree with minor*	***2** = not acceptable unless major*	***1** = not acceptable*

		reservations	*reservations addressed*	
11-14 initial rank				

E. **Most capable of implementation.**

Acceptability Ranking Scale	***4** = acceptable, I agree*	***3** = acceptable, I agree with minor reservations*	***2** = not acceptable unless major reservations addressed*	***1** = not acceptable*
11-14 initial rank				

F. **Most capable of compliance.**

Acceptability Ranking Scale	***4** = acceptable, I agree*	***3** = acceptable, I agree with minor reservations*	***2** = not acceptable unless major reservations addressed*	***1** = not acceptable*
11-14 initial rank				

G. **Is most supportable by ballot**

Acceptability Ranking Scale	***4** = acceptable, I agree*	***3** = acceptable, I agree with minor reservations*	***2** = not acceptable unless major reservations addressed*	***1** = not acceptable*
11-14 initial rank				

DRAFT STRAWMAN OPTIONS

INSTRUCTIONS: Take a minute to list pros and cons for each of the 6 options. We will review and discuss these. Then we will ask you to rank each on its own keeping in mind the assessment criteria. We will then present these in order of rank (highest average ranking score) and see if there are ways to include pros of other options not selected.

A. Incorporate FERC Order 706.

Modify the CIP standards to incorporate the requirements of FERC Order 706. Modify the CIP standards as necessary to address the other requirements of the SAR. Evaluate splitting industrial control systems (ICS) into own set of standards.

+++++ Pros- Strengths +++++	**------- Cons- Weaknesses --------**
•	•
•	•
•	•

Acceptability Ranking Scale	***4** = acceptable, I agree*	***3** = acceptable, I agree with minor reservations*	***2** = not acceptable unless major reservations addressed*	***1** = not acceptable*
11-14 initial rank				

B. Map NIST SP 800-53 to CIP standards:

Map similarities and differences between the CIP standards and NIST 800-53 requirements, and provide guidance as to how they can be managed separately but in concert with each other.

+++++ Pros- Strengths +++++			------- Cons- Weaknesses --------	
• • •			• • •	
Acceptability Ranking Scale	***4** = acceptable, I agree*	***3** = acceptable, I agree with minor reservations*	***2** = not acceptable unless major reservations addressed*	***1** = not acceptable*
11-14 initial rank				

C. Adopt NIST SP 800-53 language into CIP standards.

In addition to incorporating Option A, provide specific mapping between the CIP standards and the requirements of NIST SP 800-53. Evaluate and modify the language of CIP standards requirements and measures in light of NIST SP 800-53.

+++++ Pros- Strengths +++++			------- Cons- Weaknesses --------	
• • •			• • •	
Acceptability Ranking Scale	***4** = acceptable, I agree*	***3** = acceptable, I agree with minor reservations*	***2** = not acceptable unless major reservations addressed*	***1** = not acceptable*
11-14 initial rank				

D. Incorporate NIST Risk Management Framework.

In addition to incorporating options A and C, evaluate and incorporate the NIST Risk Management Framework into the CIP standards. This would predominately impact Critical Cyber Asset identification and technical feasibility/risk mitigation.

+++++ Pros- Strengths +++++			------- Cons- Weaknesses --------	
• • •			• • •	
Acceptability Ranking Scale	***4** = acceptable, I agree*	***3** = acceptable, I agree with minor reservations*	***2** = not acceptable unless major reservations addressed*	***1** = not acceptable*
11-14 initial				

rank				

E. Adopt IST framework and standards:
Replace CIP Standards with NIST Risk Management Framework and SP 800-53/SP 800-82. This approach represents the wholesale adoption of the NIST framework and discards the existing CIP standards.

+++++ Pros- Strengths +++++			**------- Cons- Weaknesses --------**	
• • •			• • •	
Acceptability Ranking Scale	***4** = acceptable, I agree*	***3** = acceptable, I agree with minor reservations*	***2** = not acceptable unless major reservations addressed*	***1** = not acceptable*
11-14 initial rank				

F. Start over.
Evaluate all available security/risk management frameworks, including ISO 17799/27001, ISA 99, and NIST/FISMA. Select a framework and adopt it fully in place of the existing CIP standards.

+++++ Pros- Strengths +++++			**------- Cons- Weaknesses --------**	
• • •			• • •	
Acceptability Ranking Scale	***4** = acceptable, I agree*	***3** = acceptable, I agree with minor reservations*	***2** = not acceptable unless major reservations addressed*	***1** = not acceptable*
11-14 initial rank				

Appendix # 9 — FERC 706 Background References

Regarding NIST:

25. The Commission believes that the NIST standards may provide valuable guidance when NERC develops future iterations of the CIP Reliability Standards. Thus, as discussed below, we direct NERC to address revisions to the CIP Reliability Standards CIP-002-1 through CIP-009-1 considering applicable features of the NIST framework. However, in response to Applied Control Solutions, we will not delay the effectiveness of the CIP Reliability Standards by directing the replacement of the current CIP Reliability Standards with others based on the NIST framework.

232. As proposed in the CIP NOPR, the Commission will not at this time direct NERC to incorporate specific provisions of the NIST standards into the CIP Reliability Standards. While commenters provide compelling information that suggests that the NIST standards may provide superior measures for cyber security protection, the Commission is concerned that the immediate adoption of the NIST standards would result in unacceptable delays in having any mandatory and enforceable Reliability Standards that relate to cyber security.

233. The Commission continues to believe — and is further persuaded by the comments — that NERC should monitor the development and implementation of the NIST standards to determine if they contain provisions that will protect the Bulk-Power System better than the CIP Reliability Standards. Moreover, we direct the ERO to consult with federal entities that are required to comply with both CIP Reliability Standards and NIST standards on the effectiveness of the NIST standards and on implementation issues and report these findings to the Commission. Consistent with the CIP NOPR, any provisions that will better protect the Bulk-Power System should be addressed in NERC's Reliability Standards development process. The Commission may revisit this issue in future proceedings as part of an evaluation of existing Reliability Standards or the need for new CIP Reliability Standards, or as part of an assessment of NERC's performance of its responsibilities as the ERO.

Regarding an additional guidance/reference document

61. The Commission received comments on both sides of the issue of specificity. Some commenters caution against the CIP Reliability Standards being too specific, while others request more guidance to help them comply. In general, the Commission believes it is appropriate to provide sufficient guidance to explain Requirements so that responsible entities have a high degree of certainty that they understand what is necessary to comply with a Requirement. More guidance will allow responsible entities to implement measures adapted to their specific situations more consistently and effectively. Additional guidance need not be included in a specific Requirement, but could be in the form of examples. The Commission is not directing that the ERO establish a specific end result. Our concern is simply that responsible entities have guidance on how to achieve an appropriate result in individual cases, which can vary on a case-by-case basis. Therefore, in several instances throughout this Final Rule, the Commission gives the ERO direction to provide additional guidance. In some cases, we require

that the guidance be placed in modifications to the CIP Reliability Standards. In other cases, we note that some or all of the additional guidance could be placed in a reference document separate from the CIP Reliability Standards.

253. The Commission believes that the comments affirm that responsible entities need additional guidance on the development of a risk-based assessment methodology to identify critical assets. While we adopt our CIP NOPR proposal, we recognize that the ERO has already initiated a process to develop such guidance. The CIP NOPR proposed to direct that NERC modify CIP-002-1 to incorporate the guidance. However, we are persuaded by commenters that stress the need for flexibility and the need to take account of the individual circumstances of a responsible entity. Thus, we modify our original proposal and in this Final Order leave to the ERO's discretion whether to incorporate such guidance into the CIP Reliability Standard, develop it as a separate guidance document, or some combination of the two. A responsible entity, however, remains responsible to identify the critical assets on its system.

355. The Commission believes that responsible entities would benefit from additional guidance regarding the topics and processes to address in the cyber security policy required pursuant to CIP-003-1. While commenters support the need for guidance, many are concerned about providing such guidance through a modification of the Reliability Standard. We are persuaded by these commenters. Accordingly, the Commission directs the ERO to provide additional guidance for the topics and processes that the required cyber security policy should address. However, we will not dictate the form of such guidance. For example, the ERO could develop a guidance document or white paper that would be referenced in the Reliability Standard. On the other hand, if it is determined in the course of the Reliability Standards development process that specific guidance is important enough to be incorporated directly into a Requirement, this option is not foreclosed. The entities remain responsible, however, to comply with the cyber security policy pursuant to CIP-003-1.

356. In response to ISO/RTO Council, Ontario Power and other commenters, the Commission's intent in the CIP NOPR — as well as the Final Rule — is not to expand the scope of the CIP Reliability Standards. Requirement R1 of CIP-003-1 requires a responsible entity to document and implement a cyber security policy "that represents management's commitment and ability to secure its Critical Cyber Assets." The Requirement then states that the policy, "at a minimum," must address the Requirements in CIP-002-1 through CIP-009-1. The Commission believes that there are other topics, besides those addressed in the Requirements of the CIP reliability Standards, which are relevant to securing critical cyber assets. The Commission identified examples of such topics in the CIP NOPR. Thus, the Commission, in directing the ERO to develop guidance on additional topics relevant to securing critical cyber assets, is not expanding the scope of the CIP Reliability Standards.

408. The Commission agrees with FirstEnergy on the importance of flexibility in developing a mutual distrust posture, but does not see a conflict between the need for flexibility and what it is proposing, which is simply more guidance. More guidance will allow responsible entities to implement measures adapted to their specific situations more consistently and

effectively. Additional guidance need not be included in a specific Requirement, but could be in the form of examples. We will leave it to the Reliability Standards development process and the ERO to decide whether some or all of the guidance can be contained in separate guidance documents referenced in the Reliability Standard. In response to Entergy, the Commission is not directing that the ERO establish a specific end result. Our concern is simply that responsible entities have guidance on how to achieve an appropriate result in individual cases, which can vary on a case-by case basis. We disagree that providing useful guidance affects the scope of the Reliability Standards.

502. In response to APPA/LPPC, the Commission clarifies that it does not intend to create an inflexible rule calling for redundant electronic security in all cases. While the Commission directs that a responsible entity must implement two or more distinct security measures when constructing an electronic security perimeter, the specific requirements should be developed in the Reliability Standards development process. This would include whether or not the second security measure must be "on par" with the first. The Commission also directs the ERO to consider, based on the content of the modified CIP-005-1, whether further guidance on this defense in depth topic should be developed in a reference document outside of the Reliability Standards.

511. The Commission adopts the CIP NOPR's proposal to direct the ERO to identify examples of specific verification technologies that would satisfy Requirement R2.4, while also allowing compliance pursuant to other technically equivalent measures or technologies. In response to commenters, in discussing digital certificates and two-factor authentication, the Commission was providing examples of strong authentication, not limiting authentication to those options. The Commission is not prescribing the specific methods as an exclusive solution pursuant to Requirement R2.4. The ERO can propose an alternative solution that it believes is equally effective and efficient. If the ERO believes it would be helpful to responsible entities, additional guidance beyond the examples that are eventually included in Requirement R2 can be given in a separate reference document. Since we are directing the ERO to provide guidance on what constitutes strong authentication, it is not necessary for the Commission to respond to ISO-NE's request that digital certifications or two-factor authentication are acceptable methods of authentication. In identifying examples or categories of specific verification technologies that would satisfy Requirement R2.4, the ERO should take into account the specific comments raised in this proceeding. Similarly, while encryption is one method to accomplish two-factor authentication, and is an effective process for ensuring authenticity of the accessing party, for some facilities, we leave it to the ERO in the Reliability Standards development process to evaluate whether and how to address the use of encryption. In the alternative, the ERO may identify verification technologies or categories of verification technologies in a reference document.

547. In sum, we direct the ERO to modify Requirement R4 to require these representative active vulnerability assessments at least once every three years, with subsequent annual paper assessments in the intervening years. The ERO should develop the details of how to determine what constitutes a representative system and what modifications require an active vulnerability

assessment in the Reliability Standards development process. The revised Reliability Standard should contain the essential requirement that an active assessment must be performed at least once every three years. Based on the amount of guidance contained in the modified Reliability Standard, the ERO should consider at that time whether additional guidance should be provided in a reference document.

575. In response to commenters' questions regarding specific physical access controls, the Commission clarifies that it does not intend to create an inflexible rule calling for redundant physical security. While the Commission continues to believe that a responsible entity must implement two or more distinct and complimentary physical access controls at a physical access point of the perimeter, the specific requirements should be developed in the Reliability Standards development process when the ERO develops its modifications in response to this Final Rule. The Commission also directs the ERO to consider, based on the content of the modified CIP-006-1, whether further guidance on this defense in depth topic should be developed in a reference document outside of the Reliability Standards.

609 . The Commission has discussed issues related to testing environments in CIP-005-1. In that context, the Commission clarifies the CIP NOPR proposal to require differences between the test environment and the production system to be documented. As stated with respect to CIP-005-1, the Commission understands that test systems do not need to exactly match or mirror the production system in order to provide useful test results. However, to perform active testing, the responsible entities should be required at a minimum to create a "representative system" — one that includes the essential equipment and adequately represents the functioning of the production system. We therefore direct the ERO to develop requirements addressing what constitutes a "representative system" and to modify CIP-007-1 accordingly. The Commission directs the ERO to consider providing further guidance on testing systems in a reference document.

621. While we agree that no safeguard will protect against all malicious or unintentional acts, this does not mean that systems should not be protected against such acts. In response to MidAmerican, the Commission believes that details regarding how to safeguard systems against personnel introducing, maliciously or unintentionally, viruses or malicious software to a cyber asset are best developed in the Reliability Standards development process. The revised Reliability Standard does not need to prescribe a single method for protecting against the introduction of viruses or malicious software to a cyber asset by personnel. However, how a responsible entity does this should be detailed in its cyber security policy so that it can be audited for compliance with the Reliability Standard. The Reliability Standards development process should decide the degree to which the revised CIP-007-1 describes how an entity should protect against personnel introducing viruses or malicious software to a cyber asset. The ERO could also provide additional guidance in a reference document.

629. For the reasons discussed in CIP-005-1, in directing manual log review, the Commission does not require that every log be reviewed in its entirety. Instead, the Commission will allow a manual review of a sampling of log entries or sorted or filtered logs. The

Commission recognizes that how a responsible entity determines what sample to review may not be the same for all locations. Therefore, the revised Reliability Standard does not need to prescribe a single method for producing the log sampling. However, how a responsible entity performs this sample review should be detailed in its cyber security policy so that it can be audited to determine compliance with the Reliability Standards. The Reliability Standards development process should decide the degree to which the revised CIP-007-1 describes acceptable log sampling. The ERO could also provide additional guidance on how to create the sampling of log entries, which could be in a reference document. The final review process, however, must be rigorous enough to enable the entity to detect intrusions by attackers.

644. For the reasons discussed in CIP-005-1, in directing manual log review, the Commission does not require that every log be reviewed in its entirety. Instead, the Commission will allow a manual review of a sampling of log entries or sorted or filtered logs. The Commission recognizes that how a responsible entity determines what sample to review may not be the same for all locations. Therefore, the revised Reliability Standard does not need to prescribe a single method for producing the log sampling. However, how a responsible entity performs this sample review should be detailed in its cyber security policy so that it can be audited to determine compliance with the Reliability Standards. The Reliability Standards development process should decide the degree to which the revised CIP-007-1 describes acceptable log sampling. The ERO could also provide additional guidance on how to create the sampling of log entries, which could be in a reference document. The final review process, however, must be rigorous enough to enable the entity to detect intrusions by attackers.

660. The Commission adopts the CIP NOPR proposal to direct the ERO to provide guidance regarding what should be included in the term reportable incident. In developing the guidance, the ERO should consider the specific examples provided by commenters, described above. However, we direct the ERO to develop and provide guidance on the term reportable incident. The Commission is not opposed to the suggestion that the ERO create a reference document containing the reporting criteria and thresholds and requiring responsible entities to comply with the reference document in the revised Reliability Standard CIP-008-1, but will allow the ERO to determine the best method to accomplish the goal of better defining reportable incident.

725. The Commission adopts, with modifications, the CIP NOPR proposal to develop modifications to CIP-009-1 through the Reliability Standards development process to require an operational exercise once every three years (unless an actual incident occurs, in which case it may suffice), but to permit reliance on table-top exercises annually in other years. Consistent with our goals and discussion of CIP-005-1, the Commission will not at this time require responsible entities to perform full operational exercises. Instead, the Reliability Standard should require the demonstrated recovery of critical cyber assets in a test environment, with the requirements for representative test environments and for addressing differences between the test environment and the production environment, similar to the conditions discussed for live testing in CIP-005-1. Given the range of views presented in comments regarding live testing, as the Reliability Standard development process forms the details of this “demonstrated recovery”

concept, it should consider offering guidance beyond the actual Requirements of the Reliability Standard in separate reference documents. The Commission believes this alleviates commenters' concerns about the risks associated with such testing

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Meeting Agenda — AECC Offices, Little Rock, AR
Cyber Security Order 706 — Project 2008-06

Date and Time	WebEx Details	Conference Call Details
November 12, 2008 1–5 p.m. Central	WebEx Number: 713 030 769 Meeting Password: standards	Dial-in Number: 866-289-4175 Conference Code: 6310586983
November 13, 2008 8 a.m.–5 p.m. Central	WebEx Number: 715 639 395 Meeting Password: standards	Dial-in Number: 866-289-4175 Conference Code: 6310586983
November 14, 2008 8 a.m.–noon Central	WebEx Number: 714 186 394 Meeting Password: standards	Dial-in Number: 866-289-4175 Conference Code: 6310586983

Wednesday, November 12, 2008

1:00 p.m. Welcome and Opening Remarks — Jeri Domingo-Brewer and Kevin Perry

1:05 Roll Call — Harry Tom

1:10 Review NERC Antitrust Compliance Guidelines — Harry Tom

1:15 Adopt October 22 Meeting Notes and Review of Meeting Objectives — Bob Jones

1:20 Organizational Issues — Stuart Langton

- Review of Workplan
- Adopting the SDT Consensus Guidelines
- SDT Purpose Statement

2:00 Phase I Products — Review

3:00 Break

3:15 Phase I Products — Review

5:00 Observer Comments and Suggestions

5:15 Adopting the Phase 1 Products — Straw Poll on Phase 1 Products

5:30 Recess

Thursday, November 13, 2008

8:00 a.m. Welcome and Agenda Review

8:10 Phase I Products — Refinements

9:30 Additional Straw Polls

10:00 Break

116-390 Village Blvd.
Princeton, NJ 08540
609.452.8060 | www.nerc.com

10:15	Adoption of Phase I Products
11:00	Phase II Work plan Review and Discussion — Review of Concept(s) Submitted and Strawman
noon	Working Lunch
1:00 p.m.	Phase II — NIST and CIP- 002 — Discussion
3:00	Break
3:15	Continue Discussion of NIST and CIP 002
5:00	Summary of Day Two Outcomes and Review of Day Three Agenda
5:15	Recess

Friday, November 14, 2008

8:00 a.m.	Welcome and Agenda Review
8:10	NIST and CIP 002
10:00	Break
10:15	CIP 003-009 Review
11:30	Assignments, Next Steps, and Review of Work plan
noon	Adjourn

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Cyber Security Order 706 Standard Drafting Team

DRAFT CONSENSUS GUIDELINES

CONSENSUS DEFINED

Consensus is a **process**, **an attitude and an outcome**. Consensus processes can produce better quality more informed products.

A. Consensus is a problem solving process in which all members:

1. Jointly distinguish their concerns
2. Educate each other
3. Jointly develop alternatives and then
4. Adopt recommendations everyone can embrace or at least live with.

In a consensus process, members can honestly say:

- I believe that other members understand my point of view
- I believe I understand other members' points of view
- Whether or not I prefer this decision, I support it because it was arrived at openly and fairly and because it is the best solution for us at this time

B. Consensus as an attitude provides that each member commits to work toward agreements that meet their own and other member needs and that all can support the outcome.

C. Consensus as an outcome means that agreement is reached by all members or by a significant majority of members. The level of enthusiasm for the agreement may not be the same among all members on any issue, but on balance all should be able to live with the overall package. **Levels of consensus** can include:

- Participants strongly support the solution
- Participants can "live with" the solution
- Some participants do not support the solution but agree not to veto it.

DRAFT CONSENSUS GUIDELINES

The Cyber Security Order 706 Standard Drafting Team (Team) will seek consensus on its recommendations for any revisions to the CIP standards.

General consensus is a participatory process whereby, on matters of substance, the members strive for agreements which all of the members can accept, support, live with or agree not to oppose. In instances where, after vigorously exploring possible ways to enhance the members' support for the final package of recommended revisions, and the team finds that 100 percent acceptance or support of the members present is not achievable, final consensus recommendations will require at least 75 percent favorable vote of all members present and voting. This super majority decision rule underscores the importance of actively developing consensus throughout the process on substantive issues with the participation of all members. In instances where the team finds that even 75 percent acceptance or support is not achievable, the team's report will include documentation of any differences as well as the options that were considered for which there was greater than 50 percent support from the team.

The team will develop its recommendations using consensus-building techniques with the leadership of the Chair and Vice Chair and the assistance of the facilitators. Techniques such as brainstorming, ranking and prioritizing approaches will be utilized. The team's consensus process will be conducted as a facilitated consensus-building process. Team members, NERC staff, and facilitators will be the only participants seated at the table. Only team members may participate in consensus ranking or vote on proposals and recommendations. Observers and members of the public are welcome to speak when recognized by the Facilitator and all written comments submitted on the comment forms will be included in the team and facilitators' summary reports.

The team will make decisions only when a quorum is present. A quorum shall be constituted by at least 51 percent of the appointed members being present (simple majority). The team will utilize Robert's Rules of Order *(as per the NERC Reliability Standards Development Procedure)*, as modified by the team's adopted procedural guidelines, to make and approve motions; however, the 75 percent supermajority voting requirement will supersede the normal voting requirements used in Robert's Rules of Order for decision making on substantive motions and amendments to motions. In addition, the team will utilize their adopted meeting guidelines for conduct during meetings. The team will make substantive recommendations using their adopted facilitated consensus-building procedures, and will use Robert's Rules of Order only for formal motions once a facilitated discussion is completed.

Either the presiding chair or Facilitator of the SDT, in general, should use parliamentary procedures set forth in Robert's Rules of Order, as modified by the team's adopted procedural guidelines.

To enhance the possibility of constructive discussions as members educate themselves on the issues and engage in consensus-building, members agree to refrain from public statements that may prejudge the outcome of the team's consensus process. In discussing the team process with the media, members agree to be careful to present only their own views and not the views or statements of other participants and/or may direct such inquiries to the team Chair and Vice Chair. In addition, in order to provide balance to the team process, members agree to represent and consult with their stakeholder interest group.

MEETING GUIDELINES FOR PARTICIPANTS

Participants' Role in Meetings:

- Explore possibilities.
- Listen to understand (Respect) (limit sidebar conversations).
- Be focused and concise. (Avoid repetition. No need to offer comments in "strong agreement.")
- Focus on issues, not personalities.
- Offer options to address others' concerns.
- No sidebars.

Facilitators and Staff role in Meetings:

- Assist the Chair and Vice Chair in helping the team stay on task.
- Help the group follow agreed upon ground rules.

- Design the meeting and problem solving process in consultation with the Chair and Vice Chair.
- Facilitate discussion participation of the team and other participants.
- Prepare agenda packets and reports.

CONSENSUS BUILDING TECHNIQUES

- **Brainstorming (green light thinking — not judgmental).** At certain points, the facilitator may ask the group to suspend judgment and get ideas onto the table before debating.

- **Name Stacking in Team Discussions** (use of name tents to seek attention)

- **Acceptability Consensus Ranking Scale**
  - Use a consensus acceptability scale to help focus discussion and test support in reviewing substantive issues.
  - Use to guide and focus discussion and as a poll to see where the team stands, not used as a voting mechanism.
  - Must be prepared to offer refinements and suggestions to address serious concerns.

  4 = Proposal is acceptable as it is
  3 = Proposal is acceptable; I can live with it but there are minor concerns to address
  2 = Proposal is not acceptable. Proposal may be acceptable if the major concerns are addressed
  1 = Proposal is not acceptable

- **Consensus Ranking Scale**
  4. Comfortable — I support proposal as is ♥♥♥♥
  3. Minor Reservations — I can live with this; but would like to see changes as follows♥♥♥ Be prepared to offer specific refinements or changes to address your concerns.
  2. Major Reservations — I can't support this unless following changes are addressed to meet my serious concerns ♥♥ Be prepared to offer specific refinements or changes to address your concerns.
  1. Fatal Flaws — I can't support this ♥ Be prepared to offer alternatives and options that would address your own as well as other's concerns.

- **Robert's Rules of Order and Facilitated Consensus Building Procedures**
  The Council will make substantive recommendations using their adopted facilitated consensus-building procedures, and will use Robert's Rules of Order only for formal motions once a facilitated discussion is completed.

  - Any voting member may make a motion when a quorum is present.
  - A second is required to discuss the motion.

- If a motion is seconded, the Chair or Facilitator opens the floor for discussion.
- The Chair or Facilitator will recognize members wishing to speak on the motion.
- The Chair or Facilitator will, if time permits, recognize other participants wishing to speak on the motion.
- The Chair or Facilitator may elect or be requested by the member making the motion to take a "straw poll" on the motion.
- The member making the motion may accept friendly amendments to the motion.
- After completing discussion, the Chair or Facilitator will call the discussion to a close and restate the motion, with any friendly amendments, and call for a vote.
- If the motion receives a 75 percent favorable vote of the members present and voting it will be approved.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

CYBER SECURITY ORDER 706 STANDARD DRAFTING TEAM DRAFT PURPOSE STATEMENT

The team is serving in the public interest throughout North America *to protect the critical cyber assets (including hardware, software, data, and communications networks) essential to the reliable operations of the bulk power system.*

The overall purpose of the Cyber Security Order 706 Standards Development Team is to work together to build consensus on a technically sound and complete package of revised draft cyber security standards and realistic implementation plan that is responsive to and consistent with the scope of the Standard Authorization Request (SAR), the FERC Order 706 and the ANSI process.

(Italics from the SAR "purpose" statement)

	4=acceptable	***3= minor reservations***	***2=major reservations***	***1= not acceptable***
Initial Ranking				
Revised/Amend				

Comments

TITLE: REVISIONS TO CRITICAL INFRASTRUCTURE PROTECTION STANDARDS (REVISIONS TO CIP-002 THROUGH CIP-009)

Request Date: March 1, 2008, Revision Date: June 9, 2008
Approved by Standards Committee for standard development on July 10, 2008

July 15 Announcement for Nominations to SAR (excerpt):
"For this drafting team, the Standards Committee is looking for a variety of expertise, with the possibility of having the team subdivide itself into smaller teams based on expertise."

Team Purpose: To protect the critical cyber assets (including hardware, software, data, and communications networks) essential to the reliable operations of the bulk power system.

Industry Need:
Implement Changes to the following Cyber Security Standards as indicated in FERC Order 706:

CIP-002-1 — Critical Cyber Asset Identification
CIP-003-1 — Security Management Controls
CIP-004-1 — Personnel & Training
CIP-005-1 — Electronic Security Perimeter(s)
CIP-006-1 — Physical Security of Critical Cyber Assets
CIP-007-1 — Systems Security Management
CIP-008-1 — Incident Reporting and Response Planning
CIP-009-1 — Recovery Plans for Critical Cyber Assets

Brief Description:

This set of revisions in this project includes:

- Modifying the standards so they conform to the latest approved versions of the ERO
- Rules of Procedure as outlined in the Standard Review Guidelines identified in Attachment 1.
- Addressing the directives issued by FERC, in Order 706 relative to the approved Cyber Security Standards CIP-002-1 through CIP-009-1. Refer to http://www.ferc.gov/whats-new/comm-meet/2008/011708/E-2.pdf for the complete text of the final order. Specific requirements from the Order are identified in Attachment 2.
- Emphasis on Order 706 directive for NERC to address revisions to the CIP standards considering applicable feature of the NIST Security Risk
- Management Framework among other resources.
- Incorporating clarifications from the Interpretation of CIP-006-1 Requirement 1.1.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Draft Meeting Summary

Cyber Security Order 706 SDT — Project 2008-06

December 4, 2008 | 8 a.m.–5 p.m.
December 5, 2008 | 8 a.m.–5 p.m.

SDT Draft Meeting Report By:

Robert Jones and Stuart Langton
FCRC Consensus Center, Florida State University

Thanks to Team members Sharon Edwards, Tom Hofstedler and Kevin Perry for sharing their meeting notes.

http://www.nerc.com/filez/standards/Project_2008-06_Cyber_Security.html

116-390 Village Blvd.
Princeton, NJ 08540
609.452.8060 | www.nerc.com

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Cyber Security Order 706 Standard Drafting Team
Draft December 4–5 Meeting Summary
Washington D.C.

Meeting Summary Contents

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Cyber Security Order 706 Standard Drafting Team
Draft December 4–5 Meeting Summary
Washington D.C.

EXECUTIVE SUMMARY

The Chair, and Vice Chair welcomed the members and a roll call of members and participants in the room and on the conference call was conducted. Following review of the proposed meeting agenda, Michael J. Assante, NERC Chief Security Officer who offered some comments and perspectives for the Team's consideration urging them to adopt an "outcome oriented" standards development approach with a goal of regulatory stability while focusing resources on protecting what is most important. Jake Olcott, Staff Director and Counsel, House Subcommittee on Emerging Threats, Cyber Security, Science & Technology chaired by Rep. James R. Langevin (D-RI) under the Committee on Homeland Security, offered comments on the Team's effort thus far and noted that this was an area to great and continuing interest to Congress, as witnessed by their formal comments submitted by the Committee and Subcommittee on the FERC Notice of Proposed Rulemaking for Mandatory Reliability Standards for Critical Infrastructure Protection in October, 2007.

David Taylor reviewed with the Team the need to comply with NERC's Antitrust Guidelines.
The SDT unanimously adopted the November 12-14, 2008 meeting summary with a correction in the text changing the quorum rule from 51% to 2/3's. The facilitators reviewed with the Team the consensus guidelines adopted at the Little Rock meeting.

Kelly Ziegler, NERC Manager of Communication presented a proposed Phase I Communications Plan. She outlined for the team three plan objectives: provide adequate information for voting**;** improve visibility of the SDT process**;** and drive positive media coverage**.** She then described the Webinar procedure and NERC's experience with them.

Scott Mix reviewed the "Technical Feasibility eight page document which was first reviewed at the Sacramento meeting and then again at the Little Rock meeting. The paper sections include:

- Objective/Purpose/Executive Summary/Background
- Definition of Technical Feasibility Exception:
- Application:
- Overview of Essential Elements:
- Detailed TFE Process:
- Good Faith efforts
- Sensitive Information:
- Post Approval Processes required by FERC Order:
- Appeals Process:

This was modeled after self-reporting mechanism to fit into the existing compliance program. He noted the plan was to post a white paper for Industry review after the Team reviewed and agreed on the draft. Todd Thompson, NERC Compliance, noted a process has been developed for protecting sensitive audit-

related information so it remains on site at the Responsible Entity, providing evidence if it's tampered with. Roger Lampila noted that training is being provided to regions for their CIP auditors; during recent session, there was general agreement from those present that more knowledgeable auditors will be needed. Entities need to verify with their respective regions that the individuals performing the audits are qualified.

Areas of the Paper the SDT commented on included: Documenting Mitigation; Remediation Steps and Wide Area Approval- ERO's audit process--Regional Entity and ERO Steps

Scott Mix sent out the TF Exception Paper for review by the drafting team on Thursday evening. Comments were received from several drafting team members and Mr. Mix responded on Friday with refinements to the draft. Mr. Mix agreed to determine how the paper would be presented to the industry- i.e. as a NERC or SDT product. The Team agreed to provide Scott with comments by December 12, 2008 and the SDT would review the revised white paper at the January meeting seeking to adopt it for posting thereafter for industry comments.

The balance of the meeting focused on reviewing and discussing the approach to the SDT's Phase II which had been reviewed at each of its first three SDT meetings including an options paper presented and discussed at the Little Rock meeting.

A presentation on the implementation of the NIST framework from a user's perspective was offered by SDT members Jeri Brewer, John Stamford and Keith Stouffer. They provided some perspectives on implementation and identified issues. Following the briefing, The SDT members discussed current approaches to identification of Critical Assets, risk management and the following topics:

- New Technology and Risk Management
- Threats and Risk
- NIST Guidelines and CIP Standards- Both/And?
- Risk Assessment and Resource Implications
- Component-based System Approach
- IT and Control Systems
- Levels of Risk- "One Size Fits All"? NIST and CIP
- Compliance and Audit Concerns

Following the Little Rock meeting, the facilitators asked the Vice Chair, Kevin Perry to draft some strawman draft statements and questions to serve as a starting point for the SDT's consideration of risk assessment. He introduced the statements noting they provide a statement on the industry's current methodology, a problem statement on this methodology, and 8 critical questions regarding risk management. The SDT reviewed and discussed risk management and tested the support through a 4-point acceptability ranking for the following statements:

> **The Current "Consequence-based" Assessment Methodology Draft Statement:**
> The industry focuses on the facility (asset), employing a "consequences-based" assessment methodology to determine if the facility is essential to the reliable operation of the bulk electric system:
>
> - Those that are essential are declared to be Critical Assets.

- We then determine the Cyber Assets essential to the operation of the identified Critical Asset and those become subject to the CIP standards to the exclusion of pretty much all else.

(Average Acceptability Ranking-3.9 of 4)

A Draft Problem Statement with the "Consequences-Based" Assessment Methodology:
The problem presented with this approach is that:

(a) Given the dynamic nature of the transmission system, assets that are critical today might not be tomorrow, and vice versa. *(Average Acceptability Ranking-3.8 of 4)*

(b) The industry may be "cherry-picking" the Cyber Assets to be protected, along with any collateral Cyber Assets that happen to be connected to the same network segment. *(Average Acceptability Ranking-3.1 of 4)*

- *2nd Draft* (b) Some in the industry may be selecting the Cyber Assets to be protected, along with any collateral Cyber Assets that happen to be connected to the same network segment based on economic vs. security considerations.

(c) The approach excludes all other Cyber Assets, including Cyber Assets that may provide essential data to the Critical Cyber Assets or may have a trusted relationship (communications path) that could be exploited as an attack vector. *(Average Acceptability Ranking-3.1 of 4)*

(d) Once a Cyber Asset is identified as either a Critical Cyber Asset or collateral Cyber Asset within the Electronic Security Perimeter, all of the requirements of the CIP Cyber Security Standards apply, regardless of the specific Cyber Asset's importance to the reliable operation of the Bulk Electric System. *(Average Acceptability Ranking-3.8 of 4)*

The discussion regarding risk management led to the testing of the goal of CIP 002. The following statement was offered for acceptability ranking:

> The goal/intended outcome of CIP 002 to identify the Cyber Assets (i.e. Programmable electronic devices and communication networks including hardware, software, and data, NERC Glossary) that need to be protected and to identify the level of protection. *(Average Acceptability Ranking-3.8 of 4)*

The SDT then discussed what kind of framework made sense for inventorying cyber assets which covering the following topics:

- Overall Approach
- Inside-Out Approach
- Systems View
- Protection Model
- Scope
- What Assets Included?
- Real World Examples
- Inventory and Compliance

Following the discussion, one member proposed testing support for the following inventory statement:

Inventory your cyber assets directly related to the operation of your registered NERC functionality:

- Apply a risk methodology to assign a level.
- Apply distinct controls according to the level.
- Inventory for each cyber asset should be: device + o's + function + firmware level.
- These attachments will be critical for patch management and CIP 007R1 testing.

(Average Acceptability Ranking-2.3 of 4)

Another member then proposed testing support for the following inventory statement:

> Identify the applications and computer systems within the Industry Controls Systems or information systems as well as the networks within and interfacing with the ICS. The focus should be on systems rather than devices, and should include PLCs, DCS, SCADA, and instrument bases systems that use a monitoring device such as an HMI.
> *(Average Acceptability Ranking-2.2 of 4)*

Following the lunch break on Day 2, the chair announced that Jackie Collett and William Winters had agreed to draft two "straw" documents, reviewing the SDT discussions to date, to help move the Team forward on the development of a Phase 2 roadmap:

- SDT member Jackie Collett will draft a white paper starting from an attempt to protect the best of what exists with the current CIP and incorporating NIST concepts/features.
- SDT member William Winters will draft a 2nd white paper starting with the NIST framework and incorporate the best of the CIP into it.

NERC staff presented some information and sought SDT input on the industry "Webinar" December 16 from 11:30 until 1 p.m. on the Phase I SDT products. The SDT reviewed the proposed meeting schedule to complete the Phase I process by the end of June, 2009. The next meeting will take place at the Arizona Public Services Corporation facilities in Phoenix. The Chair suggested the following agenda items:

- Organizing and initiating the review of industry comments that have been received on the posting of Revised CIP standards from Phase I;
- Finalize the SDT input to the NERC Technical Feasibility Exceptions white paper; and
- Time permitting, continue discussion of the CIP 002 approach to assets in scope for Phase II including review of the papers from SDT members Jackie Collett and William Winters.

At the conclusion of the meeting, the facilitators asked the Team to offer an evaluation of the process including what worked well during the meeting and what could be improved. There was appreciation of the meeting site in the Capital and facility, of the sound system, of the tagging on from the NERC CIPC meeting and the debate and breadth of knowledge on the team. On improvements, SDT members suggested the facilitators should try to close off open-ended discussions where we are repeating our points (i.e. "violent agreement"). The meeting adjourned at 2:15 p.m. Friday afternoon.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Draft Fourth Meeting Summary
December 4–5, 2008
Washington D. C.

I. INTRODUCTIONS, AGENDA REVIEW, PROCEDURES AND OPENING REMARKS

The Chair, and Vice Chair welcomed the members and asked NERC staff David Taylor to conduct a roll call of members and participants in the room and on the conference call *(See appendix #2*). They then reviewed with the Team and participants the proposed meeting agenda *(See appendix #1*).

The Chair introduced Michael J. Assante, NERC Chief Security Officer who offered some comments and perspectives for the Team's consideration. He thanked the Team for their commitment and work to date and urged them to adopt an "outcome oriented" standards development approach which will require rigor and discipline to follow through. He suggested the key goal should be regulatory stability – i.e. seek to establish an enduring outcome with a set of standards that will last for long time – only needing tweaking as conditions change. This will require a very sharp focus by the Team on each requirement to define the outcome you are trying to achieve and then work backwards to ensure all of the requirements achieve the desired outcome objective. To illustrate the offered two examples:

- CIP-002: approach understood, objective well intended, trying to take sensible approach to defend what is most important. But if you do work backwards, you will find gaps that need to be filled. Guard against assumptions that if you do it right you will fill the gaps. How dangerous are the assumptions? TO/TOP understands assets and can make determination of relative importance. Not true of GO/GOP that do not have planning resources.
- CIP-004: Personnel Risk Assessment/Training – plan is good, subject matter of training will change. If outcome is to assure that risky personnel cannot have unescorted access to cyber assets, then working backwards you find gaps. A missing gap is an entity must have a list of disqualifying factors. A starting point may be the Federal standards (Transportation Worked Identification Credential) a federal mandate for any entity needing access to port facilities. Then need to bring in bargaining agreements, etc.

The Team should focus resources on protecting what is most important. The CIP standards requirements may not have that focus and there may be some gaps. He challenged the Team to look at each assumption with this in mind and suggested their Phase 2 work is the right time to deliver this message.

The Chair also welcomed Jake Olcott, Staff Director and Counsel, House Subcommittee on Emerging Threats, Cyber security, Science & Technology chaired by Rep. James R. Langevin (D-RI) under the Committee on Homeland Security, and invited him to provide the Team with any comments. Mr. Olcott acknowledged the Team's effort thus far and

noted that this was an area to great interest to Congress as witnessed by their formal comments submitted by the Committee and Subcommittee on the FERC Notice of Proposed Rulemaking for Mandatory Reliability Standards for Critical Infrastructure Protection in October, 2007 *(See Appendix #9).* He noted that membership is not yet resolved for the new congress but predicted that there will be continuing interest in this topic. He noted that the Energy and Commerce Committee in the House and Senate are also very interested in this issue. He noted that he will be following the Team's work and provided his contact information for anyone wanting to follow up with him *(See, Appendix #9).*

David Taylor reviewed with the Team the need to comply with NERC's Antitrust Guidelines *(See, Appendix #3).* He urged the Team and other participants in the process to carefully review the guidelines as they would cover all participants and observers. He urged all to avoid behaviors or appearance that would be anti-competitive nature and also reminded the group of the sensitive nature of the information under discussion.

The Chair noted the November 12-14, 2008 meeting summary had been circulated to members in advance of the meeting. She noted a correction in the text changing the quorum rule from 51% to 2/3's. David Norton moved and Sharon Edwards seconded the motion to accept the summary as revised. The Team unanimously accepted the meeting summary.

The facilitators reviewed with the Team the consensus guidelines (Appendix #5) adopted at the Little Rock meeting.

II. NERC PHASE 1 COMMUNICATIONS PLAN

Kelly Ziegler, NERC Manager of Communication presented a proposed Phase I Communications Plan. She outlined for the team three plan objectives: provide adequate information for voting**;** improve visibility of the SDT process**;** driving positive media coverage**.** She then described the Webinar procedure and NERC's experience with them. They will provide a press release in advance which will note the multi-phased approach and a high level summary on the web of the Phase 1 products.

Initial Questions/Comments on the Communication Plan Approach

- Reference to 3 phases? Should be referenced as a multi-phase approach.
- It would be ideal to capture the audio webinar in a-podcast form so industry could listen to it at other times.
- Press release: timing? Plan to released next week followed up with the Webinar.

III. TECHNICAL FEASIBILITY EXCEPTION- REVIEW AND REFINEMENT

Scott Mix reviewed the "Technical Feasibility eight page document which was initially reviewed at the Sacramento meeting and then again at the Little Rock meeting. The paper sections include:

- Objective/Purpose/Executive Summary/Background
- Definition of Technical Feasibility Exception:

- Application:
- Overview of Essential Elements:
- Detailed TFE Process:
- Good Faith efforts
- Sensitive Information:
- Post Approval Processes required by FERC Order:
- Appeals Process:

This approach was modeled after self-reporting mechanism to fit into the existing compliance program. He noted that he would go through a red line version for one more round. He reviewed the requirements within the filing including the date that the TF exception is no longer necessary. After the individual filings are made, FERC has charged the ERO with the task of taking a regional and national impact of all TF exceptions. At this time, NERC does not have a consistent process for self-reporting across the regions. The TFE language may show up in 005 & 006 & 007. There were many questions concerning the right approach to presenting the straw man to the industry.
He noted the goal would be to post a paper approved by the Team for comment soon after the December or January meeting.

Todd Thompson, NERC Compliance, noted a process has been developed for protecting sensitive audit-related information so it remains on site at the Responsible Entity, providing evidence if it's tampered with. Roger Lampila noted that training is being provided to regions for their CIP auditors; during recent session, there was general agreement from those present that more knowledgeable auditors will be needed. Entities need to verify with their respective regions that the individuals performing the audits are qualified.

SDT Comments

- If we do our job right we will look at outcome-based standards. The issue is that the standard does not drive technology and that the proposed process needs to consider requirements that apply to PLCs, for example, where there is no solution in response to the requirement such as anti virus.
- Order 706 may leave room to consider replacing equipment that does not comply with the requirements with a similar vintage of equipment if necessary.
- NERC might start an effort to work with the vendors to supply solutions to security as directed in Order 706. This would be something that the ERO could do to improve and drive technology.
- Where ever possible take care of this in Phase 2. But will need a process to deal with really new problems.
- Could be a self-reported non-compliance?
- Some technical requirements may mean someone may need a TFE. Indicate in general language a requirement that you think the TFEs showing up will be reviewed on a case-by-case basis analysis.

- What about an instance of, for example, a plane crash with all staff? Self report of non-compliance. Not a technical issue but an emergency issue.
- You may need an "exception" to the exception process- "outcome basis"? Let the ERO deal with it. If denied then on the non-compliance path. If accept, look back at whether standards need adjustment.
- Each utility for each requirement, e.g. CIP 007- file an exception per requirement, per utility? Could be a deluge? Checks and balances will require paperwork associated with it. Consider the compliance process- self reported
- This may be the reason to stop thinking about generation, transmission and think about types of equipment. All bought at same time, with same problem. E.g. 10,000 of a brand of relays that can't support a password. Single filing vs. 10,000 filings. Will have to work through details
- TFE- problem with piece of equipment- probably would result in one filing.
- The required timeframe for documentation may present problems.
- Consider a paperwork avoidance procedure—while we annotate where TFEs can be taken.
- Develop a list where we know where exceptions can't be taken. When does the inconvenience/cost factor cross over into a security issue. "Infeasibility"- can't be just inconvenience.
- "Burning the strawman" in the debate- put this in a guideline. Cut down on lots of needless actions.
- Clarification- TFE procedure – same as CIP 003 R3 exception process? No. Difference. R3 is taking exception to own internal policies and not a compliance issue vs. a compliance issue taking exception to the standard.
- If built policy to mirror CIP standards, would they be interpreted as one and the same? You may do that but the ERO won't be tracking all internal policies at a company.
- If we do our job right and focus on outcome based standards this will be addressed.
- Today no consideration in current standards as to whether their application makes sense in a particular setting. Concept deserves continued debate and discussion.
- Standards do not drive technology- can't expect that sometime in future engineers will design a way to comply with standard. Also can't assume technology won't change.
- Opportunity for NERC to document the current exceptions taken to date to inform the SDT review of this? Probably right thing to do. List sounds like a roadmap to the past. How to communicate all info to all who need to take action and yet protect everyone else. Difficult problem. Devil in the details.
- Operating systems- software and purpose written software do not have the same vulnerability.
- "Improperly comply with requirement"? Literal interpretation reducing reliability. E.g. passwords not working well in a setting.
- Maybe this is literally complying vs. "improperly"
- Revision in Phase 2 should be more obvious where to apply
- Virus scanning- putting on windows platform becomes a detriment to the operation.

- Clear as to what we are asking for. E.g. list what not complying with and provide mitigation steps. Need to understand- dealing with the remaining risk or risk of not doing it at all.
- Can't anticipate everything. Probably can be clear on somewhere you can't take a TFEs.

Documenting Mitigation- *Scott Fix, NERC*

- Documenting mitigation. E.g. protect device from attack from viruses by doing something that isn't in the standard but works.
- Document a remediation plan- will be long term plans. May be open-ended plans. "when it breaks I will fix it". Need provision for these kind of plans. Tough to do with annual approval process.

Remediation Steps

SDT Comments on Remediation Steps

- Envision a technical exception to equipment password. Still purchasing equipment. So taking a TFE of where they are going, not just where they been.
- E.g. 100,000 relays in environment. 1 breaks do I replace with one everyone knows how to work with or the new one requiring new training, assessment, major purchases. Different from a new substation investment. Everything should meet standards.
- Everything done is very date-related in terms of compliance looking backwards.
- 706 position may not be right on remediation by date certain necessary in all cases.
- Para 181- new equipment- left some wiggle room for valid considerations
- NERC compiling exceptions? Can't write standards that drive the vendor community? Need to ask for a bridge that is not too far.
- What NERC might do, start working with vendors in a vendor management forum to educate and help the market respond better. Feed into this concepts like forensics?

Wide Area Approval — ERO's audit process — Regional Entity and ERO Steps

SDT Comments

- Front line for the process. Notice to the Region on TFE.
- Region apply catalogue i.d. to track- analysis and approval
- ERO needs to provide enough info for Regional entity to do job
- If not enough detail provided, claim rejected.
- Analysis of impact to reliability of TFE. Might require coordination with other entities and regions.
- Milestone slippage- grounds for non-compliance. In best interest to be upfront and forth coming.
- Sensitive info concerns. E.g. Fed agencies for FOIA requests etc.
- Post approval process- annual report to FERC. Canadians have a similar view in their systems. ERO high level view across America. "ARSAWS" (check with todd) completed for all requirements.

- Didn't invent a new appeals process. Compliance and enforcement monitoring appeals process.
- Safe harbor/good faith while request is being processed? CMEP is public document. Is this legal? FERC safe harbor wasn't thrilled. May open up self to "gaming"- have to structure it carefully.
- Cryptographic mechanisms? E.g. Disaster recovery evidence go with it. Including this for electronic documentation. Incorporated way to take encrypted data on better cds. Maintain it at responsible entity.
- Summary info to Canadian entities. Responsible entity has some sort approval? Utilities need some input on what goes forward. Regional entity, ERO and utility should be comfortable. Work towards getting something that meets all needs before reporting.
- If you go to ERO and they say no to TFE? Use the appeals process at the ERO.
- Has to be added to each regional entities CMEP for this to work. This is part of the next steps. Sooner we do this, better we will all be.
- Guidance from current compliance self report process?
- Better definition of "validity"? Fair question. Need to clarify that for industry.
- Part will be how well you write justification and how you demonstrate that you are seeking to achieve the spirit of the requirement.
- Do the RE's have the technical expertise to evaluation the appropriateness of the TFE? Typically don't know various systems. How will we expect that can do this consistently across.
- Reason why approvals are multi-step. ERO could reject even when the RE accepts.
- May become part of the formal delegation agreement?
- How good is good enough? Adequacy metrics. Regional auditors- ARSAW run through to see how vanilla IT look at cyber security environment.
- FISMA experience- Keith. SP 800 series is a lot of guidelines- best professional advice.
- SDT can't do this. Is there an encyclopedia can go to in order to help with the process.
- Federal agency- Auditor General- take a manual- (Jeri). Reports to congress annually on how effective Federal agency security program. Effectiveness of your implementation against the 853 standards. How well that is achieving the goal. FISCAM- Audit Manual
- 800 series documents have lots of best practices. Most are guidelines. GAO looks at them, says you can't blow off, must consider. Some weight.
- Unfortunately for this area are IT specific vs. cyber. 800-82 is one guidance doc. ISA 99 good material as well.
- Don't overplay how "unique" our environment increasingly is.
- Field assets are a different animal.
- This is bigger than just TF, also auditing requirements of regions. Problem recognized within the compliance structure- regions told need to solve the problem. ERO is serious as well with Mike and Todd brought on.
- First CIP auditor training recently in Princeton. Just getting underway. By the end of day 1, regions realized they needed more talented staff. Only a few with the right background. Really thinking of how to function as a audit team member.
- NERC- virtual auditor- support structure to get assistance and reach back.

- What assurances do we have this will be done before audits are happening? Auditing bodies should show how their training. This is a major concern of industry. This is a resource and knowledge issue.
- Federal- auditing with key focuses- programmatically how applied the standards and guidance. Did we id the risks and select the right controls. Test the controls to determine level of veracity and then produce a report (GAO, IG) give equal weight to IT and the cyber community. Have to do risk assessment.

Next steps — Day One

- Scott Mix will clean up and email to the team.
- SDT members will provide comments and suggestions.
- NERC internal working document and doesn't have to go through a ballot process.

SDT Comments

- Are we sure the requirements won't change. TFE for other than technical issues. Invoked where it allows. How to handle this? Hold off until we hit the version 3 standards.
- "Field test" the process.
- If this guideline is to be treated as a non binding guideline then no voting necessary. If this is the expectation that auditors will use and will become binding, industry will have to vote on it.
- This document needs to fit into and follow the current ERO auditing process.
- NERC – Roger's process for input on the audit process. Went to NERC BOT for approval. CIPSE guidelines don't go to BOT because they are not binding. Some way these will be sanctioned.
- Need to make this when implemented. Need to say where this TFE cannot be used.
- FERC- identify where positively can't be used. "Willing to be reasonable" TFE process will be out quickly and implemented quickly.
- Note, when we revisit the requirements- its only where it is currently in the standard.
- Possible at beginning of Jan meeting to agree to post.
- Do we apply only where we have it in the standards?
- Back out "only where specifically allowed" language. Note we may do this in Phase 2.
- Deleted "reasonable business judgment and acceptance of risk"
- Team appreciated.

Day Two — SDT Review and Next Steps

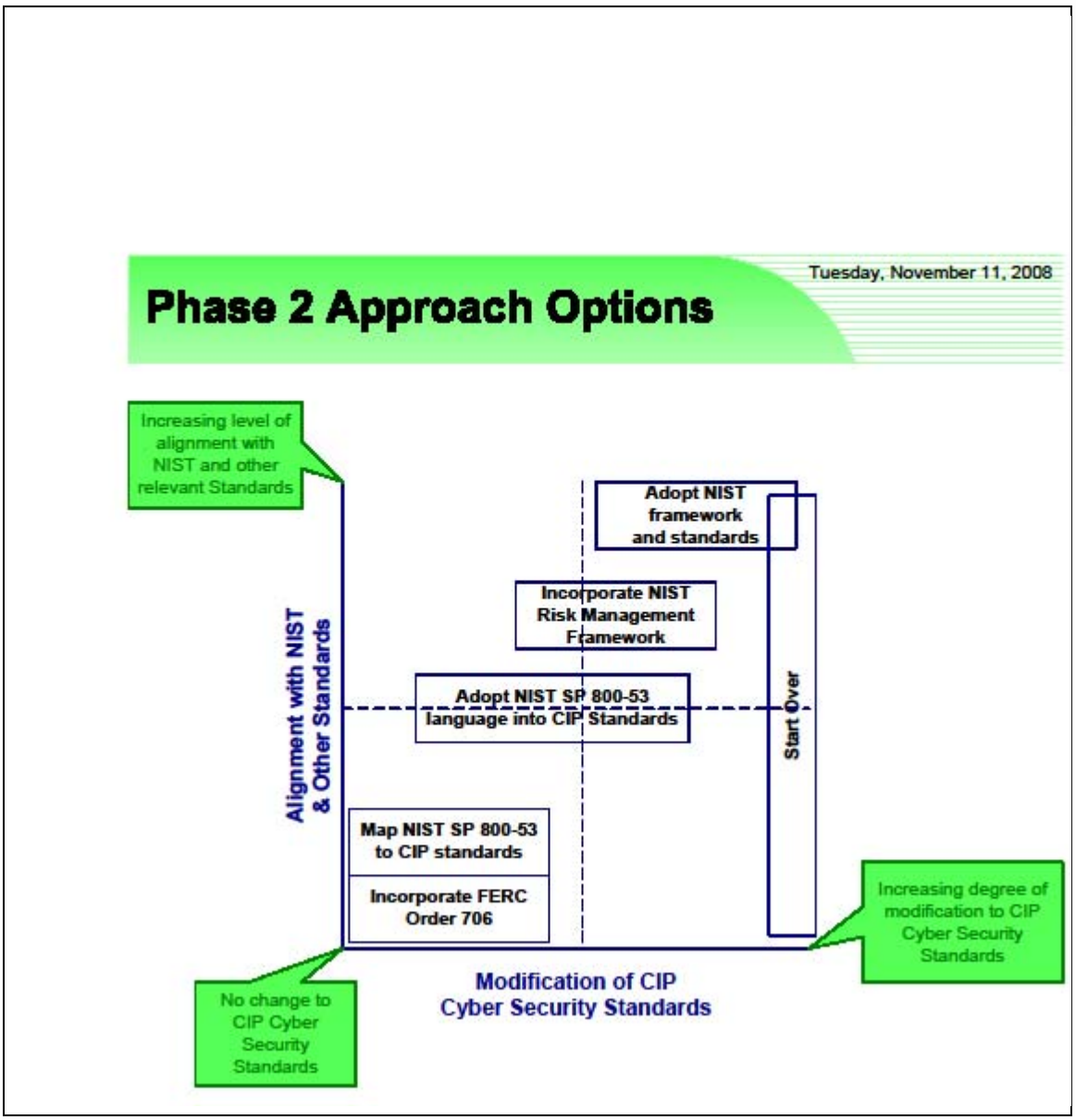
- Scott Mix had sent out the TF Exception Process for review and sent it out to the drafting team on Thursday evening. Comments were received from several drafting team members.
- There was a concern expressed around sensitive information. Scott stated that NERC staff will review the procedure with audit staff. Scott said he would like a couple more days for the rest of the drafting team to review and make comments. After that the draft will be sent out to the drafting team PLUS list.

- Scott also wants the legal staff to review. After all those steps are done, the information will be posted as a white paper for public comment.
- Scott does not expect the public posting to happen until 1st half of January. Scott raised the issue of whose name should be on the white paper when it is posted?
- When the team provides comment, Scott asked that the group provide questions that should be asked of the industry at the public posting.
- The Chairman suggested Friday, December 12, as the due date for comments. The Facilitator asked that comments be submitted to the entire drafting team.
- The technical feasibility exception is in the standard today. What NERC is creating is the procedure that utilities must follow so the change that is being proposed is a change in the rules of procedure. Therefore, this is not a new standard; the TF exception is a new NERC process. There was discussion as to whether NERC needs to post the document for public review. It was generally agreed that the new TF exception process is only a NERC procedure not a standard, and does not need to be balloted by the industry.
- This process provides approval, oversight and appeal. Order 705 Paragraph 184 - exemption is a release from a requirement; an exception is a way to deal with a requirement. There was discussion of the meaning of "exception" vs. "exemption."
- Jeri cautioned the group to get their comments in on the TF exception process. Finalizing the SDT review of the Technical Feasibility Exceptions white paper will be placed on the SDT agenda at the January meeting.

IV. REVIEW OF PHASE II APPROACH

A. Background on SDT Development of Phase II Roadmap

The SDT at its first three meetings discussed how to develop a clear roadmap for how it would engage on the issues and products in Phase II. At the conclusion of the Sacramento meeting, the Chair asked the facilitator to develop an options paper for review at the Little Rock meeting following the adoption of the Phase I package. The facilitators received comments and suggestions on approaches and options from John Varnell, Bryan Singer and William Winters and worked closely with the Chair and the Vice Chair in producing the options white paper that was initially reviewed at the Little Rock meeting. *(See Appendix #7).*



The paper suggested there is a foundational issue concerning the relative merits of the CIP and NIST (and other) cyber security standards that should be addressed for several reasons. One reason is the attention that FERC Order 706 gives to this issue (*See Appendix # 9)*; second it raises questions about the basic paradigm that NERC uses in standards development and oversight; and third, how this matter is addressed by the SDT will influence how it may address many other issues raised in FERC Order 706. For these reasons, the paper suggested the next item on the SDT agenda at the conclusion of submitting the Phase I document will be a review of the CIP cyber security standards in relation to relevant standards developed by NIST and others. A diagram (*See previous page)* was offered to graphically describe a way to chart the options presented for Phase II.

B. Perspectives on Implementing the NIST in the Context of the CIP

SDT members Jeri Brewer, John Stamford and Keith Stouffer provided some comments on implementing the NIST framework from a user's perspective

1. Briefing Issues Identified

- NIST was established around human relations and finance style systems. It was not based on the operational perspective of a control system that needs to keep the operations functional 24/7 minimizing disruptions when they happen (nature, troublemakers etc.). The NIST risk management framework gives tools from IT to apply to control sectors that give protections. 882 helped to address some of the gaps between the IT and control system perspectives.
- The basic concept calls for identifying assets and the risk these assets will have on your mission and tailoring the protections to fit your mission needs.
- Focus on is on control systems, so production impact is a greater concern than in IT. NIST Framework is tool designed for IT environment and applied to control system environment. Elements missing from 800-53 have been addressed by 800-82.
- So NIST represents a process for identifying assets and the associated risks, with protection tailored to fit systems and environment is based on impact, what is needed to address it.
- The NIST framework provides a way for the utilities to adopt the methodology tailored to the utility's specific needs.
- On the positive side, the NIST framework is technology neutral. It is “technology agnostic and risk agnostic.”
- The NIST risk management framework is also flexible for tailoring. However this can also be a negative in that it requires more work and expertise of the end user and in the control center environment to figure out how to align the system. This also extends to the auditor in determining how to assess your system. In a compliance environment the CIP standards tend to lend themselves to more prescriptive requirements--more check-the-box than risk management.
- It functions like an IT network environment with common platforms. NIST framework adapted well to the control system environment. Started in 2004 in first NIST draft.
- The NIST framework has adapted well to the control system environment, however they have not been as successful in adapting the framework for field devices which are not similar to normal IT systems on which NIST was based initially.
- This framework is superior to other methods which are available.
- In a compliance environment, more prescriptive directions for the NIST framework may be needed to facilitate auditing.
- Investing resources to give the biggest bang for you buck. Not 100% protection. Focus on minimize disruption on critical operations, get them back into production as quickly as possible
- Framework to structure and invest in those resources so you can be resilient and recover quickly.

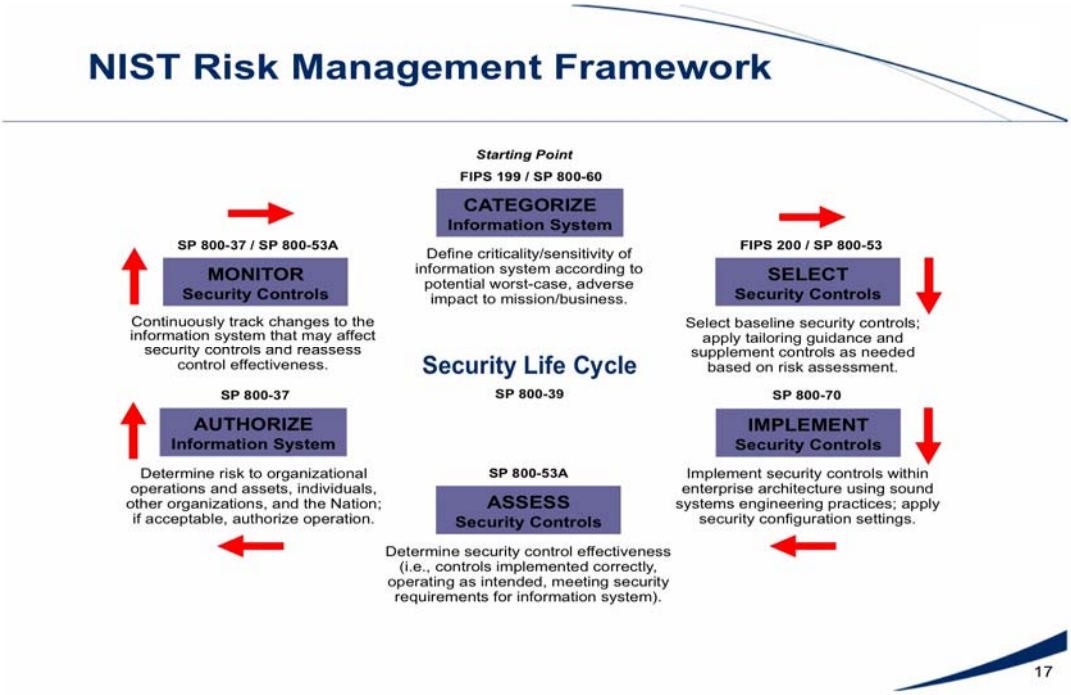
- Standardized way to establish protections with flexibility to adapt to requirements and assets to meet mission.

SDT Comments on NIST and CIP

- The SDT members discussed current approaches to identification of Critical Assets, the role of threats, and associated matters.

2. New Technology and Risk Management

- New risks are constantly being introduced as a result of bringing on new technology. This trend will continue.
- In the field this is a much bigger challenge. Smart grid and substation automation is happening and easier to consider in this light.
- Increasing use of intelligent electronic devices.
- A fundamental issue: mindset in the industry that doesn't take interconnectivity of systems into account.



3. Threats and Risk Management

- Congressional perspectives frame the issue in terms of how the model addresses threats and vulnerability. Congressional staff are looking for feedback from the SDT on how that fits into the NIST or other risk management models used by the industry.

- In the federal NIST implementation framework, most threat information comes in from DHS.
- Frankly in the federal sector from a substation control center perspective, Congress needs to sit down with people who do this every day. Homeland security data is largely worthless, as it is very generalized threats. Doesn't apply specifically to the grid and electric system.
- In recent Audit- DOE was criticized for not having good external threat information, even though it is reliant on DHS for this data.
- If you know your vulnerabilities, considering "risk" isn't viable because true risk is impossible to ascertain. Instead, the focus should be on the vulnerability & the impact if it occurs. Whatever has the greatest potential impact is the area that needs the greatest effort to protect.
- FERC suggested that threat should be taken off the table when it comes to a risk assessment. Instead look to take the best of CIP and NIST in order to provide better protection for control systems. Field devices are going to need minimal amount of protection. But there is a basic level of protection regardless.
- Internal threat profiles are frequently overlooked in many risk assessment discussions.
- We should use a consequence-based assessment- what is the consequence of comprising and taking over the system vs. just knocking the system down.
- Threat- many people believe government has good threat information. But it really isn't there or if it is, it is only available for short term (vs. longer term).
- In the risk equation, throw threat out otherwise it drives the risk lower. Never will get the granularity you want.
- For the industry the threat/risk is sanctions. Our vulnerability is unclear. Potential to separate the critical asset assessment from the standard itself.
- What is the vulnerability of BES from any asset we control. Drive down to risk assessment- do we employ a graded-mitigation model? With a high risk, there will be a higher level of mitigation. Not a proponent of low-level mitigation.
- Missing vulnerability information related to our assets. No model in place for determining the effect of the loss of a given asset. E.g. that component has the following vulnerability.
- Have to take the vendor's assessment of that.
- Concern about the quality of the vendor companies for the assessment. National labs available to do this. Get additional funding not just from the industry.
- Develop a national security assessment model?
- Is exclusion of vendors from the standards development a problem?

- Threat and vulnerability- last posted draft of the CIPC- "threat and vulnerabilities" are going to exist. Becomes an impact analysis for the reliability or operability of the BES. Risk based assessment method- does an asset if destroyed impact the reliability of the BES.
- Threat and vulnerability should be irrelevant. Impact analysis is what matters and it is what we do best.

4. NIST Guidelines and CIP Standards — Both/And?

- Is there a key difference between guidelines vs. a standard? CIP is already using a lot of the framework. When the industry re-did the CIP standards, it took a risk-based approach. Sees a lot of good points from NIST that could be added to the CIP standards.
- Most valuable aspect of FISMA framework is doing the risk-based approach to whatever asset you are dealing with.
- While it is not easy to implement, it is superior to others e.g. ISA 99.
- Based on the CIP and NIST experience evidence suggested it may be possible to use both standards and controls to help strengthen the CIP.
- NIST is proscriptive to systems applied to. Hardware, software, people and processes.
- Can do things in field you can't do in CIP. Look at like assets. Mitigate risks to assets in a repeatable way.
- CIP is all or nothing. Black or white. CIP standards are more requirements. Put you in a path you may not be able to get out of.
- NERC assessment- Bonneville is self-funded not subject to appropriations. When NERC a non-compliance finding happens, it is taken very seriously. The SDT job is to marry the two approaches together so we are not wasting time, effort and resources.
- The SDT should use the concepts of the framework and not the specifics—that's what the SDT needs to focus on. Industry needs reasonable and achievable controls, giving them options where appropriate.
- Ideally, adopt the best of CIP & NIST. CIP's biggest problem: identification of critical assets. If protection is focused on those items alone, the other assets related to control systems are left potentially vulnerable. A minimal level of protection would be identified if an organization used NIST process. Everything needs some protection; the most essential assets need more protection.
- The NIST standards & FISMA are not focusing efforts from a national perspective; that's a core problem for this industry to look at issues from this viewpoint.
- This approach is valuable because the oversight responsibilities of NERC & the Regions will offer a different perspective than government utilizes for addressing issues of national concern that extend beyond the boundaries of a specific agency/organization.

Day Two SDT Comments

- Every federal system has to meet baseline controls at a minimum
- Concern that CIP didn't meet even minimum baselines compared to NIST

- Determining scope is an application specific issue; preliminary activities are needed regardless of approach. CIP takes more piecemeal approach and then applies all rules to what's been identified.
- NIST is more systems oriented; looks at identify boundaries around important things, then all aspects of each identified information system are managed—things over which you do have control. A risk based decision needs to be made about what will (or should) come across interfaces from outside that environment. Since every component is not equally able to apply controls, there is a more comprehensive approach.
- NIST may not be readily auditable so it will be a challenge to modify that approach for our purposes.
- CIP vs. NIST. Better adapting the best of each to come up something better.
- Flaw of the "critical asset" — cyber is a different animal can get to all assets at the same time (#274 control stations/centers). N-1 method of id critical assets is not good enough.
- NIST- what is electrically important to the grid- armor those assets. But need to provide basic protection for the rest.
- Resources using the NIST framework are ultimately aligned in most effective manner and threats are not (and cannot be) eliminated, but resources can be structured to address the greatest risks.
- NIST only identify information systems not control systems. Need to merge the two. CIP missing some of the NIST components.
- Conformance and compliance works well when you have check box spec system.
- Risk management may be what is needed to be done- but as a standard for compliance. Will be difficult to map up the two.
- Is there another tool to promote risk management other than a compliance approach?

5. Risk Assessment and Resource Implications

- Risk assessment done in federal sector by independent organizations. E.g. Iowa labs. It is an iterative process, like maintenance on car. Annual basis sometimes quarterly. Constant tweaks. Continuous improvement.
- The primary goal of the assessment process is impact analysis.
- We know the assets we need to protect. Are we mitigating the right risk for the right asset. Most valuable threat info (comes best from locally).
- It might be useful for INL or similar group to develop a risk assessment model for the industry, specifying what requirements actually are mandatory.
- In Florida, came up with "Risk = Impact divided by level of effort to accomplish the bad deed." From there they graded the risk levels of different deeds. A ratio (picked 1.0 threshold below which standard protection). Kept applying assets and compensation measures until risks went low. Critical assets review- risk assessment methodology.
- Risk assessment- grading security to the assets we have to take care of. Not sure how it has to work, but there is got to be a way to do it.

- Risk management and conformance – if outcome based standards with a risk management approach you can build a conformance model around that. Not always mutually exclusive.
- If the risk assessment framework were adopted, would it be a significant resource burden on the industry? Yes, it does take lots of resources to go through the FISMA exercise. CIP is narrower applying only to critical asset and cyber asset.

6. Component-Based Systems Approach

- Does a systems based approach vs. a component-based approach make any difference? More risks with certain components. Not adding or getting out of anything by using the NIST standards. Could probably modify the framework to deal with critical components.
- The SDT can modify anything in the NIST if it accurately assesses the risk of each component across and within the system.
- Component based vs. system based? Take the framework concepts and not the literal framework, we might have the opportunity to focus on what really needs protection. Give the industry appropriate, reasonable and achievable control and where they are given the options. This may present a challenge for auditors and the auditing process, but this may be the right step to take for the industry.
- The control system mechanism requires protection. Limiting the focus to "critical assets" necessarily overlooks areas of the control system that are essential but miss the target for receiving protection.

7. IT and Control Systems

- The overall issue is conventional IT vs. control systems. Before interconnection, no problems
- Opportunity: continue treating control systems as special, and build accordingly
- Alternative: emphasize reliability & resiliency, w/ chance to lead industry:
- The conventional IT environment has been geared to accept occasional outages as a cost of doing business, but that approach is not acceptable for control systems
- There is a "corporate IT" and "power system IT"; effective management and change control

8. Levels of Risk- “One Size Fits All”? NIST and CIP

- The fundamental problem with CIP that the SDT should address is the one size fits all in terms of critical cyber asset. There isn’t the high, medium low judgment made in the NIST framework. It will be important for the industry to invest money and staff into focusing in on most important (i.e. high).
- Don’t throw the CIP standards out and plug NIST in wouldn’t work. Because it comes from a IT background not from a power plant control systems and control centers. What constitutes a cyber threat pushed out to specific equipment. Gap needs to be addressed in NIST and one size fits all in CIP needs to be addressed.
- The CIP standards effort tried to make it work otherwise. Don’t need to throw all out the CIPs to address levels of compliance or types of equipment.

- We need lots of works on levels, controls. Try to preserve the industry investment made while making our existing framework better.
- Auditors may need to consider "appropriateness", perhaps. The current approach of CIP standards w/ all or none/one size fits all is not working.

9. Compliance and Audit Concerns

- In a compliance environment, more prescriptive directions for the NIST framework may be needed to facilitate auditing.
- FISMA and NERC amount of penalty associated with NERC standard. Doesn't exist in NIST framework. Compliance environment with flexibility-
- SDT members offered to continue to lend the Federal lessons learned from implementing NIST and surviving numerous audits to the SDT. It has been an eye opening experience.
- Some federal entities are not subject to NERC sanctions, but there are implicit sanctions for them—appropriations lacking, or rate payers who are subject to the penalties for entities that are self supporting.
- Auditing community needs re-educated; they're typically in a checklist mentality because of other NERC Standards. Without the technical knowledge, they can't adequately determine whether efforts adequately address potential vulnerabilities in the cyber area.
- Conformance & compliance work well w/ a specific standard (pass/fail checklist); for cyber security. If risk management is the approach, another tool is needed besides conformance to compliance.
- What's needed isn't a "culture of compliance"; what's needed is a "culture of security."
- NIST standards are not unlike others and audits are possible.
- FERC is concerned about the quality of what an entity does; it's not just checking off an item on a list.
- On audit issue, whichever route we take, the biggest culture change will be in the auditor community. Checklist mentality. Cyber requires analysis of what have you done. If they don't have technical knowledge or working with that mindset.
- "Defense in depth"- filtering wall, firewall have BS. Can have those all and not have a secure architecture.

C. Risk Management- Key Concepts and Questions

The facilitators asked Kevin Perry to draft some strawman statements and questions to serve as a strawman for the SDT's consideration. He introduced the statements noting it provides an overview of the statement of the current methodology a problem statement for the SDT's consideration followed by 8 critical questions regarding risk management.

1. The Current "Consequence-based" Assessment Methodology Draft Statement:

The industry focuses on the facility (asset), employing a "consequences-based" assessment methodology to determine if the facility is essential to the reliable operation of the bulk electric system:

- Those that are essential are declared to be Critical Assets.
- We then determine the Cyber Assets essential to the operation of the identified Critical Asset and those become subject to the CIP standards to the exclusion of pretty much all else.

Acceptability Ranking Scale	***4 =** acceptable, I agree*	***3 =** acceptable, I agree with minor reservations*	***2 =** not acceptable unless major reservations addressed*	***1 =** not acceptable*	***Avg.***
12-5 rank	**16** (13 + 3)	**0**	**2**	**0**	**3.9 of 4**

Comments before ranking

- Review of current process for assessing critical assets & corresponding CCAs.
- Focus on critical facilities/assets begs the issue of dynamic systems (e.g., flowgates)
- Industry could easily be "cherry picking" what they want to protect—the systems, related cyber systems. As a result, quality of review may vary
- An ESP doesn't address trusted path that crosses it (e.g., VPNs). A potentially vulnerable/out-of-scope system then has unrestricted access inside the perimeter.
- "All or nothing": there are no gray areas; a system either has to follow all CIP requirement or none.
- The "as is" statement describing the current methodology isn't accurate; by saying that non-critical assets are exempt from CIP Standards in the current scenario overlooks processes and activities that some have used to address situations such as those used in the example.
- The statement is accurately describing the situation that currently exists.
- The team needs to develop standards that can be audited against; there are various ways to accomplish that. The CIPC effort to develop guidelines for identifying critical assets has generated a lot of comments & won't be finalized for several months. However, whatever we create needs to align with the guidelines or vice versa.

Comments after ranking

- **2=** Don't agree with statement. CIP standards isn't a system approach. However don't see that CIP excludes a systems approach. Took an assets.
- 2= concern about the phrase "to the exclusion of pretty much everything else."
- Reason focus is on the critical assets is because NERC charge to deal with BES. Make sure all critical assets protected. This statement can't be right if we really think about what NERC's charge is.
- Standards say we can exclude. Drawing the line not in CIP. We exclude them from the CIP standards. Only requirement for maintenance. Logging at access point.

2. A Draft Problem Statement with the "Consequences-Based" Assessment Methodology

Kevin Perry presented the following problem statement as a strawman for the SDT's review and consideration.

The problem presented with this approach is that:

(a) Given the dynamic nature of the transmission system, assets that are critical today might not be tomorrow, and vice versa.

Acceptability Ranking Scale	*4 = acceptable, I agree*	*3 = acceptable, I agree with minor reservations*	*2 = not acceptable unless major reservations addressed*	*1 = not acceptable*	*Avg.*
12-5 SDT rank	**16** *(14 + 2)*	**5** *(2 + 3)*	**0**	**0**	**3.8 of 4**

SDT Comments

- None

(b) The industry may be "cherry-picking" the Cyber Assets to be protected, along with any collateral Cyber Assets that happen to be connected to the same network segment.

Acceptability Ranking Scale	*4 = acceptable, I agree*	*3 = acceptable, I agree with minor reservations*	*2 = not acceptable unless major reservations addressed*	*1 = not acceptable*	*Avg.*
12-5 SDT rank	**9** *(6 + 3)*	**5** *(3 + 2)*	**5** *(5 + 0)*	**1**	**3.1 of 4**

SDT Comments

- Not related to this approach- accept gaming is part of the deal and move on.
- Not a problem statement for standards. This is part of implementation statement for the solutions.
- This implies industry is dishonest in "cherry picking." Not necessarily the case.
- Should delete or reword this as a part of the problem statement.
- The "cherry picking" issue isn't primarily driven by a desire to not protect systems, but to make them exempt from CIP because of sanction issues

- **2nd Draft E.g. (b) Some in the industry may be ~~"cherry-picking"~~ selecting the Cyber Assets to be protected, along with any collateral Cyber Assets that happen to be connected to the same network segment based on economic vs. security considerations.**

(c) The approach excludes all other Cyber Assets, including Cyber Assets that may provide essential data to the Critical Cyber Assets or may have a trusted relationship (communications path) that could be exploited as an attack vector.

Acceptability Ranking Scale	*4 = acceptable, I agree*	*3 = acceptable, I agree with minor reservations*	*2 = not acceptable unless major reservations addressed*	*1 = not acceptable*	*Avg.*
12-5 SDT rank	**5 + 1**	**6 + 2**	**2 + 1**	**1**	

SDT Comments

- Doesn't necessarily exclude. This is matter of interpretation.

(d) Once a Cyber Asset is identified as either a Critical Cyber Asset or collateral Cyber Asset within the Electronic Security Perimeter, all of the requirements of the CIP Cyber Security Standards apply, regardless of the specific Cyber Asset's importance to the reliable operation of the Bulk Electric System.

Acceptability Ranking Scale	*4 = acceptable, I agree*	*3 = acceptable, I agree with minor reservations*	*2 = not acceptable unless major reservations addressed*	*1 = not acceptable*	*Avg.*
12-5 SDT rank	**17 *(13+4)***	**1**	**0**	**1**	**3.8 of 4**

SDT Comments

- When ever you have a perimeter, it is protecting your assets.
- Is this a problem
- Other issues to consider: are we addressing facilities? What are "systems"?
- Focus perhaps should be on functions vs. assets.
- The current approach focuses too much on "how we affect the national grid"; instead, entities should be looking at their own mission—what do they need to do to protect themselves? The result of that effort would lead to protection of the BES, in a manner more inclusive than the current approach. Using the national grid as the criteria allows too many loopholes to applying the standards.
- The definition of "critical assets" needs to be limited to physical assets. By bringing in the logical components would increase the complexity of identifying critical assets in another context (e.g., physical protection standards that might be developed in the future).
- These standards shouldn't be focused on Critical Assets; the cyber issues ought to be the priority.
- The SDT shouldn't overlook the interest shown by Congress, and the promise to take action if industry doesn't respond in a timely or adequate manner. The input to the NOPR by a couple members of the committee was historic and unprecedented. The SDT needs to take that issue seriously.
- The focus is cyber security engineering, not electrical engineering.
- Is the current definition of "cyber asset" in the Glossary accurate & acceptable?
- Kevin Perry sent this to members over night: Definition of Computer System and Control System
- Definition of Computer System (http://www.webopedia.com/TERM/C/computer_system.html):
- "A complete, working computer. The computer system includes not only the computer, but also any software and peripheral devices that are necessary to make the computer function. Every computer system, for example, requires an operating system.
- Definition of Control System (DHS Catalog of Control Systems Security: Recommendations for Standards Developers): 'A set of hardware and software acting in concert that manage the behavior of other devices."

- Maybe can be added to the glossary and added to the definition of Cyber Asset. For example: Cyber assets include Computer Systems, Control Systems, programmable electronic devices, and communication networks including hardware, software, and data.
- Current NERC Glossary definition of Cyber Asset: "Programmable electronic devices and communication networks including hardware, software, and data.") His concern: the focus is on "the box", and an integrated system may not adequately be addressed.
- The existing taxonomy resulted from the historic focus on power engineering & bulk electric system reliability. Otherwise, a bottom-up approach would result in application of the standards to areas outside FERC's jurisdiction: market systems, etc.
- Be clear about "cyber asset" definition (e.g., data?).
- Don't overlook who our audience is.

D. Risk Management and CIP 002

1. CIP 002 Goal

The discussion regarding risk management led to a discussion and testing of a goal statement for CIP 002.

SDT Comments before Ranking

- What are we trying to accomplish w/ CIP-002? What is it's intent/end goal? The intended outcome?
- One possible answer: It's to identify cyber assets that need to be protected (& to what level—Mike Winters)
- What is the best way to identify those cyber assets/the best way to get there? [e.g. FDIC approach]
- By focusing on these two questions, we address the real needs and also satisfy the outcome focus that Mike Assante described this morning.
- The existing taxonomy resulted from the historic focus on power engineering & bulk electric system reliability. Otherwise, a bottom-up approach would result in application of the standards to areas outside FERC's jurisdiction: market systems, etc.
- Be clear about "cyber asset" definition (e.g., data?).
- Also critical to be considered is compromise of assets vs. loss of assets. An instance of malicious compromise of assets might be more damaging than its loss.
- The SDT shouldn't overlook who our audience is.
- Disparity between use of terms "bulk power" and "bulk electric?" The definition in FERC Order 693 clarifies that.
- "Dueling risk assessments." Id critical assets, then cyber. Risk of compliance second. Avoid that. Need is protection of system not just compliance.
- Understandable enough to see real goal is protection and compliance is a side effect not a goal.

The following CIP 002 goal statement was offered for ranking:

The goal/intended outcome of CIP 002 to identify the Cyber Assets (i.e. Programmable electronic devices and communication networks including hardware, software, and data, NERC Glossary) that need to be protected and to identify the level of protection.

Acceptability Ranking Scale	*4 = acceptable, I agree*	*3 = acceptable, I agree with minor reservations*	*2 = not acceptable unless major reservations addressed*	*1 = not acceptable*	*Avg.*
12-5 rank	**16** *(15 +1)*	**4** *(3 +1)*	**0**	**0**	**3.8 of 4**

SDT Comments after Ranking

- Minor Concerns: Some felt that CIP 003 should only identify the CCAs but not go into the level of production.
- The SDT's key task is to identify what is the best way to get there.

2. What Should be the Framework for an Inventory of Cyber Assets?

SDT Discussion Points

a. Overall

- Key questions:
  - Are we getting to the inventory level we need to do under CIP's?
  - How do we set up a process that removes as much as possible that are not essential or critical?
  - How do we conduct the inventory?
  - What is the scope necessary for considering the protection of the infrastructure? To what level do we have to protect our "lifestyle"? (goes to SDT)
- Perhaps have entity initially catalog the cyber assets they use to support environment, then look at those assets from the perspective of how their loss, compromise, etc. would impact the BES
- Mindset problem in industry- interconnectivity and solve problem by changing. This go beyond communication and education.
- CIP 002 how do we apply the inventory framework. How well does it apply in that setting?
- Support the need for inventorying your assets. When you are identifying cyber asset using to control your generation, transmission, coordination centers. "Need to look at who is talking to me."
- Got to do inventory. How you do it is another issue. From a system point. Put arms around the outer limits. There was a clear concept with the first drafting team. We have to acknowledge that you have to know what you have in order to know what and how to protect. In future more routable protocols will produce more attack vectors.

- This is an engineering problem- critical asset facilities, applying engineering principles. Cyber security is not a physics problem. Can't apply the same principles. Developed a risk assessment methodology for 2 control centers. I.d. the 7 filtering criteria for determining the critical cyber asset. Easier today CMBB/ ITELL allow you to do the inventory.
- Will that approach address FERC's concerns?
- Concerns about "cherry picking" that removes things in the purview of CIP. Don't want in there simply because the sanctions threat. Whether this is the purview of NERC or not with the logging process. We do this now at a very high level. If someone can conclude that you can leave off your control system, that is just plain wrong.
- President Sergel's testimony: Characterized CCA as a priority-setting process. However it appears that entities in the industry are using it to identify what is in scope.
- Agreement that there needs to be a risk framework from a control system perspective.

b. Inside-Out Approach

- Good idea to use "inside out" approach
- Identify assets according to the areas they impact
- Go from the inside view inventory and get up. Then how to get auditable compliance. Not lots of confidence there are other options to test.
- Initial focus on cyber systems is logical and valuable. However law on BES vs. BPS differ; BPS is more expansive
- Would this approach lead to very few individual assets that actually would be covered by standard?

c. Systems View

- Needs to be viewed from aggregated view of systems
- What should the system look like- what is the vision?
- Need to know what's there; i.e., inventory
- There are systems that seem obviously critical from a common sense perspective, but fail to appear on lists; the risk assessment process is broken. An electrical engineering point of view is not working
- Mis-configuration is a major problem- systems management on configuration. Problem may be in the field organizations not in the data centers. Supports the idea of taking inventory. Find where it is. What is the outer limit of the system we are operating.
- There are many systems that are used for non-BES processes that would muddy the
- Critical to consider cyber systems and impact on other systems.
- Should market systems be covered by CIP? Taking information and sending instructions.

d. Protection Model

- If we were to devise an approach of a "protection model" that fit with the engineers' mindset, it might be a better way to reach them, teach them and satisfy the needs.
- Industry at large- understand operations thoroughly. Down to an art. Others know how to plan things, same tools with different models. What we don't have, is a protection model. We can use the same tools with a different set of models to figure out what we need to protect.

e. Scope

- If we start inventorying cyber assets- everything in north American grid with a chip in it? If you do at that level, you will have few cyber assets. We have to bump this up to a system level vs. a cyber assets level. Define and do it at that level. Need to look at aggregated points of control.
- Critical asset- 2 things. Protection critical to electric sector and then cyber security.
- Why should we inventory everything initially? Lot of systems that don't and won't have an impact on the BES.
- At what level do we assess what is on our inventory? Individual asset level or a system.
- Clarify what is the scale of inventory- not implying we don't need to do. Not ESO but ERO, write reliability standards.
- Not every cyber system is under the tent. Need to define the filtering what is important/not importance (FERC wide span of control etc.)

f. What Assets Included?

- Not necessarily everything in data center would be included
- Pure, raw, means of production are the key assets to be managed (also the approach original drafting team followed)
- IP-based assets are going to increase
- Problem is not data centers, but field organizations
- Need to protect the control system mechanisms.
- "Criticality of equipment"-- prioritizing how we go after the issue.
- Take an inventory; find where things are, what's the outer limits of systems that are operating
- One device in the substation that can't talk to anyone else will still need protection.
- Even if it's painful, it needs to be done
- Can't do anything unless you have an inventory- boxes and connections.
- Problem with going out and finding all assets- shouldn't be dealing with things outside those critical to the BES. To what level is it required. Identify a second tier level.
- Identifying negative potential impacts of software. The more subtle the error implemented, is a higher impact than a blue screen. Methodology to protect against.

g. Real World Examples

- Real world examples demonstrate the need for inventorying assets, better controlling systems & understanding dependencies. Better defined guidance for priorities is essential
- Similar approach for guidance for the AMI security task force. Domain based analysis. Attacker may go for something trivial vs. valuable and then hop-over. Draw domain around things. Use tools to define domain.
- Three legs of security- "availability" is the third leg. E.g. Southern-- Nuclear plant had an incident. Software on a business network. Communication. Engineer installing update on business system, didn't know it would affect the other system. Fixed.
- Look at incidents at Duke a few years ago. In the Florida incident, can't get a clear line of whether distribution or generation as the source of the threat.

h. Inventory and Compliance

- CIP 1- came up with an auditable framework. Creative way to make this a system to be auditably compliant. Can't model malicious control. PSSC tool leads to gross underestimating of cyber assets. Will have to go to a large set.
- CIP wasn't designed to preclude NIST framework to do your procedures. CIP is the auditable part. That's how the can be utilized and pulled together.
- Manage to compliance vs. cyber assets. N-1 is a part of the problem. Need to tie to something bigger than that. Come up a way to model more than N-1.
- Some of NIST is mandatory. Consider 800 standards. Issue of compliance was dealt with FISMA
- Current auditing in this sector is focused on checklist- dialogue needed- what are you trying to do, what means you have used, how effective. Talked about "quality" of what you did in terms of audit.

3. Draft SDT Inventory Statements

Following the inventory discussion, one member proposed testing SDT support for the following inventory statement:

a. Draft Inventory Statement

Inventory your cyber assets directly related to the operation of your registered NERC functionality:

- Apply a risk methodology to assign a level.
- Apply distinct controls according to the level.
- Inventory for each cyber asset should be: device + o's + function + firmware level.
- These attachments will be critical for patch management and CIP 007R1 testing.

Acceptability	*4 = acceptable, I*	*3 = acceptable, I agree with*	*2 = not acceptable unless major*	*1 = not*	*Avg.*

Ranking Scale	*agree*	*minor reservations*	*reservations addressed*	*acceptable*	
12-6 rank	**2** *(1 + 1)*	**6** *(3 + 3)*	**8** *(7 + 1)*	**4** *(4 + 0)*	**2.3 of 4**

Comments from SDT members finding the statement unacceptable or with major reservations:

- SDT member suggested that the above does not take into consideration of the reliability of the BES sufficiently.
- Need to start with Critical Assets, not devices.
- The starting point of the inventory was too broad; there may be a way of identifying the functions of the devices and including only some, but not all.
- Another member believed that the only important considerations should be only identification of the devices and the function of the devices;
- Add a new bullet that addresses the interconnection of the devices.
- FERC staff stated that the above approach moved in the right direction along with a way to identify other systems such as market systems where appropriate.

b. Draft Inventory Systems Statement

Following the first statement discussion, another SDT member proposed testing support for the following inventory statement:

> **Identify the applications and computer systems within the Industry Controls Systems or information systems as well as the networks within and interfacing with the ICS. The focus should be on systems rather than devices, and should include PLCs, DCS, SCADA, and instrument bases systems that use a monitoring device such as an HMI.**

Acceptability Ranking Scale	*4 = acceptable, I agree*	*3 = acceptable, I agree with minor reservations*	*2 = not acceptable unless major reservations addressed*	*1 = not acceptable*	*Avg.*
12-6 rank	**0**	**9**	**6**	**5**	**2.2 of 4**

Comments from SDT members finding the statement unacceptable or with major reservations:

- One SDT member believes that lack of specifying impact on the BES or BPS made the above unacceptable.
- the bottom up approach is not an acceptable approach.
- Another member believed that the impact profile of the entity should be considered in order for any proposal to be thorough.
- In response to an SDT member question, FERC staff stated that they have no limiting agenda. FERC through its order indicated it wants all of the systems protected to some degree and they like the framework that allows the entities to properly protect the systems as opposed to the CIP systems which are black and white. Under CIP if an asset is not designated as 'Critical' under the current regulations, no security or protection is required. FERC finds this approach lacking. However, FERC staff agreed that not everything should be protected to

the highest level. The assets that really are important should be protected at the highest level; however, nothing should be ignored.

SDT Discussion Points

- Start with a more inclusive view of all these devices. 002-R3 called out now some devices. Attack vectors.
- General concept of inventory of the devices- what are the appropriate filters.
- If we are called to testify- can we respond that our standards process is ensuring we are protecting the BES.
- Why are we here? Because there is inadequate IT life cycle management and power system IT--fragmented within. Are we good stewards of our company's assets and devices used?
- Everything should be inventoried- in corporate IT or power system IT. Reluctant to use IT but call it power system IT. Inadequate change management and loss of control
- Do it by design and explicit management decision. Doing a little bit of "greenfield design" here. Look at all cyber assets. Now with your full inventory.
- "It is all" IT 101- need to know what you are managing in your Skada.

E. Phase II Going Forward Proposal

Following the lunch break, the chair announced that Jackie Collett and William Winters had agreed to draft two "straw" documents to help move the Team forward on the Phase 2:

- Jackie Collett will start from an attempt to protect the best of what exists with the current CIP and incorporate NIST concepts/features.
- William Winters will start with the NIST framework and incorporate the best of the CIP into it.

SDT Advice to the Team Authors

- Authors agree to post to the SDT list
- Produce a workflow chart- business process management flow. Inputs/ outputs.
- Be as visual as possible
- All should read the House Committee's comments on FERC NOPR for CIP standards *(See Appendix #10)*

V. NEXT STEPS AND EVALUATION

A. SDT/NERC Phase 1 Webinar — December 16, 2008

NERC staff presented some information and the SDT discussed the industry "Webinar" on the Phase I SDT products.

- Time/Date: December 16 from 11:30 until 1 p.m. will be the Webinar on the topic of Phase I version of revised CIP.

- There will be a Standards Committee meeting that date.
- Dave Taylor will ask that the Committee listen to the SDT Phase I Webinar.
- SDT members should mark this date on the calendar.
- NERC will be putting out an press announcement on this next week.

The SDT then discussed the presentations for the Webinar:

- The emphasis should be on why we're doing what we're doing, give presentation and allow questions.
- Provide & explain information from the Phase 1 Comment Form.
- New asset implementation plan needs thorough explanation for industry.
- Mention why Phase I being done to begin with, draw attention to government scrutiny that we're receiving.
- Mention the new Congressional Cybersecurity Caucus that's beginning, point to FERC order requirements. Note why a phased approach was taken by the SDT and why we are proposing to take action now.
- Michael Peters agreed to prepare and provide background information.
- The Chair, Vice Chair and Scott Mix will present.
  - Jeri Brewer- 10 minutes on the Background reasons
  - Scott Mix - Actual Changes
  - Kevin Perry - Technical Feasibility Exception
  - Scott Mix - Schedule (near the end)
  - NIST - framework and how it applies in this scenario
- Note that there will be some Canadian government interest in issue. Need to follow-up needed to determine extent and whether it should be addressed.

B. Review of Phase I Schedule

Dave Taylor reviewed the proposed schedule to complete the Phase I process by the end of June, 2009. He noted the concerns that times are tight but noted the schedule provides very limited flexibility to extend the comment time – if we do so it extends the end of the time line into the middle of July

- *December 16 — 11:30 a.m.–1 p.m., NERC Webinar on Phase 1*
- **January 7–9 SDT Meeting, Phoenix, AZ** ½ / 1/½ day format. Wednesday through Friday
- January 15 WebEx meeting
- January 21 WebEx meeting
- **February 2–4, 2009 Meeting in Phoenix, AZ,** ½ / 1/½ day format. Monday through Wednesday
- **February 18–19, 2009 Meeting in Boulder City, NV**
- February 25, 2009 WebEx meeting
- **March 10–11, 2009 Meeting in Tampa, FL,** 2–day format
- March 18, 2009 WebEx meeting

- **April 14–16, 2009 Meeting in Charlotte NC,** ½ / 1/½ day format. Wednesday through Friday
- March 18, 2009 WebEx meeting
- **May 13–14, 2009 Meeting in Dallas TX,** 2–day format
- June, WebEx meeting
- **June 17–18, SDT Meeting, Location TBD,** 2–day format
- June, WebEx meeting

C. January Meeting Agenda Review

NERC announce that the next meeting will take place in Phoenix at an Arizona Public Service Corporation conference facilities and will be a ½ day/1 day/ ½ day format. The proposed agenda items will include:

- Organizing to review and answer industry comments that have been received on the posting of Revised CIP standards from Phase I
- Finalize the SDT input to the NERC Technical Feasibility Exceptions white paper
- Time permitting, continued discussion of the CIP 002 approach to assets in scope for Phase II reviewing papers from Jackie Collett and William Winters.

D. SDT Meeting Evaluation — *What Worked and What Could Be Improved* ?

At the conclusion of the meeting, the facilitators asked the Team to offer an evaluation of the process including what worked well during the meeting and what could be improved.

What worked?

- Meeting in Washington, DC and exposure to Congressional perspective
- Appreciated being tagged onto the NERC CIPC meeting to allow others to participate as well as participation by NIST, Congressional committee member, etc.
- Good sound system.
- Appreciated the debate and the breadth of wisdom knowledge on the team.

What could be improved?

- Appreciate everyone have a chance to voice decisions. However sometimes we are saying the same things and repeating thoughts. Facilitators should try to close off open-ended discussion more quickly and move forward towards resolution.
- Place flip charts higher.

Meeting adjourned at 2:15 p.m. on Friday afternoon.

Appendix # 1 — Meeting Agenda
Washington, D.C. 20005

Thursday, December 4, Day One Agenda

1. 8:00 Opening Remarks - Jeri Domingo-Brewer, Chair & Kevin Perry, Vice Chair
   a. Welcome — announcements, logistics
   b. NERC Antitrust Compliance Guideline
   c. FSU/CRC review of last meeting and adoption of November 12–14 meeting summary
2. 8:15 SDT Organizational Issues: Review of Adopted Consensus Procedures
3. 8:30 NERC Presentation and Discussion of Phase I Communications Plan
4. 9:00 Technical Feasibility Strawman, Review and Refinement
5. 10:00 Break
6. 10:15 Technical Feasibility Strawman, Review and Refinement
7. 12:00 Lunch — working (return to meeting at 12:45PM ET)
8. 12:45 Summary of Phase II Concept- Next Steps
9. 1:15 Potential Application of NIST to CIP-Background Briefing and Discussion
10. 3:00 Stretch Break
11. 3:15 Risk Management — Conceptual Approach
12. 5:00 Recess

Friday, December 5, Day Two Agenda

13. 8:00 Opening, Review of Day One Results and Day Two Agenda — Jeri Domingo-Brewer, Chair & Kevin Perry, Vice Chair
14. 815 SDT Organizational Issues *(TBD)*
15. 8:30 Review and Further Refinement of Technical Feasibility Draft
16. 10:30 BREAK
17. 10:45 Final Review and Adoption of Technical Feasibility Draft
18. 11:15 Continue Review of Risk Management Approach, NIST and CIP 002-009 — Approach
19. 12:00 Lunch — working (return to meeting at 12:45 p.m. ET)
20. 12:45 Implications from Risk Management Discussion for CIP 002
21. 2:30 Review of meeting schedule and drafting assignments
22. 2:45 Next Steps and Evaluation
23. 3:00 Adjourn

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Appendix # 2

Project 2008-06 Cyber Security for Order 706 SDT Attendees List

Washington D.C.
December 4–5, 2008

Attending in Person — SDT Members

1 **Jeri Domingo-Brewer, Chair**	U.S. Bureau of Reclamation
2. Jackie Collett	Manitoba Hydro
3. Jay S. Cribb	Information Security Analyst, Principal, Southern Company Services, Inc.
4. Joe Doetzl	Manager, Information Security, Kansas City Power & Light Co. *(Dec 4, in room, Dec 5 on phone)*
5. Sharon Edwards	Project Manager, Duke Energy
6. Tom Hoffstetter	Midwest ISO, Inc
5. Scott Fixmer	Senior Security Analyst Exelon Corporate Security, Exelon Corp. *(in room Dec 4, by phone Dec 5)*
6. Gerald S. Freese	Director, Enterprise Information Security America Electric Power
7. Richard Kinas	Orlando Utilities Commission
8. John Lim	CISSP, Department Manager, Consolidated Edison Co. NY
9. David Norton	Policy Consultant, CIPEnergy Corporation
10. **Kevin B. Perry, Vice Chair**	Director, IT-Infrastructure, Southwest Power Pool
11. Christopher A. Peters	ICF International
12. David S. Revill	Georgia Transmission Corporation
13. Scott Rosenberger	Luminant Energy
14. Keith Stouffer	National Institute of Standards & Technology
15. John D. Varnell	Technology Director, Tenaska Power Services Co.
16. William Winters	Hydro One Networks, Inc.
1. Roger Lampilla	NERC
2. David Taylor	NERC
3. Scott R. Mix	NERC
4. Todd Thompson	NERC
5. Kelly Ziegler	NERC, *Dec 4*
6. Mike Assante	NERC, *Dec 4*
7. Robert Jones	FSU/FCRC Consensus Center
8. Stuart Langton	FSU/FCRC Consensus Center
9. Joe Bucciero	Bucciero Consulting LLC

SDT Members Attending via WebEx and Phone

1.Phillip Huff	Arkansas Electric Coop Corporation
2.Kevin Sherlin	Sacramento Municipal Utility District *(Day 2)*
3. Bryan Singer	Kenexis Consulting Corp.
4.Jonathan Stanford	Bonneville Power Administration
5.Michael Winters	Hydro One

Attending — Participants *(in person and by phone and WebEx)*

Chuck Abell	Ameren *(in room Dec 4, on phone Dec 5)*

Joseph Baxter	Associated Electrical *(by phone Dec 5)*
Jim Brenton	ERCOT *(in room Dec 4 and Dec 5)*
Markus Braewole	ABB *(by phone Dec 4)*
Steve Breziwa	WAPA *(by phone Dec 4 and Dec 5)*
Mike Fischette	Lansing Board of Water and Light *(by phone Dec 4)*
Jerome Farqumarson	Burns and McDowell Engineering *(in room Dec 4 and Dec 5)*
Brian Harrel,	SERC Reliability *(by phone Dec 4 and Dec 5)*
Darren Highfill	EnerNex Corporation *(in room Dec 4, on phone Dec 5)*
Steve McElwee	PJM *(In room Dec 4, by phone Dec 5)*
William McEvoy	Northern Utilities, *(In room Dec 4)*
Austin Montgomery	Salisbury Institute, CMU *(in room Dec 4, on phone Dec 5)*
Mike Peters	FERC (*in room Dec 4 and Dec 5)*
Matt Schnell	Nebraska Public Power District *(Dec 5 on phone)*
Mark Simon	Encari, *(by phone Dec 4)*
Michael Toeaker	Burns and McDowell Engineering *(by phone Dec 4 and Dec 5)*
Karen Yoder	First Energy *(by phone Dec 4 and Dec 5)*

Appendix # 3
NERC Antitrust Compliance Guidelines

I. General

It is NERC's policy and practice to obey the antitrust laws and to avoid all conduct that unreasonably restrains competition. This policy requires the avoidance of any conduct that
violates, or that might appear to violate, the antitrust laws. Among other things, the antitrust laws forbid any agreement between or among competitors regarding prices, availability of service, product design, terms of sale, division of markets, allocation of customers or any other activity that unreasonably restrains competition.

It is the responsibility of every NERC participant and employee who may in any way affect NERC's compliance with the antitrust laws to carry out this commitment.

Antitrust laws are complex and subject to court interpretation that can vary over time and from one court to another. The purpose of these guidelines is to alert NERC participants and employees to potential antitrust problems and to set forth policies to be followed with respect to activities that may involve antitrust considerations. In some instances, the NERC policy contained in these guidelines is stricter than the applicable antitrust laws. Any NERC participant or employee who is uncertain about the legal ramifications of a particular course of conduct or who has doubts or concerns about whether NERC's antitrust compliance policy is implicated in any situation should consult NERC's General Counsel immediately.

II. Prohibited Activities

Participants in NERC activities (including those of its committees and subgroups) should refrain from the following when acting in their capacity as participants in NERC activities (e.g., at NERC meetings, conference calls and in informal discussions):

- Discussions involving pricing information, especially margin (profit) and internal cost information and participants' expectations as to their future prices or internal costs.
- Discussions of a participant's marketing strategies.
- Discussions regarding how customers and geographical areas are to be divided among competitors.
- Discussions concerning the exclusion of competitors from markets.
- Discussions concerning boycotting or group refusals to deal with competitors, vendors or suppliers.

III. Activities That Are Permitted

From time to time decisions or actions of NERC (including those of its committees and subgroups) may have a negative impact on particular entities and thus in that sense adversely
impact competition. Decisions and actions by NERC (including its committees and

subgroups) should only be undertaken for the purpose of promoting and maintaining the reliability and adequacy of the bulk power system. If you do not have a legitimate purpose consistent with this objective for discussing a matter, please refrain from discussing the matter during NERC meetings and in other NERC-related communications.

You should also ensure that NERC procedures, including those set forth in NERC's Certificate of Incorporation and Bylaws are followed in conducting NERC business. Other NERC procedures that may be applicable to a particular NERC activity include the following:

- Reliability Standards Process Manual
- Organization and Procedures Manual for the NERC Standing Committees
- System Operator Certification Program

In addition, all discussions in NERC meetings and other NERC-related communications should be within the scope of the mandate for or assignment to the particular NERC committee or subgroup, as well as within the scope of the published agenda for the meeting.

No decisions should be made nor any actions taken in NERC activities for the purpose of giving an industry participant or group of participants a competitive advantage over other participants. In particular, decisions with respect to setting, revising, or assessing compliance with NERC reliability standards should not be influenced by anti-competitive motivations.

Subject to the foregoing restrictions, participants in NERC activities may discuss:

- Reliability matters relating to the bulk power system, including operation and planning matters such as establishing or revising reliability standards, special operating procedures, operating transfer capabilities, and plans for new facilities.
- Matters relating to the impact of reliability standards for the bulk power system on electricity markets, and the impact of electricity market operations on the reliability of the bulk power system.
- Proposed filings or other communications with state or federal regulatory authorities or other governmental entities.
- Matters relating to the internal governance, management and operation of NERC, such as nominations for vacant committee positions, budgeting and assessments, and employment matters; and procedural matters such as planning and scheduling meetings.

Any other matters that do not clearly fall within these guidelines should be reviewed with NERC's General Counsel before being discussed.

Appendix # 4

Below is a link to all of the documents reviewed by the SDT 706 Team during the full Team discussions in Washington D.C. as well as Phase 1 SDT Products:

http://www.nerc.com/filez/standards/Project_2008-06_Cyber_Security-RF.html

Appendix # 5 — SDT Consensus Guidelines

Adopted Unanimously, November 13, 2008

The Cyber Security for Order 706 Standard Drafting Team (Team) will seek consensus on its recommendations for any revisions to the CIP standards.

General consensus is a participatory process whereby, on matters of substance, the members strive for agreements which all of the members can accept, support, live with or agree not to oppose. In instances where, after vigorously exploring possible ways to enhance the members' support for the final package of recommended revisions, and the Team finds that 100% acceptance or support of the members present is not achievable, final consensus recommendations will require at least 75% favorable vote of all members present and voting. This super majority decision rule underscores the importance of actively developing consensus throughout the process on substantive issues with the participation of all members. In instances where the Team finds that even 75% acceptance or support is not achievable, the Team's report will include documentation of any differences as well as the options that were considered for which there was greater than 50% support from the Team.

The Team will develop its recommendations using consensus-building techniques with the leadership of the Chair and Vice Chair and the assistance of the facilitators. Techniques such as brainstorming, ranking and prioritizing approaches will be utilized. The Team's consensus process will be conducted as a facilitated consensus-building process. Team members, NERC staff and facilitators will be the only participants seated at the table. Only Team members may participate in consensus ranking or vote on proposals and recommendations. Observers/members of the public are welcome to speak when recognized by the Facilitator and all written comments submitted on the comment forms will be included in the Team and facilitators' summary reports.

The Team will make decisions only when a quorum is present. A quorum shall be constituted by at least 51% of the appointed members being present (simple majority). The Team will utilize Robert's Rules of Order *(as per the NERC Reliability Standards Development Procedure),* as modified by the Team's adopted procedural guidelines, to make and approve motions; however, the 75% supermajority voting requirement will supercede the normal voting requirements used in Robert's Rules of Order for decision making on substantive motions and amendments to motions. In addition, the Council will utilize their adopted meeting guidelines for conduct during meetings. The Council will make substantive recommendations using their adopted facilitated consensus-building procedures, and will use Robert's Rules of Order only for formal motions once a facilitated discussion is completed.

The presiding chair and/or Facilitator of the SDT, in general, should use parliamentary procedures set forth in Robert's Rules of Order, as modified by Council's adopted procedural guidelines.

To enhance the possibility of constructive discussions as members educate themselves on the issues and engage in consensus-building, members agree to refrain from public statements that may prejudge the outcome of the Team's consensus process. In discussing the Team process with the media, members agree to be careful to present only their own views and not the views or statements of other participants and/or may direct such inquiries to the Team Chair and Vice Chair. In addition, in order to provide balance to the Team process, members agree to represent and consult with their stakeholder interest group.

Meeting Guidelines for Participants

Participants' role in meetings:

- Explore possibilities
- Listen to understand (Respect) (limit sidebar conversations)
- Be focused and concise. (Avoid repetition. No need to offer comments in "strong agreement.")
- Focus on issues, not personalities.
- Offer options to address others' concerns.
- No sidebars.
- If participating by phone, indicate who is speaking.
- If participating by phone, please use the mute button. **Do not** put the phone on hold.

Facilitators/Staff role in meetings:

- Assist the Chair and Vice Chair in helping the Team stay on task
- Help the group follow agreed upon ground rules
- Design the meeting and problem solving process in consultation with the Chair and Vice Chair
- Facilitate discussion participation of the Team and other participants
- Prepare agenda packets and reports

Consensus Building Techniques

- **Brainstorming** (green light thinking – not judgmental) At certain points, the facilitator may ask the group to suspend judgment and get ideas onto the table before debating.

- **Name Stacking in Team Discussions** (use of name tents to seek attention)

- **Acceptability Consensus Ranking Scale**
  - Use a consensus acceptability scale to help focus discussion and test support in reviewing substantive issues.

- Use to guide and focus discussion and as a poll to see where the Team stands, not used as a voting mechanism.
- Must be prepared to offer refinements and suggestions to address serious concerns.

4 = Proposal is acceptable as it is
3 = Proposal is acceptable; I can live with it but there are minor concerns to address
2 = Proposal is not acceptable. Proposal may be acceptable if the major concerns are addressed
1 = Proposal is not acceptable

- **Consensus Ranking Scale**
  4. Comfortable—I support proposal as is ♥♥♥♥
  3. Minor Reservations— I can live with this; but would like to see changes as follows♥♥♥ Be prepared to offer specific refinements or changes to address your concerns.
  2. Major Reservations—I can't support this unless following changes are addressed to meet my serious concerns ♥♥ Be prepared to offer specific refinements or changes to address your concerns.
  1. Fatal Flaws—I can't support this ♥ Be prepared to offer alternatives and options that would address your own as well as other's concerns.

- **Robert's Rules of Order and Facilitated Consensus Building Procedures**

The Council will make substantive recommendations using their adopted facilitated consensus-building procedures, and will use Robert's Rules of Order only for formal motions once a facilitated discussion is completed.

Appendix #6
Technical Feasibility Framework White Paper, Scott Mix, NERC
December 5, 2008
Objective, Purpose, Executive Summary, and Background

The purpose of this whitepaper is to describe a proposed framework to address the Technical Feasibility exception provisions introduced in the cyber security standards (CIP-002-1 through CIP-009-1).

The proposed Technical Feasibility Exception process is modeled after the existing Self-report of Non-Compliance with Mitigation Plan process. These similarities are beneficial because it is anticipated that this Technical Feasibility process will be administered by the same staff at both the Regional Entity and ERO.

Definition of Technical Feasibility Exception:
A Technical Feasibility Exception (TFE) may arise when compliance with a requirement or sub-requirement under a CIP Reliability Standard is not technically possible, technically safe or operationally reasonable given the responsible entity's environment. A TFE may be invoked by a Responsible Entity only on a case-by-case basis within the Technical Feasibility Framework.

Application:
A Responsible Entity may invoke a Technical Feasibility Exception (TFE) to a NERC Reliability Standard requirement only where explicitly allowed by the language of a specific standard requirement or sub-requirement. Entities may file a Self-Report of Non-Compliance in cases (1) where they cannot meet the requirements specified in the Reliability Standard and no allowance for a TFE is requested or (2) where the TFE process requirements cannot be met (see FERC Order 706 paragraph 160).

Overview of Essential Elements:
Each TFE request must contain the following essential elements, as described in FERC Order 706, paragraph 222:

- Document mitigation steps.
- Document a remediation plan.
- Document a timeline for eliminating the use of the TFE unless appropriate justification otherwise is provided.
- Provide regular review of whether it continues to be necessary to invoke the exception.
- Document internal approval by the Senior Manager.
- **Document wide-area approval through the ERO's audit process.**

Additionally, the TFE process requires cooperation with the ERO to provide FERC with high-level, wide-area analysis regarding the effects of the TFE on the reliability of the Bulk Electric System. In other words, where a TFE is requested, the impact on interconnected assets must be considered in the development of a remediation plan. This may require coordination with one or more Responsible Entities prior to submission for approval.

In addition to the FERC-directed elements, the following steps are proposed:

- The request must reference the NERC standard and requirement for which the TFE is being requested.
- The "regular" review will be an annual review by the Responsible Entity, Regional Entity, and ERO.
- To facilitate cataloging and tracking, each TFE will be assigned a unique identifier by the Regional Entity that initially receives the TFE, during its review process.

Detailed TFE Process:
The TFE process described herein is based on the existing NERC Compliance Self-Report of Non-Compliance to a Reliability Standard. Each of the essential elements of a TFE report is described below.

The following elements are the responsibility of the Responsible Entity requesting the TFE:

- **Document the exception**
  Each TFE request must reference the specific NERC Reliability Standard requirements or sub-requirements for which the TFE is being requested[1].

  Each TFE request must include a description of the equipment, process, or procedure that prevents the entity from meeting the requirement and explain the reason for the inability to meet the requirement. The justification should focus on the impact to reliability that will result if the requirement cannot be met. Also included in this explanation may be a discussion of the impact of not complying with the requirement, or the impact of improperly literally complying with the requirement. This explanation may also discuss how other factors impact the TFE

[1] It is anticipated that future limitations on where TFEs may be implemented. These limitations will be implemented through modifications to the language of the standards. However, the immediate need for the TFE process requires that the process be developed in advance of these modifications. This proposed process can be implemented in a "field test" environment to allow the future specification of where TFEs may be requested, leading to modifications of the standards language during the next review and approval cycle. The determination as to whether specific requirements should be allowed or disallowed will be deferred until that point. These changes must include a discussion of operational and safety concerns, as discussed in FERC Order 706, paragraphs 178 and 182.

request, such as scarce technical resources, funding availability, equipment availability, etc.

A single TFE request may be associated with multiple equipment instances that share a common issue with regard to the request for the TFE. The issues, situations, mitigations and timelines associated with the TFE are assumed to be similar, and the approval process and impact analysis is expected to be the same.

- **Document and implement mitigating and/or compensating steps**
  Each TFE request must include a description of what actions the Responsible Entity has taken to mitigate, compensate, or lessen the impact of the vulnerability resulting from not being able to comply with the requirement(s) of the Reliability Standard.

  The Responsible Entity must demonstrate the implementation of the mitigating and/or compensating steps to the Regional Entity or the ERO upon request.

  For example, in standard CIP-005 R2.4, if a TFE is being requested for the lack of "strong procedural or technical controls at the access points to ensure authenticity of the accessing party," a mitigation measure might be to implement additional procedures to log all access attempts, more aggressively monitor those logs for unauthorized access, and provide a rapid response when an unauthorized access attempt is detected. In the same example, a compensating measure might be to install an extra in-line communications device to provide the strong authentication component, and force all access to go through the extra device. For purposes of meeting the intent of the requirement, either (or both) could be acceptable, but the chosen method would need to be documented as a mitigating or compensating measure on the TFE request.

- **Document and implement a remediation plan**
  Each TFE request must include a plan for resolving the issue being requested. The remediation plan may provide an extended (e.g., multi-year) plan, for example, to upgrade equipment to versions that are compliant with the Standards requirement, to allow for contract renegotiations, or to allow for regulatory amendment. Alternatively, the remediation plan may be to implement mitigating and/or compensating measures sufficient to protect the component until the equipment for which the TFE is requested reaches its natural end of life and is replaced with a compliant version of the equipment if such equipment exists at that time.

  The Responsible Entity must demonstrate the implementation of the remediation plan to the Regional Entity or the ERO upon request.

- **Document a timeline for eliminating the use of the TFE unless appropriate justification is provided**

Each TFE request must include, as part of its remediation plan, a timeline for the elimination of the need for the TFE. There are no specific requirements for the timeline: it may be short or multi year; it may be detailed or general. It must, however, effectively communicate the Responsible Entity's commitment to resolving the TFE in a manner consistent with maintaining appropriate cyber security and Bulk Electric System reliability.

In some cases, there is no possibility for eliminating the TFE. For example, providing a completely enclosed boundary around a circuit breaker containing an embedded controller that may be classified as a Critical Cyber Asset is not possible. Also, completing personnel risk assessments prior to providing access to Critical Cyber Assets may not be possible during restoration activities after a natural disaster. In such cases, the timeline cannot include a definite end date; therefore, the timeline discussion must include a justification for not having an end date, in addition to specifying that there is no end date. Note that absent a compelling argument for maintaining the TFE request, the Responsible Entity is expected to become compliant with the Reliability Standard requirement upon replacement of the equipment necessitating the TFE request (see FERC Order 706 paragraph 181).

In cases where there are milestones associated with a timeline, the Responsible Entity must show progress meeting the identified milestones to the Regional Entity or the ERO upon request.

- **Provide regular (annual) internal review of whether it continues to be necessary to maintain the exception**
  Each Responsible Entity requesting a TFE must at least annually provide documentation, subject to an audit, that (1) the TFE remains necessary, (2) all remediation plan steps requested by the TFE remain in place and are effective, and (3) any timeline milestones for the elimination of the TFE are on schedule for successful completion of the remediation plan. The documentation must be provided upon request to the Regional Entity and ERO, subject to audit (see also "Sensitive Information" section below).

- **Document internal approval by the Senior Manager**
  The TFE request must be signed and dated by the Senior Manager[2] appointed per Requirement R2 of *CIP-003-1 – Security Management Controls* (no delegation allowed). The request must indicate that the Senior Manager has read and understands all of the components requested by the TFE. The TFE must be reviewed and approved by the Senior Manager at least annually based on the date of the initial TFE request. The Senior Manager must also review and document the progress the Responsible Entity is making toward completing the remediation plan timeline. All missed milestones must be approved by the Senior Manager and reported through the wide-area approval process described below.

- **Submit TFE to Regional Entity (and subsequently to the ERO)**
  Notice of each TFE, when complete and approved by the Responsible Entity's Senior Manager, must be submitted to the compliance office of the appropriate Regional Entity to catalog.

  In each instance, the Responsible Entity must make available for review the details of the TFE, including background and justification for requesting the TFE. Failure to make the TFE details available upon request to authorized representatives of the Regional Entity or ERO, subject to the protection requirements described below, will result in automatic disapproval of the TFE.

  Note that 'submitted' does not necessarily mean that the full TFE documentation is physically or electronically transmitted to the Regional Entity or ERO; it may mean that only a notice of TFE is transmitted to the Regional Entity and ERO.

  The annual re-approval by the Responsible Entity shall re-submitted to the Regional Entity.

The following elements are the responsibility of Regional Entity and ERO:

- **Receive TFE submissions from Responsible Entities**
  Upon submission of the TFE to the Regional Entity, the Regional Entity shall assign a unique catalog identifier to the TFE for further reference. The Regional Entity will ensure that the TFE submissions are complete, and that sufficient information is included to allow the required approvals and analysis.

[2] The Compliance Monitoring and Enforcement Program (CMEP) refers to the approval entity as a Senior Officer. Since the CIP Standards use the term Senior Manager, it is used here. These individuals may be the same person for a specific Responsible Entity.

- **Annual review of TFE**
  The Regional Entity shall review the resubmitted TFE requests to verify that the re-submitted TFE remains valid. Any resubmitted TFE must be analyzed to determine if the TFE must be reapproved.

- **Document wide-area approval through the ERO's audit process**
  Each TFE will be individually analyzed and evaluated prior to approval by the Regional Entity. This analysis and evaluation will take into account all documented particular circumstances and justifications to ensure that the TFE request is valid, that the mitigating and/or compensating measures are appropriate for the TFE and the mitigating and/or compensating measures address the associated impact to the reliable operations of the Bulk Electric System. Only information included in the TFE request will be analyzed; if additional information is required, the TFE request may be updated by the Responsible Entity during the approval analysis and evaluation process.

  Upon receipt of the notice of TFE, the Regional Entity may need to visit the Responsible Entity to review the details of the TFE request in order to analyze and approve the TFE request.

  Included in the Regional Entity approval process is an analysis of the impact to Bulk Electric System reliability for the TFE request. This may require coordination with one or more Responsible Entities prior to submission for approval in addition to any analysis performed by the Regional Entity.

  Updates to the TFE, specifically including updates to the Responsible Entity's completion of milestones in the remediation plan, must also be submitted to the Regional Entity for wide-area approval through the ERO's audit process. Significant unreported and unapproved deviation from meeting the established remediation plan milestone dates may result in a finding of non-compliance with the requirements of the Reliability Standard (see FERC Order 706 paragraph 160).

  Following approval by the Regional Entity, notice of the TFE must be submitted to the ERO for its cataloging and for input into the wide-area analysis, following a similar process.

  Note that separate approval analyses and evaluations will be conducted by the Regional Entity and the ERO; therefore, the TFE request may need to be updated during each review.

Good Faith efforts
Responsible Entities may assume TFEs submitted in good faith are valid and accepted until rejected during the review process, provided the submitted TFE is technically sound, complete and addresses the exemption. Any preliminary rejection determinations should be investigated to determine if the Responsible Entity could modify and resubmit its TFE request to satisfy the reason for the rejections.

Sensitive Information:
It is recognized that many TFE requests will contain sensitive information that must be protected against disclosure, including information that must be protected from Freedom of Information Act (FOIA) release for certain U.S. Government agencies. The Regional Entities and the ERO will work with the Responsible Entity to minimize the possibility of release, but must have access upon request to the TFE requests in order to carry out their regulatory oversight responsibilities. Similarly, the Regional Entity and the ERO will work with the Responsible Entity to ensure that personnel with proper clearances are assigned to the review. Note that inability to review the TFE request, regardless of reason, may result in the disapproval of the request. Information used in the TFE approval and analysis process shall be protected pursuant to NERC's Rules of Procedure section 1500.

As discussed above, review of the TFE by the Regional Entity and ERO does not require that the Regional Entity or ERO take physical possession of the TFE documentation; an on-site review of the TFE documentation will, in many cases, suffice. Actions taken during the review will be mutually agreed to by the Responsible Entity and the reviewing party, and depend on specific legal requirements.

Post Approval Processes required by FERC Order:
Additionally, the TFE process requires cooperation with the ERO to provide the FERC with high-level, wide-area analysis regarding the effects of the TFE on the reliability of the Bulk Electric System.

The ERO, in conjunction with the Regional Entities, must provide a summary report to the FERC providing a high-level, wide-area analysis of the combined effects of all current TFE requests. In order to produce this report, the ERO and the Regional Entities must have appropriate access to the TFE requests from each Responsible Entity. In some cases, it may be necessary to conduct interviews of the individual Responsible Entities to determine the individual and combined impact of the TFE requests within that Responsible Entity, and to determine what wide-area impact, if any, the TFE requests represent in aggregate (see FERC Order 706 paragraph 221). Failure to cooperate with the ERO or the Regional Entity to provide such information upon formal request may result in the rejection of the TFE, and subsequent possibility of non-compliance with the Reliability Standard (see FERC Order 706 paragraph 160).

This wide-area impact analysis shall be re-conducted annually using the most recently submitted TFEs.

Appeals Process:
The appeals process for any TFE request that is rejected by either the Regional Entity or the ERO shall follow the existing Compliance Monitoring and Enforcement program appeals process.

Sample TFE Request Form Fields:
(A form will need to be developed)

Responsible Entity:

Entity Name:

NERC Compliance Registry ID Number:

Compliance Contact Name and Title:

Compliance contact Phone

Compliance Contact email

Technical Contact Name and Title:

Technical Contact Phone:

Technical Contact email:

Date of Technical Feasibility Request submission:

NERC Standard:

Requirement in Standard:

Justification for requesting a Technical Feasibility Exception:

Mitigation and/or Compensation taken:

Remediation Plan steps, milestones and timeline:
If no timeline is given, provide justification for not providing a timeline

Initial Internal Approval by Senior Manager or compliance Senior Officer
Name, title, Date of Approval:

Internal Annual Re-approval by Senior Manager if timeline is longer than one year or no timeline is given

Justification for continued re-approval:

Regional Entity Approval:

Regional Entity:

Technical Feasibility Exception Number (assigned by Regional Entity)

Regional Entity Approval Name

Regional Entity Approval Date

Regional Assessment of impact of Technical Feasibility Exception:

ERO Approval:

ERO Approval Name

ERO Approval Date

ERO Assessment of impact of Technical Feasibility Exception:

Appendix #7 — Phase II Assessment Criteria and Workplan Options

2nd DRAFT PHASE 2 OPTIONS ASSESSMENT CRITERIA

(Presented, Revised and Added to by SDT in its review on November 14, 2008)

1. The option is consistent with the SDT purpose statement and is responsive to the FERC 706 directives and the SAR.
2. C. The option is achievable given the SDT schedule and workplan.
3. The option does most to advance and enhance cyber security
4. The option helps the SDT address the foundational issues with the current standards.
5. The option is capable of implementation.
6. The option is capable of improving compliance.
7. The option helps protect the current investments and wherever possible builds on what has already been done.
8. The option helps to identify and mitigate risk on an ongoing basis
9. The option balances a systems orientation with a facilities orientation to asset protection approach.
10. The option is capable of being extended into related interests by others (distribution, AMI, Smart Grid, etc.).
11. The option enables the industry provide the appropriate level of security (not over securing nor under securing the cyber assets).
12. The option allows for discrimination among the various types of infrastructure that supports the BES

Phase II Work plan Options in Rank Order

(Identified and ranked by SDT November 14, 2008)

1. Address Risk management first then proceed with the rest

Acceptability Ranking Scale	*4 = acceptable, I agree*	*3 = acceptable, I agree with minor reservations*	*2 = not acceptable unless major reservations addressed*	*1 = not acceptable*	*Avg.*
11-14 rank	9	5	4	0	3.27 of 4

2. Adopt/adapt NIST into CIP or Merge NIST into CIP

Acceptability Ranking Scale	*4 = acceptable, I agree*	*3 = acceptable, I agree with minor reservations*	*2 = not acceptable unless major reservations addressed*	*1 = not acceptable*	*Avg.*
11-14 rank	3	9	4	0	2.93 of 4

3. Revise CIP as directed — leave as is and add in only items identified by FERC order

Acceptability Ranking Scale	*4 = acceptable, I agree*	*3 = acceptable, I agree with minor reservations*	*2 = not acceptable unless major reservations addressed*	*1 = not acceptable*	*Avg.*
11-14 rank	5	7	7	0	2.89 of 4

4. Start Over — in terms of a starting point

Acceptability Ranking Scale	*4 = acceptable, I agree*	*3 = acceptable, I agree with minor reservations*	*2 = not acceptable unless major reservations addressed*	*1 = not acceptable*	*Avg.*
11-14 rank	2	5	7	5	2.21 of 4

Appendix #8 Risk Management Worksheet

The SDT Conceptual Approach Risk Management

NOTE: The following points and questions were developed by Kevin Perry to help focus the SDT discussion on risk management. The purpose of this discussion is to provide an initial consideration of important information, options and arguments regarding risk management.

The Current "Consequence-based" Assessment Methodology:

We focus on the facility (asset), employing a "consequences-based" assessment methodology to determine if the facility is essential to the reliable operation of the bulk electric system:

1) Those that are essential are declared to be Critical Assets.
2) We then determine the Cyber Assets essential to the operation of the identified Critical Asset and those become subject to the CIP standards to the exclusion of pretty much all else.

Acceptability Ranking Scale	***4 =*** *acceptable, I agree*	***3 =*** *acceptable, I agree with minor reservations*	***2 =*** *not acceptable unless major reservations addressed*	***1 =*** *not acceptable*	***Avg.***
12-5 rank					

A Draft Problem Statement with the "Consequences-Based" Assessment methodology

The problem presented with this approach is that:

(a) Given the dynamic nature of the transmission system, assets that are critical today might not be tomorrow, and vice versa.
(b) The industry may be "cherry-picking" the Cyber Assets to be protected, along with any collateral Cyber Assets that happen to be connected to the same network segment.
(c) The approach excludes all other Cyber Assets, including Cyber Assets that may provide essential data to the Critical Cyber Assets or may have a trusted relationship (communications path) that could be exploited as an attack vector. And
(d) Once a Cyber Asset is identified as either a Critical Cyber Asset or a collateral Cyber Asset within the Electronic Security Perimeter, all of the requirements of the CIP Cyber Security Standards apply, regardless of the specific Cyber Asset's importance to the reliable operation of the Bulk Electric System.

Acceptability Ranking Scale	***4 =*** *acceptable, I agree*	***3 =*** *acceptable, I agree with minor reservations*	***2 =*** *not acceptable unless major reservations addressed*	***1 =*** *not acceptable*	***Avg.***
12-5 rank					

Overview of Considerations and Key Discussion Questions

1. Should the current Critical Cyber Asset identification process continue without modification?
2. Should the concepts of the NIST Risk Management Framework be adopted in some form, allowing for degrees of importance and corresponding protection controls?
3. Should the same risk management approach be used for field assets (e.g. generation plants, substations) as are used for traditional datacenter environments (e.g. control centers)?
4. Should there be a distinction between Critical Assets and non-Critical Assets (facilities) or should Cyber Assets in all facilities be protected to some degree?
5. Should the Critical Cyber Asset identification process consider the interaction of connected Cyber Assets and the vulnerabilities therein?
6. Should all Cyber Assets at a Critical Asset (facility) be subject to at least a minimal set of basic cyber security standards?
7. How does the NIST framework concept of risk acceptance compare/conflict with the FERC Order 706 and could it work given the FERC's current position on the subject?
8. Should there be some consideration of the importance and potential impact to a Critical Cyber Asset/Bulk Electric System reliability when assessing compliance penalties? For example, if all Cyber Assets at a facility require compliance with at least a minimal set of security standards, should a compliance failure charged against an office PC be subject to the same penalty structure as a Critical Cyber Asset?

Should any of these questions be deleted, reworded or changed in regard to the order?

Are there any additional questions to be considered?

For each question:

- *What are the issues at play in answering this question?*
- *Any guidance or directives from FERC Order 706 that the SDT should consider?*
- *Any additional information needed to answer this question?*
- *Following the discussion of the questions above, are there any draft statements that should be ranked for acceptability? (4,3,2,1 scale)*

FERC 706 Background References

Regarding NIST:

25. The Commission believes that the NIST standards may provide valuable guidance when NERC develops future iterations of the CIP Reliability Standards. Thus, as discussed below, we direct NERC to address revisions to the CIP Reliability Standards CIP-002-1 through CIP-009-1 considering applicable features of the NIST framework. However, in response to Applied Control Solutions, we will not delay the effectiveness of the CIP Reliability Standards by directing the replacement of the current CIP Reliability Standards with others based on the NIST framework.

232. As proposed in the CIP NOPR, the Commission will not at this time direct NERC to incorporate specific provisions of the NIST standards into the CIP Reliability Standards. While commenters provide compelling information that suggests that the NIST standards may provide superior measures for cyber security protection, the Commission is concerned that the immediate adoption of the NIST standards would result in unacceptable delays in having any mandatory and enforceable Reliability Standards that relate to cyber security.

233. The Commission continues to believe – and is further persuaded by the comments – that NERC should monitor the development and implementation of the NIST standards to determine if they contain provisions that will protect the Bulk-Power System better than the CIP Reliability Standards. Moreover, we direct the ERO to consult with federal entities that are required to comply with both CIP Reliability Standards and NIST standards on the effectiveness of the NIST standards and on implementation issues and report these findings to the Commission. Consistent with the CIP NOPR, any provisions that will better protect the Bulk-Power System should be addressed in NERC's Reliability Standards development process. The Commission may revisit this issue in future proceedings as part of an evaluation of existing Reliability Standards or the need for new CIP Reliability Standards, or as part of an assessment of NERC's performance of its responsibilities as the ERO.

Reliability Standards. In other cases, we note that some or all of the additional guidance could be placed in a reference document separate from the CIP Reliability Standards.

Regarding Risk Management

253. The Commission believes that the comments affirm that responsible entities need additional guidance on the development of a risk-based assessment methodology to identify critical assets. While we adopt our CIP NOPR proposal, we recognize that the ERO has already initiated a process to develop such guidance. The CIP NOPR proposedDocket No. RM06-22-000 - 71 -to direct that NERC modify CIP-002-1 to incorporate the guidance. However, we are persuaded by commenters that stress the need for flexibility and the need to take account of the individual circumstances of a responsible entity. Thus, we modify our original proposal and in this Final Order leave to the ERO's discretion whether to incorporate such guidance into the CIP

Reliability Standard, develop it as a separate guidance document, or some combination of the two. A responsible entity, however, remains responsible to identify the critical assets on its system.

254. Commenters raise a number of topics that they believe should be addressed in the NERC guidance, such as how to assess whether a generator or a blackstart unit is "critical" to Bulk-Power System reliability, the proper quantification of risk and frequency, facilities that are relied on to operate or shut down nuclear generating stations, and the consequences of asset failure and asset misuse by an adversary. We believe these are all appropriate topics to be addressed and direct the ERO to consider these commenter concerns when developing the guidance.

255. The Commission proposed in the CIP NOPR that the ERO and Regional Entities provide reasonable technical support to relatively smaller entities that may have difficulty determining whether a particular asset is critical because, for example, the impact of the facility may be dependent on their connection with a transmission owner or operator. While we believe that there is a need to assist entities that lack a wide-area view, we are mindful of the ERO's concern that it would place an undue burden on it and the Regional Entities. If the ERO believes that it and the Regional Entities do not have sufficient resources to take on this responsibility, it should designate another type of entity with a wide-area view, such as a reliability coordinator, to provide needed assistance. This approach is consistent with our determination (discussed later in this Final Rule) regarding the external review of critical asset lists. Accordingly, we direct either the ERO or its designees to provide reasonable technical support to assist entities in determining whether their assets are critical to the Bulk-Power System.

256. Regarding MidAmerican's comments on use of the N minus 1 criterion when applying a risk-based assessment methodology to the identification of critical assets, we agree with MidAmerican that an N minus 1 criterion is not an appropriate risk-based assessment methodology for identifying critical assets. While the N minus 1 criterion may be appropriate in transmission planning, use of an N minus 1 criterion for the risk based assessment in CIP-002-1 would result in the nonsensical result that no substations or generating plants need to be protected from cyber events. A cyber attack can strike multiple assets simultaneously, and a cyber attack can cause damage to an asset for such a time period that other asset outages may occur before the damaged asset can be returned to service. Thus, the fact that the system was developed to withstand the loss of any single asset should not be the basis for not protecting that asset. Also, we note that the definition of "critical assets" is focused on the criticality of the asset, not the Docket No. RM06-22-000 - 72 - likelihood of an outage. Based on this reasoning, in response to US Power, we clarify that a generator should not assume that none of its individual generating assets would be regarded "critical" to the Bulk-Power System.**84**

257. With regard to Xcel's request for clarification regarding the meaning of the phrase "used for initial system restoration," in CIP-002-1, Requirement R1.2.4, we direct the ERO to consider this clarification in its Reliability Standards development process.

258. As to Entergy's suggestion that the ERO provide a DBT profile of potential adversaries, the

ERO should consider this issue in the Reliability Standards development process. Likewise, the ERO should consider Northern California's suggestion that the ERO establish a formal "feedback loop" to assist the industry in developing policies and procedures.**85**

FN84 Further, Requirement R.1.2.3 provides that the risk-based assessment must consider "generation resources that support the reliable operation" of the Bulk-Power System. This language indicates that certain generation facilities, and presumably some facilities within a region identified as critical, must be considered in an assessment. Beyond this, we leave it to the ERO to provide sufficient guidelines to inform generation owners and operators on how to determine whether it should identify a facility as a critical asset. As discussed later in the Final Rule, the Commission will monitor and evaluate the outcome of this endeavor – the list of critical assets.

FN85 Consistent with our approach in Order No. 693, the ERO should address NOPR comments suggesting specific new improvements to the CIP Reliability Standards. The Commission, however, does not direct any outcome other than that the comments receive consideration. See Order No. 693 at P 188.

272. Based on the range of comments received on this topic, the Commission is convinced that the consideration and designation of various types of data as a critical asset or critical cyber asset pursuant to CIP-002-1 is an area that could benefit from Docket No. RM06-22-000 - 76 -greater clarity and guidance from the ERO. Accordingly, the Commission directs the ERO, in developing the guidance discussed above regarding the identification of critical assets, to consider the designation of various types of data as a critical asset or critical cyber asset. In doing so, the ERO should consider Juniper's comments. Further, the Commission directs the ERO to develop guidance on the steps that would be required to apply the CIP Reliability Standards to such data and to consider whether this also covers the computer systems that produce the data.
273. The Commission also agrees with ISO-NE that experience in the implementation of the CIP Reliability Standards may indicate a need to further address this topic in a future proceeding.

Regarding an additional guidance or reference document

61. The Commission received comments on both sides of the issue of specificity. Some commenters caution against the CIP Reliability Standards being too specific, while others request more guidance to help them comply. In general, the Commission believes it is appropriate to provide sufficient guidance to explain Requirements so that responsible entities have a high degree of certainty that they understand what is necessary to comply with a Requirement. More guidance will allow responsible entities to implement measures adapted to their specific situations more consistently and effectively. Additional guidance need not be included in a specific Requirement, but could be in the form of examples. The Commission is not directing that the ERO establish a specific end result. Our concern is simply that responsible entities have guidance on how to achieve an appropriate result in individual cases, which can vary on a case-by-case basis. Therefore, in several instances throughout this Final Rule, the Commission gives the ERO direction to provide additional guidance. In some cases, we require that the guidance be placed in modifications to the CIP

355. The Commission believes that responsible entities would benefit from additional guidance regarding the topics and processes to address in the cyber security policy required pursuant to CIP-003-1. While commenters support the need for guidance, many are concerned about providing such guidance through a modification of the Reliability Standard. We are persuaded by these commenters. Accordingly, the Commission directs the ERO to provide additional guidance for the topics and processes that the required cyber security policy should address. However, we will not dictate the form of such guidance. For example, the ERO could develop a guidance document or white paper that would be referenced in the Reliability Standard. On the other hand, if it is determined in the course of the Reliability Standards development process that specific guidance is important enough to be incorporated directly into a Requirement, this option is not foreclosed. The entities remain responsible, however, to comply with the cyber security policy pursuant to CIP-003-1.

356. In response to ISO/RTO Council, Ontario Power and other commenters, the Commission's intent in the CIP NOPR – as well as the Final Rule – is not to expand the scope of the CIP Reliability Standards. Requirement R1 of CIP-003-1 requires a responsible entity to document and implement a cyber security policy "that represents management's commitment and ability to secure its Critical Cyber Assets." The Requirement then states that the policy, "at a minimum," must address the Requirements in CIP-002-1 through CIP-009-1. The Commission believes that there are other topics, besides those addressed in the Requirements of the CIP reliability Standards, which are relevant to securing critical cyber assets. The Commission identified examples of such topics in the CIP NOPR. Thus, the Commission, in directing the ERO to develop guidance on additional topics relevant to securing critical cyber assets, is not expanding the scope of the CIP Reliability Standards.

408. The Commission agrees with FirstEnergy on the importance of flexibility in developing a mutual distrust posture, but does not see a conflict between the need for flexibility and what it is proposing, which is simply more guidance. More guidance will allow responsible entities to implement measures adapted to their specific situations more consistently and effectively. Additional guidance need not be included in a specific Requirement, but could be in the form of examples. We will leave it to the Reliability Standards development process and the ERO to decide whether some or all of the guidance can be contained in separate guidance documents referenced in the Reliability Standard. In response to Entergy, the Commission is not directing that the ERO establish a specific end result. Our concern is simply that responsible entities have guidance on how to achieve an appropriate result in individual cases, which can vary on a case-by case basis. We disagree that providing useful guidance affects the scope of the Reliability Standards.

502. In response to APPA/LPPC, the Commission clarifies that it does not intend to create an inflexible rule calling for redundant electronic security in all cases. While the Commission directs that a responsible entity must implement two or more distinct security measures when constructing an electronic security perimeter, the specific requirements should be developed in the Reliability Standards development process. This would include whether or not

the second security measure must be "on par" with the first. The Commission also directs the ERO to consider, based on the content of the modified CIP-005-1, whether further guidance on this defense in depth topic should be developed in a reference document outside of the Reliability Standards.

511. The Commission adopts the CIP NOPR's proposal to direct the ERO to identify examples of specific verification technologies that would satisfy Requirement R2.4, while also allowing compliance pursuant to other technically equivalent measures or technologies. In response to commenters, in discussing digital certificates and two-factor authentication, the Commission was providing examples of strong authentication, not limiting authentication to those options. The Commission is not prescribing the specific methods as an exclusive solution pursuant to Requirement R2.4. The ERO can propose an alternative solution that it believes is equally effective and efficient. If the ERO believes it would be helpful to responsible entities, additional guidance beyond the examples that are eventually included in Requirement R2 can be given in a separate reference document. Since we are directing the ERO to provide guidance on what constitutes strong authentication, it is not necessary for the Commission to respond to ISO-NE's request that digital certifications or two-factor authentication are acceptable methods of authentication. In identifying examples or categories of specific verification technologies that would satisfy Requirement R2.4, the ERO should take into account the specific comments raised in this proceeding. Similarly, while encryption is one method to accomplish two-factor authentication, and is an effective process for ensuring authenticity of the accessing party, for some facilities, we leave it to the ERO in the Reliability Standards development process to evaluate whether and how to address the use of encryption. In the alternative, the ERO may identify verification technologies or categories of verification technologies in a reference document.

547. In sum, we direct the ERO to modify Requirement R4 to require these representative active vulnerability assessments at least once every three years, with subsequent annual paper assessments in the intervening years. The ERO should develop the details of how to determine what constitutes a representative system and what modifications require an active vulnerability assessment in the Reliability Standards development process. The revised Reliability Standard should contain the essential requirement that an active assessment must be performed at least once every three years. Based on the amount of guidance contained in the modified Reliability Standard, the ERO should consider at that time whether additional guidance should be provided in a reference document.

575. In response to commenters' questions regarding specific physical access controls, the Commission clarifies that it does not intend to create an inflexible rule calling for redundant physical security. While the Commission continues to believe that a responsible entity must implement two or more distinct and complimentary physical access controls at a physical access point of the perimeter, the specific requirements should be developed in the Reliability Standards development process when the ERO develops its modifications in response to this Final Rule. The Commission also directs the ERO to consider, based on the content of the modified CIP-

006-1, whether further guidance on this defense in depth topic should be developed in a reference document outside of the Reliability Standards.

609 . The Commission has discussed issues related to testing environments in CIP-005-1. In that context, the Commission clarifies the CIP NOPR proposal to require differences between the test environment and the production system to be documented. As stated with respect to CIP-005-1, the Commission understands that test systems do not need to exactly match or mirror the production system in order to provide useful test results. However, to perform active testing, the responsible entities should be required at a minimum to create a "representative system" – one that includes the essential equipment and adequately represents the functioning of the production system. We therefore direct the ERO to develop requirements addressing what constitutes a "representative system" and to modify CIP-007-1 accordingly. The Commission directs the ERO to consider providing further guidance on testing systems in a reference document.

621. While we agree that no safeguard will protect against all malicious or unintentional acts, this does not mean that systems should not be protected against such acts. In response to MidAmerican, the Commission believes that details regarding how to safeguard systems against personnel introducing, maliciously or unintentionally, viruses or malicious software to a cyber asset are best developed in the Reliability Standards development process. The revised Reliability Standard does not need to prescribe a single method for protecting against the introduction of viruses or malicious software to a cyber asset by personnel. However, how a responsible entity does this should be detailed in its cyber security policy so that it can be audited for compliance with the Reliability Standard. The Reliability Standards development process should decide the degree to which the revised CIP-007-1 describes how an entity should protect against personnel introducing viruses or malicious software to a cyber asset. The ERO could also provide additional guidance in a reference document.

629. For the reasons discussed in CIP-005-1, in directing manual log review, the Commission does not require that every log be reviewed in its entirety. Instead, the Commission will allow a manual review of a sampling of log entries or sorted or filtered logs. The Commission recognizes that how a responsible entity determines what sample to review may not be the same for all locations. Therefore, the revised Reliability Standard does not need to prescribe a single method for producing the log sampling. However, how a responsible entity performs this sample review should be detailed in its cyber security policy so that it can be audited to determine compliance with the Reliability Standards. The Reliability Standards development process should decide the degree to which the revised CIP-007-1 describes acceptable log sampling. The ERO could also provide additional guidance on how to create the sampling of log entries, which could be in a reference document. The final review process, however, must be rigorous enough to enable the entity to detect intrusions by attackers.

644. For the reasons discussed in CIP-005-1, in directing manual log review, the Commission does not require that every log be reviewed in its entirety. Instead, the Commission will allow a manual review of a sampling of log entries or sorted or filtered logs. The

Commission recognizes that how a responsible entity determines what sample to review may not be the same for all locations. Therefore, the revised Reliability Standard does not need to prescribe a single method for producing the log sampling. However, how a responsible entity performs this sample review should be detailed in its cyber security policy so that it can be audited to determine compliance with the Reliability Standards. The Reliability Standards development process should decide the degree to which the revised CIP-007-1 describes acceptable log sampling. The ERO could also provide additional guidance on how to create the sampling of log entries, which could be in a reference document. The final review process, however, must be rigorous enough to enable the entity to detect intrusions by attackers.

660. The Commission adopts the CIP NOPR proposal to direct the ERO to provide guidance regarding what should be included in the term reportable incident. In developing the guidance, the ERO should consider the specific examples provided by commenters, described above. However, we direct the ERO to develop and provide guidance on the term reportable incident. The Commission is not opposed to the suggestion that the ERO create a reference document containing the reporting criteria and thresholds and requiring responsible entities to comply with the reference document in the revised Reliability Standard CIP-008-1, but will allow the ERO to determine the best method to accomplish the goal of better defining reportable incident.

725. The Commission adopts, with modifications, the CIP NOPR proposal to develop modifications to CIP-009-1 through the Reliability Standards development process to require an operational exercise once every three years (unless an actual incident occurs, in which case it may suffice), but to permit reliance on table-top exercises annually in other years. Consistent with our goals and discussion of CIP-005-1, the Commission will not at this time require responsible entities to perform full operational exercises. Instead, the Reliability Standard should require the demonstrated recovery of critical cyber assets in a test environment, with the requirements for representative test environments and for addressing differences between the test environment and the production environment, similar to the conditions discussed for live testing in CIP-005-1. Given the range of views presented in comments regarding live testing, as the Reliability Standard development process forms the details of this “demonstrated recovery” concept, it should consider offering guidance beyond the actual Requirements of the Reliability Standard in separate reference documents. The Commission believes this alleviates commenters’ concerns about the risks associated with such testing

Appendix # 9

FERC 706 NOPR Response of House Committee on Homeland Security

UNITED STATES OF AMERICA
BEFORE THE
FEDERAL ENERGY REGULATORY COMMISSION

NOTICE OF PROPOSED RULEMAKING	**) Docket No. RM06-22-000)**
MANDATORY RELIABILITY STANDARDS FOR	**)**
CRITICAL INFRASTRUCTURE PROTECTION	**)**

COMMENTS OF

REP. BENNIE G. THOMPSON (D-MS), CHAIRMAN,
COMMITTEE ON HOMELAND SECURITY
REP. PETER T. KING (R-NY), RANKING MEMBER,
COMMITTEE ON HOMELAND SECURITY

REP. JAMES R. LANGEVIN (D-RI), CHAIRMAN, SUBCOMMITTEE ON EMERGING THREATS, CYBERSECURITY, SCIENCE AND TECHNOLOGY
REP. MICHAEL T. MCCAUL (R-TX), RANKING MEMBER, SUBCOMMITTEE ON EMERGING THREATS, CYBERSECURITY, SCIENCE AND TECHNOLOGY

REP. SHEILA JACKSON-LEE (D-TX), CHAIRMAN,
SUBCOMMITTEE ON TRANSPORTATION SECURITY AND INFRASTRUCTURE PROTECTION
REP. DANIEL E. LUNGREN (R-CA), RANKING MEMBER,
SUBCOMMITTEE ON TRANSPORTATION SECURITY AND INFRASTRUCTURE PROTECTION

ON THE NOTICE OF PROPOSED RULEMAKING FOR MANDATORY RELIABILITY
STANDARDS FOR CRITICAL INFRASTRUCTURE PROTECTION

UNITED STATES OF AMERICA
BEFORE THE
FEDERAL ENERGY REGULATORY COMMISSION

NOTICE OF PROPOSED RULEMAKING	**) Docket No. RM06-22-000)**
MANDATORY RELIABILITY STANDARDS FOR	**)**
CRITICAL INFRASTRUCTURE PROTECTION	**)**

COMMENTS OF

**REP. BENNIE G. THOMPSON (D-MS), CHAIRMAN,
COMMITTEE ON HOMELAND SECURITY
REP. PETER T. KING (R-NY), RANKING MEMBER,
COMMITTEE ON HOMELAND SECURITY**

**REP. JAMES R. LANGEVIN (D-RI), CHAIRMAN, SUBCOMMITTEE ON EMERGING THREATS, CYBERSECURITY, SCIENCE AND TECHNOLOGY
REP. MICHAEL T. MCCAUL (R-TX), RANKING MEMBER, SUBCOMMITTEE ON EMERGING THREATS, CYBERSECURITY, SCIENCE AND TECHNOLOGY**

**REP. SHEILA JACKSON-LEE (D-TX), CHAIRMAN,
SUBCOMMITTEE ON TRANSPORTATION SECURITY AND INFRASTRUCTURE PROTECTION
REP. DANIEL E. LUNGREN (R-CA), RANKING MEMBER,
SUBCOMMITTEE ON TRANSPORTATION SECURITY AND INFRASTRUCTURE PROTECTION**

**ON THE NOTICE OF PROPOSED RULEMAKING FOR MANDATORY RELIABILITY
STANDARDS FOR CRITICAL INFRASTRUCTURE PROTECTION**

I. INTRODUCTION

As Members of Congress, we are pleased to provide these comments in response to the Notice of Proposed Rulemaking ("NOPR") issued in the above-captioned docket.[3] We support the efforts of the Federal Energy Regulatory Commission ("FERC") to require the North American Electric Reliability Corporation ("NERC") to develop modifications to the Critical Infrastructure Protection ("CIP") Reliability Standards. However, we believe that the reliability of the nation's bulk-power system ("BPS") will be better protected by a cyber security standard that incorporates the additional security measures of National Institute of Standards and Technology ("NIST") Special Publication ("SP") 800-53 as applied to industrial control systems.

II. NOTICES AND COMMUNICATIONS

Notices and communications with respect to this filing may be addressed to:
Jacob Olcott
Subcommittee Director and Counsel
Emerging Threats, Cyber security,
Science and Technology Subcommittee
Committee on Homeland Security

[3] Notice of Proposed Rulemaking: Mandatory Reliability Standards for Critical Infrastructure Protection (Docket No. RM06-22-000), issued July 20, 2007.

U.S. House of Representatives
H2-176 Ford House Office Building
Washington, D.C. 20515
(202) 226-2616
(202) 226-4499 (facsimile)
Jacob.Olcott@mail.house.gov

III. BACKGROUND

The BPS of the United States and Canada has more than $1 trillion in asset value, more than 200,000 miles of transmission lines, and more than 800,000 megawatts of generating capability serving over 300 million people.[4] The effective functioning of this infrastructure is highly dependent on control systems, computer-based systems that are used to monitor and control sensitive processes and physical functions. Once largely proprietary, closed-systems, control systems are becoming increasingly connected to open networks, such as corporate intranets and the Internet. According to the United States Computer Emergency Readiness Team ("US-CERT"), "this transition towards widely used technologies and open connectivity exposes control systems to the ever- present cyber risks that exist in the information technology world in addition to control system specific risks."[5]

The cyber risk to these systems is becoming increasingly dangerous. Ten years ago, the President's Commission on Critical Infrastructure Protection ("PCCIP") released a report on the risks associated with interconnected computer systems on the BPS, stating that "the widespread and increasing use of supervisory control and data acquisition systems for control of energy systems provides increasing ability to cause serious damage and disruption by cyber means."[6] Since the release of that study, numerous unintentional cyber incidents – from the Davis-Besse power plant incident in 2003, to the Northeast blackout, to the Browns Ferry nuclear power plant failure in 2006 – suggest that the concerns raised by the PCCIP were warranted.

But nothing quantified the intentional threat to the BPS quite like the experiment performed by the Idaho National Laboratory for the Department of Homeland Security. In September 2007, the Department disclosed that its researchers successfully destroyed a generator while conducting an experimental cyber attack. According to news reports, the attack involved a controlled hack of a replicated control system commonly found throughout the BPS.[7] The

[4] U.S. Government Accountability Office, Report to Congressional Requesters, *Critical Infrastructure Protection: Multiple Efforts to Secure Control Systems Are Under Way, but Challenges Remain* (October 2007), p. 27.

[5] U.S. Department of Homeland Security, Control System Security Program Fact Sheet, available at http://www.us-cert.gov/control_systems/pdf/CSSP_FactSheet_sml.pdf.

[6] U.S. Government Accountability Office, Report to Congressional Requesters, *Critical Infrastructure Protection: Challenges and Efforts to Secure Control Systems* (March 2004), p. 2.

[7] (2007, Sept. 27). "Mouse click could plunge city into darkness, experts say," Retrieved Sept. 28, 2007,

results of this experiment suggest that malicious actors could use the same attack vector against larger generators and other critical rotating equipment that could cause widespread and long-term damage to the electric infrastructure.

Clearly, intentional and unintentional control system failures on the BPS can have a significant and potentially devastating impact on the economy, public health, and national security of the U.S. For a society that runs on power, the discontinuity of electricity to chemical plants, banks, refineries, hospitals, water systems, and military installations presents a terrifying scenario. Economists recently suggested that the loss of power to a third of the country for three months would result in losses of over $700 billion.[8] This figure does not consider the negative societal or health ramifications that such an event would have on the American people.

The FERC proposes to approve a set of reliability standards to help safeguard the nation's BPS against potential disruptions from cyber attacks. The proposed standards require certain users, owners and operators of the grid to establish plans, protocols and controls to safeguard physical and electronic access to systems, to train personnel on security matters, to report security incidents, and to be prepared to recover information. The FERC recently created an Office of Electric Reliability ("OER") designed to focus on the development and implementation of these standards for the users, owners, and operators of the grid.

Unfortunately, we believe the standards proposed by the NERC for adoption by the FERC do not sufficiently ensure the production or delivery of power in the event of intentional or unintentional cyber incidents involving critical infrastructures. We are primarily concerned with five issues: 1) the limitations of CIP-002-1 which exclude critical assets from the risk methodology; 2) the failure of the NOPR to consider the dependencies of critical infrastructures on the BPS; 3) the absence of clearly defined characteristics that will comprise a risk methodology; 4) the interconnectivity of industrial control system data networks; and 5) the vulnerabilities created by using a separate standard for publicly- and privately-owned infrastructures. The fact that our comments are primarily related to the first of the proposed eight standards should not be construed as support of the remaining standards, but demonstrate our deep concern with the implementation of CIP-002-1. We believe that the reliability of the nation's BPS would be better protected by a cyber security standard that incorporates the additional security measures of NIST Special Publication 800-53 as applied to industrial control systems.

IV. DISCUSSIONS OF MAJOR ISSUES OUTLINED IN THE NOPR

Though we applaud FERC's efforts and support many of its modifications to the NERC CIP Reliability Standards, we are primarily concerned with five issues: 1) the limitations of CIP-

---

from http://www.cnn.com/2007/US/09/27/power.at.risk/index.html.

[8] (2007, Sept. 27). "Mouse click could plunge city into darkness, experts say," Retrieved Sept. 28, 2007, from http://www.cnn.com/2007/US/09/27/power.at.risk/index.html.

002-1 which exclude critical assets from the risk methodology; 2) the failure of the NOPR to consider the dependencies of critical infrastructures on the BPS; 3) the absence of clearly defined characteristics that will comprise a risk methodology; 4) the interconnectivity of industrial control system data networks; and 5) the vulnerabilities created by using a separate standard for publicly- and privately-owned infrastructures.

NERC's proposed CIP-002-1 requires an entity to identify its "critical assets" and "critical cyber assets" using a risk-based methodology. Identifying assets is arguably the most important step in the entire assessment process. With control systems becoming increasingly interconnected to each other, and also interconnected with corporate data networks and the Internet, many assets that were once thought to be isolated are now vulnerable.[9] As noted in the FERC Staff Preliminary Assessment, "because CIP-002-1 addresses the assessment methodology and process for identifying critical assets and critical cyber assets, it represents the critical first step that can fundamentally affect the chances for successful implementation of the remaining CIP Reliability Standards."[10] However, if implemented in its present form, CIP-002-1 would not require responsible entities to comprehensively secure "critical assets" that could in fact have a significant impact on the safety and security of the United States.

The problem lies with the NERC definitions of "critical assets." NERC defines "critical cyber assets" as "cyber assets essential to the reliable operation of critical assets."[11] "Critical assets" are defined as "facilities, systems, and equipment that would affect the reliability or operability of the BPS."[12] This is a conceptual mistake that fails to understand the importance of the reliability and operability of individual elements of the grid, which are essential to the delivery of power to the nation's critical infrastructure.

The BPS is an enormous, interconnected network that is both redundant and resilient, making the sole focus on "reliability" and "operability" of the grid as a whole inappropriate. Practically, there are several assets that would fall outside the scope of NERC's definition of "critical" which should not. For instance, although generation units serving communities locally regularly trip offline due to both unexpected events and routine maintenance alike, service to customers generally remains constant. This is a credit to the design of the greater grid, which is engineered to withstand these kinds of singular events.[13] Critical to providing power for

[9] Today, the existing "NERCnet" employed for inter-control center coordination arguably provides a direct link for hacker access to most utility control centers in North America.

[10] Federal Energy Regulatory Commission, *Staff Preliminary Assessment of the North American Electric Reliability Corporation's Proposed Mandatory Reliability Standards on Critical Infrastructure Protection*, December 11, 2006.

[11] North American Electric Reliability Corporation, Critical Infrastructure Protection Reliability Standard 002-1.

[12] North American Electric Reliability Corporation, Critical Infrastructure Protection Reliability Standard 002-1.

[13] North American Electric Reliability Corporation, Transmission Planning Series Standards (TPL).

citizens, businesses, and other critical infrastructures, these units would not be defined as such because they would not affect the reliability or operability of the BPS itself. Similarly, individual substations may experience reliability problems, but unless the load shed exceeds a certain level of megawatts, it is unlikely that a single substation would be recognized as a critical asset under the NERC definition. Telecommunications equipment would also be excluded from the "critical cyber assets" list even though there are documented cases of computer worms denying service from control systems to substations.[14]

Finally, though it is impossible to argue that they are not critical to the safety and security of the U.S., distribution assets would be excluded because they are not essential to reliability of the BPS. Again, real world examples expose problems with this logic. Though the BPS was restored within days to the primary areas affected by Hurricane Katrina, it took some municipal water department pumps over a year to get back up and running because the distribution systems remained off-line. In a June 2007 incident, an outage in Tempe, Arizona, caused by the unexplained activation of the distribution load shedding program in the energy management system affected nearly 100,000 customers.[15]

It is easy to see that an intentional or unintentional cyber incident on the BPS resulting in the disability of any connected asset – from distribution control systems to telecommunications equipment – can have a significant impact on the nation's security. Every critical infrastructure in the country is dependent on the BPS: chemical plants, banks, refineries, hospitals, water systems, and military installations all rely on the effective operation in their region. Focusing on assets relative to the functioning of the grid as a whole misses the importance of each individual asset to the functioning of our society. Unfortunately, recognition of the major infrastructure dependencies on the BPS is entirely absent from the FERC NOPR. Though the NOPR suggests that FERC "will revisit this matter through future proceedings and with other agencies," it is difficult to understand why cross-sector dependencies on the BPS are not the main focus of this standards process.[16] To address this shortcoming, we suggest that every electronically connected asset be considered "critical," as failures on those systems could potentially cause cascading outages of the BPS that could affect every critical infrastructure associated with it.

We strongly support FERC's efforts to provide guidance on the content to be applied in the

---

[14] On June 20, 2003, NERC issued a lessons learned advisory about the "SQL Slammer Worm," a computer worm that caused a denial of service on some Internet hosts and dramatically slowed down general Internet traffic in early 2003. However, CIP-002-1 excludes telecommunications equipment because it is not a "critical asset."

[15] U.S. Department of Energy, Office of Electricity and Delivery Reliability, Infrastructure Security and Energy Restoration, "Energy Assurance Daily" (June 29, 2007), available at http://www.oe.netl.doe.gov/docs/eads/ead062907.pdf.

[16] Notice of Proposed Rulemaking: Mandatory Reliability Standards for Critical Infrastructure Protection (Docket No. RM06-22-000), issued July 20, 2007.

risk-based assessment methodology and require that a senior manager annually review and approve the methodology. We do hope, however, that FERC will create a meaningful deadline for the issuance of such guidance so that it can be effectively promoted across the system. It is true that one singular methodology is probably not appropriate for all situations or entities, but FERC should define the acceptable characteristics of a methodology. While flexibility is important, allowing each responsible entity to craft its own methodology may lead to difficulties in assessing risk across the system. Explicit requirements will avoid a situation where neighboring utilities with the same equipment can have completely different critical cyber assets by virtue of their interpretation of the definitions. Ultimately, however, as long as a responsible entity uses a risk-based methodology focusing on the reliability of the BPS rather than the critical infrastructure end user, safety and security concerns remain paramount. We expect FERC will establish an expedited timeline for responsible entities to complete their assessments and mitigation efforts.

V. CONCLUSIONS AND ACTIONS REQUESTED

The Energy Policy Act of 2005 created a statutory impediment on federal regulators seeking to enact higher standards of security on responsible entities operating within the BPS. We are concerned that the regulatory framework may lead to delays in the implementation of security standards that would better protect the BPS infrastructure and the critical infrastructures that depend on its operation. We endorse the FERC's interpretation of the Section 215 provision requiring "due weight" to be given to the technical expertise of the Electric Reliability Organization with respect to the content of a proposed standard without complete deference.[17] We believe that the FERC staff's technical expertise in control systems and cyber security and the proposals that they set forward in this rulemaking provide a valuable security perspective for the responsible entities charged with implementing these regulations.

A painful lesson from the September 11th attacks on our country is that a system is only as strong as its weakest link. On that day, several terrorists entered the U.S. transportation system through a small airport in Portland, Maine. Once inside the system, they were able to carry out their plans unimpeded. The Federal government must remain vigilant in eliminating weak links that can be exploited by those who wish to do us harm. In that vein, because of the interconnections between publicly- and privately-owned infrastructures that comprise the BPS, we believe that every responsible entity should be held to the same standards for securing their critical assets.

NIST is responsible for developing standards and guidelines, including minimum requirements, for providing adequate information security for all Federal agency non- national security operations and assets. In 2005, NIST released Special Publication (SP) 800-53, "Recommended Security Controls for Federal Information Systems." This publication was originally developed for use with traditional information technology systems. Recently, however, NIST established the Industrial Control System Security Project to improve the security of publicly- and privately-owned industrial control systems. The major focus of the

[17] Energy Policy Act of 2005, Pub. L. No. 109-58, Title XII, Subtitle A, 119 Stat. 594, Section 215(d)(5) (2005).

project is to clarify and rectify problems experienced in applying SP 800-53 to industrial control systems and develop new requirements in those areas. In December 2006, NIST published SP 800-53 Revision-1 that provides interim guidance on the application of the security controls to industrial control systems. These specifications are binding on federal government agencies.

NIST research also focused on comparing the proposed NERC Reliability Standards for cybersecurity with SP 800-53. According to a NIST-sponsored review published in March 2007, an organization conforming to the baseline set of security controls in SP 800-53 will also comply with the management, operational and technical security requirements of the NERC Reliability Standards, though the converse may not be true. For instance, in the Tempe outage and SQL Slammer Worm incidents, the NERC Reliability Standards allow for the exclusions of telecommunications and distribution equipment from the "critical assets" list. Under the SP 800-53 requirements, however, there is no similar exclusion, and it is reasonable to conclude that a responsible entity could identify and mitigate vulnerabilities in these assets prior to an incident. The technical report concluded that the NERC Reliability Standards are both "inadequate for protecting critical national infrastructure," and "inadequate for all electric energy systems when the impact of regional and national power outages is considered."[18] In its February 2007 comments on the FERC Preliminary Staff Assessment, NIST researchers concurred, stating that the NERC standards "do not provide levels of protection commensurate with the mandatory minimum federal standards (FIPS) prescribed by NIST."[19]

Because of the interconnectivity between Federally- and privately-owned elements of the BPS, inconsistent regulatory structures create weak links and potential vulnerabilities in the entire system. A responsible entity in the private sector may fully implement the NERC Reliability Standards but will fall short of the security measures implemented by a public entity. According to a report by MITRE sponsored by NIST, "to date, there has been no serious effort to ensure that the cyber security standards and best practices emerging from the electric power industry are consistent with the federal standards and guidelines being developed by NIST in response to the FISMA."[20] We believe that this is a significant problem that must be addressed immediately. Though the NOPR specifically declines to propose that NERC incorporate any provisions of the NIST guidelines in the CIP Reliability Standards, in light of the security concerns at issue in this rulemaking, we urge the FERC to modify the standard so that it incorporates aspects of SP 800-53 and the related NIST standards.

In closing, we applaud FERC for proposing these regulations. We are hopeful that both FERC and NERC will find these comments helpful and incorporate them when finalizing their

[18] Marshall D. Abrams, "Addressing Industrial Control Systems in NIST Special Publication 800-53," MITRE Technical Report (March 2007), p. 2-20.

[19] Stuart Katzke and Keith Stouffer, *Comments on the FERC Staff Preliminary Assessment of the NERC Proposed Mandatory Reliability Standards on Critical Infrastructure Protection issued* December 11, 2006 Docket RM06-22-000, Feb. 6, 2007.

[20] Marshall D. Abrams, "Addressing Industrial Control Systems in NIST Special Publication 800-53," MITRE Technical Report (March 2007), p. 2-20.

rules for cyber security.

10

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Meeting Agenda

Cyber Security Order 706 SDT — Project 2008-06

December 4, 2008 | 8 a.m.–5 p.m.
December 5, 2008 | 8 a.m.–3 p.m.
Dewey & LeBoeuf, LLP
1101 New York Avenue, N.W — First Floor Conference Room
Washington, D.C. 20005

Proposed Meeting Objectives

- To receive and discuss a NERC presentation on a Phase I communications plan.
- To review, refine, and adopt a Technical Feasibility Paper for Industry review and comment.
- To continue the review of a Phase II work plan.
- To review and discuss the conceptual approach to risk management in Phase II.
- To receive a presentation on NIST and its application to CIP.
- To review assignments and the January 7–8 meeting objectives.

Thursday, December 4, Day One Agenda

1. **8:00 a.m.** Opening Remarks — Jeri Domingo-Brewer, Chair and Kevin Perry, Vice Chair
    a. Welcome — Announcements and Logistics
    b. NERC Antitrust Compliance Guidelines
    c. FSU/CRC review of last meeting and adoption of November 12–14 meeting summary
2. **8:15** SDT Organizational Issues: Review of Adopted Consensus Procedures
3. **8:30** NERC Presentation and Discussion of Phase I Communications Plan
4. **9:00** Technical Feasibility Strawman, Review and Refinement
5. **10:00** Break
6. **10:15** Technical Feasibility Strawman, Review and Refinement
7. **noon** Lunch — Working (return to meeting at 12:45 p.m. ET)
8. **12:45 p.m.** Presentation and Discussion of 2nd Draft Phase II Work plan including

		Applicable FERC Directives
9.	**1:45**	NIST Application to CIP-Background Presentation and Discussion
10.	**3:00**	Stretch Break
11.	**3:15**	Risk Management — Conceptual Approach (Strawman?)
12.	**5:00**	Adjourn

Friday, December 5, Day Two Agenda

13.	**8:00 a.m.**	Opening, Review of Day One Results and Day Two Agenda — Jeri Domingo-Brewer, Chair and Kevin Perry, Vice Chair
14.	**815**	SDT Organizational Issues (TBD)
15.	**8:30**	Review and Further Refinement of Technical Feasibility Draft
16.	**10:30**	BREAK
17.	**10:45**	Final Review and Adoption of Technical Feasibility Draft
18.	**11:15**	Continue Review of Risk Management Approach, NIST and CIP 002-009-Approach
19.	**noon**	Lunch — working (return to meeting at 12:45 p.m. ET)
20.	**12:45 p.m.**	Review of CIP 002 — Issues from FERC Order including NIST comparison
21.	**2:30**	Review of meeting schedule and drafting assignments
22.	**2:45**	Next Steps and Evaluation
23.	**3:00**	Adjourn

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Revised Meeting Agenda

Cyber Security Order 706 SDT — Project 2008-06

January 7, 2009 | 1–5 p.m. PST
January 8, 2009 | 8 a.m.–5 p.m. PST
January 9, 2009 | 8 a.m.–noon PST
Arizona Public Service Deer Valley Campus
Black Canyon 3 Building (BC-3)
2133 W. Peoria Ave.
Phoenix, AZ (609-250-1117)

Wednesday January 7, 2009

1:00 p.m. **Welcome and Opening Remarks — Jeri Domingo-Brewer and Kevin Perry**

a. Roll Call
b. NERC Antitrust Compliance Guidelines
c. FSU/FCRC Review of December meeting and adoption of December 4–5 Meeting Summary

1:15 **Review of Meeting Objectives and Agenda — Jeri Domingo and Bob Jones**

1:20 **Organizational Issues and Review of Phase 1 and early Phase II Schedule — Stuart Langton**

- Review of Phase 1 — Work-plan, January — May 2009 including small group proposal
- Review of Phase 2 — January—June, 2009 — including CIP-002 conceptual approach and industry input and feedback.

2:00 **Overview of Phase I Industry Responses — Number and Issues and Procedure Going Forward — Kevin Perry**

2:30 **Technical Feasibility Exception (TFE) — Briefing on NERC Review and Proposal Going Forward — Scott Mix**

3:00 **Break**

3:15 **TFE White Paper — Review of Changes and Additional Suggestions**

4:00	**Phase I Comment Review and Refinement — Full SDT Discussion of Cross Cutting Issues**
4:50	**Summary of Day One Outcomes and Review of Day Two Agenda**
5:00	**Recess**

Thursday January 8, 2009

8:00	**Welcome — Agenda Review and Review of Day One Results**
8:10	**Phase I Comment Review and Refinement- Plenary Discussion of Overall and Cross Cutting Issues**
9:00	**Break**
9:10	**Possible Small Group Breakouts — Review and Draft Responses**
noon	**Working Lunch *(Return to plenary meeting at 12:45)***
12:45	**Initial Small Group Reports on Draft Responses and Full SDT Discussion**
2:45	**Break**
3:00	**Initial Small Group Reports on Draft Responses and Full SDT Discussion**
4:20	**Next Steps for Drafting Group WebEx Meetings in preparation for February 2–3, 2009 Meeting**
4:50	**Summary of Day Two Outcomes and Review of Day Three Agenda**
5:00	**Recess**

Friday January 9, 2009

8:00	**Welcome and Agenda Review**
8:10	**Learning from Other Initiatives — John Sykes, NERC System Protection and Control Task Force**
9:00	**SDT Discussion of Implications for Phase II 002 Critical Asset Identification**
10:00	**Break**

10:15	**Phase II White Paper Development — Early Thoughts and Preview and Questions of the SDT to aid in the drafting- Jackie Collette and William Winters**
11:30	**Assignments — Next Steps and Review of Work-plan**
noon	**Adjourn**

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Cyber Security Order 706 SDT — Project 2008-06
JANUARY — JUNE 2009 DRAFT SDT SCHEDULE

NOTE: Below are draft considerations developed by the facilitators in consultation with the Chair, Vice Chair and NERC staff and following the December SDT NERC Communication Plan briefing and Phase 1 Webinar on December 16. The facilitators also reviewed the SDT criteria for a "roadmap approach" to revising the CIP standards discussed and refined in Little Rock at its November, 2008 meeting (See pp 4 below for a list of the criteria) These considerations were used to construct a draft schedule for the SDT for the first half of 2009.

Short Term 2009 Schedule Draft Considerations

1. Follow the ANSI standard development process but use creative ways to efficiently secure input from the industry on emerging concepts and approaches to the CIP standards.
2. Seek creative ways to get advice and input to the SDT from experts in cyber security.
3. Seek creative ways to get focused input from industry stakeholders.
4. Take advantage of input opportunities from related NERC committees that will be meeting in the first half of 2009 (e.g. working with the NERC Members Representative Committee, CIPC, BOT, and industry committees such as the Electricity Sector Coordinating Council, etc.)
5. Seek, as soon as possible but no later than late Spring, 2009, to establish a consensus on the way forward for the SDT in its efforts to revise the CIP standards.
6. Track any follow up to the "Securing Cyberspace for the 44th Presidency" report of the Commission on Cybersecurity for the 44th President.

SDT Draft Schedule — January–June 2009

Overview

- 7 SDT Face-to-Face Meetings
- Multiple SDT subgroup and subcommitees WebEx Meetings
- 1 Cyber Expert Workshop (March 10 or 11, 2009)
- 1 NERC CIPC presentation? (Feb. 9, 2009)
- Industry Comments on CIP 002 White Paper (April 17–June 3)
- 1 NERC Members Representative Committee, May 1, 2009

- OTHER MEETINGS?

SDT Draft Schedule — January–June, 2009

1. January 7–9 SDT Meeting — Phoenix, AZ ½–1/½ day format — Wednesday–Friday

- Review of Technical Feasibility Exceptions white paper
- Review of Industry Comments on Phase 1 products- Establish and convene small groups
- Initial Review of Phase 2 White papers

January 15 — WebEx meeting(s)

- Small group draft responses to industry.

January 21 — WebEx meeting(s)

- Small group draft responses to industry.

2. February 2–4, 2009 SDT Meeting — Phoenix, AZ, ½–1/½ day format — Monday–Wednesday

- Review of Small Group responses and recommendations on Industry comments and adopt draft of Phase 1 products, as revised, for review by NERC/Maureen.
- Review of Phase 2 White papers and Testing of a Phase 2 CIP 002 concept going forward

February 9, 2009 — CIPC Meeting — Update on SDT Progress and Input?
February 11 — WebEx meeting

- Phase 2 drafting concept group?

3. February 18–19, 2009 SDT Meeting — Boulder City, NV

- Review of Maureen's comments and adoption of Phase 1 products for balloting.
- Further discussion and adoption of a draft Phase 2 CIP 002 Concept for review by experts and stakeholders in March and beyond.

February 25 — WebEx meeting(s)

- Phase 2 drafting concept group?
- Development of Phase 2 CIP 002 Workshop for review by experts and stakeholders

4. March 10–11, 2009 SDT Meeting — Tampa, FL, 2-day format

- Invited Cyber Security Experts join SDT in a workshop to provide expert feedback to draft CIP 002 concept.
- Further SDT refinement of the CIP 002 proposed concept

March NERC Balloting on Phase 1 Products

March 18 **—** WebEx meeting(s)

- Phase 2 drafting concept group?

5. April 14–16, SDT Meeting, Charlotte NC — ½–1/½ day format. Wednesday-Friday

- Continue review and refinement of 002 concept and adopt White Paper on CIP 002 concept for Industry Comment

Industry Comment Period on White Paper **—** 45-days (April 17–June 3)

*May 1, **NERC Member Representative Committee**, Presentation of the Phase 2 CIP 002 Approach for MRC input. (Agenda item, Possible Workshop?)*

6. May 13–14 — SDT Meeting — Dallas, TX, 2-day format

- Review and respond to MRC input and further SDT refinement of the CIP 002 proposed concept and SDT CIP roadmap.
- Organize SDT in subcommittees to begin effort to draft revisions to CIP 003-008 or to address key issue areas.

June **—** following June 3 — WebEx meeting(s)

- SDT subcommittee meetings to review and draft responses to Industry comments on the CIP 002 concept.

7. June 17–18, SDT Meeting — Location TBD —2-day format

- Review Subcommittee responses to Industry comments on 002 approach
- Charge subcommittees and conduct organizational meetings
- Subcommittees meet to draft revisions to CIP 003-008

June **—** WebEx meeting

- SDT Subcommittee meetings

July–December, 2009 — SDT and subcommittees meet and continue CIP drafting

2nd DRAFT PHASE 2 ROADMAP APPROACH ASSESSMENT CRITERIA

(Presented, Revised, and Added to by SDT in its review on November 14, 2008)

1. The approach is consistent with the SDT purpose statement and is responsive to the FERC 706 directives and the SAR.

2. The approach is achievable given the SDT schedule and workplan.
3. The approach does most to advance and enhance cyber security in the BES.
4. The approach helps the SDT address the foundational issues with the current standards.
5. The approach is capable of implementation.
6. The approach is capable of improving compliance.
7. The approach helps protect the current investments and wherever possible builds on what has already been done.
8. The approach helps to identify and mitigate risk on an ongoing basis.
9. The approach balances a “systems” orientation with a “facilities” orientation to asset protection.
10. The approach is capable of being extended into related interests by others (distribution, AMI, Smart Grid, etc.).
11. The approach enables the industry to provide the appropriate level of security (i.e. not over securing nor under securing the BES cyber assets).
12. The approach allows for discrimination among and targeting the various types of infrastructure that support the BES

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Meeting Summary
Cyber Security Order 706 SDT — Project 2008-06

January 7, 2009 | 1–5 p.m. MST
January 8, 2009 | 8 a.m.–5 p.m. MST
January 9, 2009 | 8 a.m.–5 p.m. MST
Phoenix, Arizona, Arizona Public Service

Provisionally Adopted, February 4, 2009 Finally Adopted as Revised, February 19

SDT Meeting Summary by:

Joe Bucciero, Hal Beardall, Robert Jones, and Stuart Langton

SDT Facilitators
Bucciero Associates,
FCRC Consensus Center, Florida State University

Thanks to Team member Tom Hoffstetter for sharing his meeting notes.

http://www.nerc.com/filez/standards/Project_2008-06_Cyber_Security.html

116-390 Village Blvd.
Princeton, NJ 08540
609.452.8060 | www.nerc.com

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Cyber Security Order 706 Standard Drafting Team
5th Meeting Summary
Phoenix AZ

Meeting Summary Contents

EXECUTIVE SUMMARY

The Chair and Vice Chair welcomed the members and a roll call of members and participants in the room and on the conference call was conducted, following review of the proposed meeting agenda. David Taylor reviewed with the team the need to comply with NERC's Antitrust Guidelines. The SDT agreed to review, and unanimously adopted, the December 4–5, 2008 SDT meeting summary on Friday.

Scott Mix provided an update on the Technical Feasibility Exception process since the SDT December meeting. The Technical Feasibility Exception (TFE) process is based on discussion with utility management. The process is not about the technical requirements and standards that the SDT is addressing, but it is more about whether compliance has been met; compliance is more than just the audit process. Technical feasibility exception was intended to address the issues where compliance could not be met quickly, thereby allowing for good reason to be technically out of compliance while significant issues can be addressed.

The TFE White Paper is being reviewed by NERC management. Compliance and Legal counsel were sought concerning how the white paper should be positioned and what it would mean to enforcement. It needs its own vetting process within NERC, and it may require modification to the Compliance Monitoring and Evaluation Program (CMEP). Changes to the CMEP are applicable across all of NERC's standards, so the TFE needs to well thought through and vetted within NERC. Mike Assante, Chief Security Officer at NERC, has agreed to sponsor the TFE through the compliance process at NERC. Scott Mix will work with NERC Management to determine the best approach for getting this done.

For the Phase I industry comments, Kevin Perry provided a preliminary overview of the 119 pages of comments received from the 46 industry respondents. The comments were organized by NERC staff, and the latest set of comments was released to the SDT on January 7th.

The SDT reviewed several approaches to responding to the Phase I Comments on the cyber security standards. The preferred approach was to break up into small working groups to review an assigned grouping of standards in parallel. There was agreement to begin the Phase II discussion with the full SDT following the development and agreement on responses to Phase I comments. Following the small group breakouts, the full group would meet to discuss the findings and responses from each of the small working groups. Any cross-references or duplicative responses would be addressed and made consistent during this group review session.

Six small working groups were formed to review the industry comments and to develop the SDT's responses. The six groups were created to craft the SDT's responses and to make appropriate edits to the text of the CIP Standards. The six groups and the SDT members participating included:

Working Group Assignments

CIP Standard No.	Questions Nos.	Assignments/Volunteers
002 & 003	Q1 & Q2	Jeri Brewer, Gerald Freese, Dave Norton, Dave Revill
004 & 007	Q3 & Q6	Chris Peters, Keith Stouffer, Mike Winters, William Winters
005 & 006	Q4 & Q5	John Varnell, John Lim, Rich Kinas, Scott Fixmer, Scott Rosenberger
008 & 009	Q7 & Q8	Tom Hofstetter, Joe Doetzel, Kevin Sherlin
Compliance	ALL Qs	Roger Lampila, Todd Thompson, Jackie Collett
Implementation	Q9, Q10, Q11, Q12	Kevin Perry, Scott Mix, Phil Huff
Q13	Q13	Tom Hofstetter and various small groups

The SDT agreed that whatever was not completed by the end of this meeting (January 7–9, 2009) could be taken up in the WebEx calls scheduled for January 15th and January 21st.

The members of each small working group considered the following in presenting their findings to the full group:

- Present substantive issues and responses from most to least contentious (10–15 total minutes for each small group report);
- The full SDT will focus on most contentious issues to confirm response(s); and
- Small groups may reconvene to refine responses.

The SDT reviewed all 13 questions and draft responses to industry comments and addressed compliance issues raised across all of the comments.

On the third day the small groups met again to review and refine their comments further in light of the SDT review on day two.

Scott Mix introduced John Sykes, Vice Chair of the NERC System Protection and Control Subcommittee, which is looking at redundancy in control and protection systems, as an aspect of critical asset protection. They are early in their process of review. The NERC SPCS has written a technical white paper, a proposed working paper for a standard, and has prepared the

presentation. It took two an a half years to get to this point, and the SPCS need lots of industry input because of the high potential cost to the industry. The major topic of discussion was on the methods for determining risk. Do we write a prescriptive standard or a performance-based standard? Key initial question, helped decide on the performance based approach.

Stu Langton introduced a review of the Phase II White Paper process. He reviewed discussion from the previous SDT meeting in Washington where we came away with proposal to prepare and review two straw proposals, one starting from the CIP standards perspective and looking to incorporate applicable NIST concepts and the other starting from the NIST standards perspective and looking to incorporate CIP concepts.

Jackie Collett took a look at the NIST 800-53 standard and sees promise, but she also sees aspects of the standard that may cause concern for electric power systems. Jackie reviewed her take on the original intent of the NERC CIP-002 standard. William Winters offered initial thoughts on his approach from NIST, and how he might address some of the gaps in the standards but recognizing the concerns the industry may have with the NIST risk assessment approach, particularly cost. Bill will look at what NIST does regarding asset identification, focusing on CIP-002, not CIP-003.

This discussion provided guidance to Jackie and William to develop their approaches for review in February. Jackie noted she would be working with other members in developing the paper. William will look at how NIST can be tailored to fit with the CIP standards, while Jackie will look at how the CIP standards can be adopted into the NIST framework. Both will be brought together to see if and how a hybrid might work effectively. Both products will be circulated before the next face-to-face meeting in early February.

The SDT must sign off on the edits by the end of the next meeting in Phoenix to meet the proposed schedule for Phase I. The facilitators reviewed the schedule for the meetings through June 2009.

The meeting was adjourned at 11 a.m. on January 9, 2009.

Fifth Meeting Summary,
January 7–9, 2009
Phoenix, Arizona

I. INTRODUCTIONS, AGENDA REVIEW, PROCEDURES AND OPENING REMARKS

The Chair and Vice Chair welcomed the members and asked NERC staff David Taylor to conduct a roll call of members and participants in the room and on the conference call *(See appendix #2*). They then reviewed with the team and participants the proposed meeting agenda *(See appendix #1*).

David Taylor reviewed with the team the need to comply with NERC's Antitrust Guidelines *(See, appendix #3).* He urged the team and other participants in the process to carefully review the guidelines as they would cover all participants and observers. He urged all to avoid behaviors or appearance that would be anti-competitive nature and also reminded the group of the sensitive nature of the information under discussion.

The Chair noted the December 4–5, 2008 meeting summary had been circulated to members in advance of the meeting. The team unanimously accepted the meeting summary.

II. TECHNICAL FEASIBILITY EXCEPTION- UPDATE, REVIEW AND REFINEMENT

Scott Mix provided an update on the Technical Feasibility Exception process since
The Technical Feasibility Exception (TFE) process is based on discussion with utility management. The process is not about the technical requirements and standards that the SDT is addressing, but it is more about whether compliance has been met; compliance is more than just the audit process. TFE was intended to address the issues where compliance could not be met quickly, thereby allowing for good reason to be technically out of compliance while significant issues can be addressed.

The TFE White Paper is being reviewed by NERC management. Compliance and Legal counsel were sought concerning how the white paper should be positioned and what it would mean to enforcement. It needs its own vetting process within NERC, and it may require modification to the Compliance Monitoring and Evaluation Program (CMEP). Changes to the CMEP are applicable across all of NERC's standards, so the TFE needs to well thought through and vetted within NERC.

Mike Assante, Chief Security Officer at NERC, has agreed to sponsor the TFE through the compliance process at NERC. Scott Mix will work with NERC Management to determine the best approach for getting this done.

Member Comments

- Is there a schedule for getting something to NERC's Mike Assante? Still missing legal information on how it can be done.
- This is an important issue linked to the removal of reasonable business judgment language in Phase I draft changes.

III. PHASE I INDUSTRY COMMENT and SDT RESPONSES

A. Overview of and Response to Phase I Comments on the SDT Standards

Kevin Perry provided a preliminary overview of the 119 pages of comments received from the 46 industry respondents. The comments were organized by NERC staff, and the latest set of comments was released to the SDT on January 7th. In summary, there were:

- No show stoppers
- Lots of duplication in the comments received
- Some comments cross multiple standards with common concerns such as:
  - Compliance Enforcement Authority
  - "a" vs. "the" senior manager and the delegation of authority
- New compliance language received lots of comments and maybe confusing to industry
- Confusion regarding data retention requirements warrants further discussion

Mr. Perry recommended that the Compliance team pay close attention to the new compliance wording so as to avoid the possibility of impact on all of the cyber security standards.

B. SDT Approach for Reviewing Phase I Comments

The SDT reviewed several approaches to responding to the Phase I comments on the cyber security standards. The preferred approach was to break up into small working groups to review an assigned grouping of standards in parallel. There was agreement to begin the Phase II discussion with the full SDT following the development and agreement on responses to Phase I comments. Following the small group breakouts, the full group would meet to discuss the findings and responses from each of the small working groups. Any cross-references or duplicative responses would be addressed and made consistent during this group review session.

The SDT agreed the Industry Comments need to be addressed in January 2009 through the face-to-face meeting and WebEx that were scheduled. The plan was to have the responses ready for review by NERC by the February 2–4, 2009 meeting for group adoption and eventual posting. Some of the SDT member overview comments included:

1. Many comments could be contentious and caution should be taken such that we answer comments at face value and not be drawn into the arguments.
2. Avoid getting drawn into discussing the Aurora incident; it is out of scope for the SDT.

3. A lot of the issues will be considered in Phase II; our response needs to indicate that the commenter should review their concern when Phase II documents are published for industry review and comment. An appropriate response may be "we will consider the comment in Phase II".
4. We will receive comments during the ballot period that we will need to respond to — hopefully the highly contentious issues are identified now before sending out the Phase I standards for ballot.
5. A "significant" change to a standard versus a "minor" change is a judgment call initially made by SDT and reviewed by the NERC Standards Manager (Maureen Long).
6. If we make a significant change to what's already been published, we'll have to seek comments again.
7. If we do not change the requirement but move it to a different standard, is that a significant change? Some clarification may be needed.
8. The plan is to issue the responses to the industry comments without requiring another round of industry comments.
9. If we receive a particularly contentious comment, consider removing the item for further consideration in Phase II.
10. Compliance comments and issues should be addressed by the Compliance small group which will have one SDT member participating.
11. Keep responses short and concise; don't water it down or get involved in long explanations; take the issue on in the appropriate language.
12. Point to reference documents, where appropriate, to address confusion about what some requirements mean.
13. Put the background material into the responses and refer to it, if needed.
14. A suggestion was made to include an introduction to the standards comments response document that describes the approach and what is being accomplished in Phase I and that the major issues will be addressed in Phase II.

C. Small Working Groups

Six small working groups were formed to review the industry comments and to develop the SDT's responses. The six groups were created to craft the SDT's responses and to make appropriate edits to the text of the CIP standards. The six groups and the SDT members participating included:

Working Group Assignments

CIP Standard No.	Questions Nos.	Assignments/Volunteers
002 & 003	Q1 & Q2	Jeri Brewer/Gerald Freese/Dave Norton/Dave Revill
004 & 007	Q3 & Q6	Chris Peters/Keith Stouffer/Mike

		Winters/William Winters
005 & 006	Q4 & Q5	John Varnell/ John Lim/ Rich Kinas/Scott Fixmer/Scott Rosenberger
008 & 009	Q7 & Q8	Tom Hofstetter/Joe Doetzel/Kevin Sherlin
Compliance	ALL Qs	Roger Lampila/Todd Thompson/Jackie Collett
Implementation	Q9, Q10, Q11, Q12	Kevin Perry/Scott Mix/Phil Huff
Q13	Q13	Tom Hofstetter and various small groups

The SDT agreed that whatever was not completed by the end of this meeting (January 7–9, 2009) could be taken up in the WebEx calls scheduled for January 15th and January 21st.

The members of each small working group were asked to consider the following in presenting their findings to the full group:

- Present substantive issues and responses from most to least contentious (10-15 total minutes for each small group report);
- The full SDT will focus on most contentious issues to confirm response(s); and
- Small groups may reconvene to refine responses.

The WebEx was re-initiated after lunch. The facilitator reviewed the expectations for the group reports with a focus on the most contentious or substantive issues that will need full group input for possible additional refinement. The small group reports were brief with an opportunity for groups to revise their work.

1. **Questions 1 and 2 (CIP 002 & 003)**
   Three sets of substantive issues were presented by the small group:

   1. Concern about assigning a senior manager in CIP-003 rather than in CIP-002.
   2. Clarify delegation of senior manger responsibilities
   3. Industry concern about the responsibility of a senior manager vs. a responsible entity (accountability issue?)

   SDT members noted there was some confusion over how to delegate responsibilities. For example, does the Senior Manager have the authority to: assign specific actions; identify which responsibilities will be delegated; document only those delegations assigned to each delegate; delegate authority for specific actions (added) “assigned to the senior manager” to a named delegate or delegates.

Other items the small group proposed for changes included:

- Delete "business phone" information. Yes
- Use "calendar days" throughout CIP-002 to 009.
- Add: "assigned to the senior manager" to a named delegate or delegates.

An SDT straw poll was taken to test support for adding/deleting this language to the requirement: *(Result: 7 for; 10 against, falling short of 75% support).* As a result of poll, the small group would draft responses consistent with this direction back to those offering the language in their comments.

2. **Questions 3 and 6 (CIP-004 and CIP-007)**
Substantive issues raised by the small group and discussed by the SDT included the following:

- How should the SDT respond to comments on addressing ambiguity in "specified circumstances"? SDT should answer that the language was included as directed in FERC Order 706.
- The SDT agreed they need to be specific in responses, not necessarily clarifying, but more explicit about what the drafting team will do with the issue raised.
- Don't change any language, but specify where the wording came from.
- Phase II will not change the language either.
- We should be careful about what we are promising to do in Phase II.
- Leave first sentence of the response as is and refine second sentence into a shorter version without promising future action
- SDT needs to avoid creating any linkages between guidance and standards.

The small group highlighted the following key items for discussion:

1. For R3 — need to specify critical assets. Added access "to critical cyber assets" - much the same reference in R2 — consistency issue
2. Added "all" in front of "other" cyber assets to remove any potential ambiguity. Need to be consistent across the different standards — use the same terminology

A SDT straw poll was taken to test adding securing "all" Cyber Assets within an ESP: (*10 yes; 8 no falling short of 75 percent support).* As a result of the poll, the guidance for the small group was to respond that these changes will be addressed in Phase II.

The SDT agreed not to take out "acceptance of risk" which did not make a substantive change but review of the response for group support. Recommendation is to consider language modification, residual risk analysis would demonstrate that an entity has

exercised due diligence when compensation measures have been applied. The SDT agreed that the response should be that the analysis will be considered in development of the technical feasibility (TFE) process.

Within the measures the team initially agreed with changing M2 to make it consistent with other measures, but suggest alternative language to add "and records" to M2 — (make available documentation "and records of its ports and services process" as specified in Requirement R2). SDT agreed to remove "and records" in order to limit the "heartburn". The SDT could revisit this in Phase 2?

A SDT straw poll taken to test if there support for adding the language. (*7 yes; 11 no falling short of 75 percent support)*. As a result of the poll, the guidance for the small group was to respond that these changes will be addressed in Phase II

The team may need to re-explain in the responses the need for the Phase I changes to meet the June audit deadline set by FERC Order when the response document is sent out for comment.

3. **Questions 4 and 5 (CIP-005 and CIP-006)**
Substantive Issues:

   a. Substitute "subsequent" phases for Phase II; "subsequent" phases anticipate significant changes

   b. Intent is to include only devices that perform access control or monitoring, not those devices that are receiving alerts

   c. Only a few real changes suggested and agreed to:

      - Change "maintain and implement" to "implement and maintain"
      - "Continuous" is a clarification of active escort and SDT agreed not to remove it from the requirement.
      - Agree that R1.4 should reference R4 and not R3
      - Competing authorities is outside the scope of the SDT – offer to refer it to appropriate entity (NERC)
      - Reliability standards only prescribe what and not how

   d. Is there a more positive way of asking commenters to resubmit during the next phase?

   e. In Phase II, the SDT will need to address differences between logging and monitoring/

   f. Use of "documents" versus "documentation" – need to be consistent in use

4. **Questions 7 and 8 (CIP-008 and CIP-009)**
    a. Concern with the addition of the word "dated" into the measures
    b. CIP 009-02 R3 missed the mark
    c. CIP 008-02 confusing wording

Actions:

a. "Dated": Remove the word "dated" from the measures.

b. CIP-009-02 R3:
- Rewrite to meet intent of FERC Order 706 (P731)
- Change control — updates shall be completed within 30 days and communicated within 90 calendar days (What is meant by "completed"?)
- Subsequent discussions led to the decision to wait to make any changes until Phase II development of the CIP Standards.

c. CIP-008-02 R1.3 to R1.6:
- Remove "process for" from each requirement
- R1.5 and R1.6 add annual testing of the response plan
- *Comments:*
    - Add to the compliance section as additional guidance?
    - Is this a major change requiring submittal for further comments?
    - Putting it in as additional compliance guidance - is it a major or minor modification to the standard?
    - This comment is not related to a change made in the last revision to the standards, but rather is a new additional item. These changes should be addressed as part of Phase II
    - Do we need to weigh the number of commenters making the comment that this section is confusing?
- Subsequent discussion to accept these comments or pull them for consideration in Phase II led to the conclusion to wait until Phase II. A good strawman will be needed to start the process at that time.

5. **Questions 9 to 12 (Implementation)**
    Actions to be taken:
    1. Update Implementation Tables
    2. Modify the SDT implementation plan to clarify emergency provision
    3. Change category 3
    4. Change #3 to add "cyber"
    5. Reference "other" CA rather than "non-critical" CA
    6. Modify timeframe to 18 months after the new CCA is identified
    7. Update Table 2 to reflect the addition of two new requirements

8. Any further updates to Table 2

Decisions:

a. Implementation plan as a separate document — consider incorporating in subsequent revisions

b. Guidelines for identifying CA and CCA are being developed

c. Six months is reasonable — the SDT agreed to leave it and not change it as requested to nine months

d. Nuclear facilities are out of the scope of this SDT group

Explanations:

- "In the event of a merger or acquisition of a company, … allow one year for the programs to be harmonized." If one party has a program then continue it while merging, if they have competing programs, then take a year to sort it out – this is a response to a comment, not making any changes to standard.
- Concern about how this applies when a holding company owns separately registered entities — will address by revising language here
- Reviewed items "tossed over the wall" to the Compliance small group

Proposed effective date in implementation plan — add "compliant" to clarify from "auditably compliant". There was no opposition. There was a test to leave without "compliant" which concluded with no objection. Why does title include "proposed"? Not adopted yet and consistent with other implementation plans

6. Compliance Issues (All CIPs)

- The wording in Compliance Section 1.1.1 does not specify who is responsible for the enforcement – not changing it at this time but probably will need to – have sent it to NERC (Maureen) for possible clarification
- Do the terms ERO and Compliance Enforcement Authority need to be defined in the glossary? They are already defined in the Rules of Procedure of NERC, which is hierarchically higher in terms of precedence of documentation, and therefore governs the definition - is not needed in the standards glossary
- Can we just add the same definition to the glossary? Keep response simple here that definition is already covered in the Rules of Procedure.
- "Dated" – do we revise the measures for all standards to include "dated"?
  - (Comment: - In phase I, leave it like it is – revisit in Phase II)
- Reinstate "duly authorized exceptions will not result in non-compliance"?
  - Referring back to NERC for follow up
- "In conjunction" leaves open possible interpretation – referred back to NERC

Jackie will review the rest of the compliance issues, but expects most new comments will be repeats from responses covered above. Jackie will flag any additional issues that the group may need to address.

7. **Question 13 (All CIPs)**
   Tom Hofstetter described how he assigned many of the comments to the appropriate small group. The small groups will need to tag or segregate their responses to Question 13 items so they can be pulled out to include as a set of responses under Question 13.

   Tom reviewed a few basic responses that he proposes to comments that are not related to other questions or small groups.

IV. NERC System Protection and Control Presentation (Jon Sykes)

Scott Mix introduced John Sykes, Vice Chair of the NERC System Protection and Control Subcommittee, which is looking at redundancy in control and protection systems, as an aspect of critical asset protection. They are early in their process of review.

The NERC SPCS has written a technical white paper, a proposed working paper for a standard, and has prepared the presentation. It took two an a half years to get to this point, and the SPCS need lots of industry input because of the high potential cost to the industry.

The major topic of discussion was on the methods for determining risk. Do we write a prescriptive standard or a performance-based standard? Key initial question, helped decide on the performance based approach.

Defined "redundancy", and reviewed protection system performance requirements Methodology to determine adequate redundancy of a Protection System:

- Determine redundancy of the PS
- Ascertain the performance of the PS
- Compare protection systems performance with electric system performance requirements in the TPL standards
- Mitigate all performance shortfalls

V. White Paper Discussions for Phase II

Stu Langton introduced a review of the Phase II White Paper process. He reviewed discussion from the previous SDT meeting in Washington where we came away with proposal to prepare and review two straw proposals, one starting from the CIP standards perspective and looking to incorporate applicable NIST concepts and the other starting from the NIST standards perspective and looking to incorporate CIP concepts.

Jackie Collett took a look at the NIST 800-53 standard and sees promise, but she also sees aspects of the standard that may cause concern for electric power systems. Jackie reviewed her take on the original intent of the NERC CIP 002 Standard.

William Winters offered initial thoughts on his approach from NIST, and how he might address some of the gaps in the standards but recognizing the concerns the industry may have with the NIST risk assessment approach, particularly cost. Bill will look at what NIST does regarding asset identification, focusing on CIP-002, not CIP-003. Some of the items addressed were:

- Concerns expressed by members about the disincentive for including critical assets, particularly for purposes of audits
- NIST may allow for gradations of identification, but that can complicate compliance – will the NIST approach work in the end?
- Energy Act 2005 and FERC announcements have come subsequent to the drafting of the standards which were written for data centers - industry concern about the cost and need for the identification of the critical assets
- Understand where and why we are where we are today to help figure out how to avoid potential industry refection – if industry does not accept, then FERC will do something because they now have clear Congressional support to do something
- Change in administration attitude about the need for industry regulation – we need to do a better job of educating the industry on the cyber risk in order to get their support for changes and limit the gaming – people want to do the right thing, if they understand why
- NERC SDT is focused on critical assets for the bulk power system, but the NIST framework covers the whole spectrum of systems used by the federal system.
- Generation aspect does not necessarily include transmission – we need to understand the different needs but be sure to include both – one size will not fit all for different systems
- Homeland Security list exists – need to resolve how industry list supports this other broader list
- ISA 99 takes a multi-level approach to security
- Identify the cyber assets that do x, y and z – then if it fails what bad happens – that identifies critical cyber assets system wide – is the information flow essential, follow out to find boundary, even where it crosses company boundaries – need to get away from applying physical engineering to the flow of information
- How do we reorganize what we consider critical?

This discussion provided guidance to Jackie and William to develop their approaches for review in February. Jackie noted she would be working with other members in developing the paper.

Should the approaches be combined now for review next time? Or parallel approaches to be merged later? Jackie envisioned parallel approaches to then be compared, and William agreed. Also they agreed that the items/issues identified are the starting points to be addressed. William will look at how NIST can be tailored to fit with the CIP standards, while Jackie will look at how the CIP Standards can be adopted into the NIST framework. Both will be brought together to see if and how a hybrid might work effectively.

Both products will be circulated before the next face-to-face meeting in early February. Some manner of blending will occur — just a matter of how much, however no one is saying start over from scratch. They will review and discuss the balance and trade-offs especially from an audit perspective. Five issue areas will be used by Jackie as part of the problem statement.

VI. Wrap-Up and Next Steps

The SDT must sign off on the edits by the end of the next meeting to meet the proposed schedule for Phase I. The next meeting is scheduled at the downtown Phoenix Hyatt Regency, please plan on staying the full meeting time, and especially try to stick around for the afternoon of the third day.

Beyond the February 2–4, 2009 meeting in Phoenix:

- February 18–19, 2009 in Fairfax, VA (ICFI Offices)
- March 10, 2009 Workshop
  - Progress at the next few meeting will help move us toward preparations for that workshop. Need to work in February to prepare for the workshop, which is preliminarily scheduled in conjunction with the March 10–12, 2009 SDT Meeting in the Orlando or Tampa area.
  - Purpose of the Workshop is to broaden our outreach and enlist review and input from cyber security experts in other industries as well as the electric industry.
  - The workshop will lead to a presentation to the NERC MRC on or about May 1, 2009.
- April 14–16, 2009 in Charlotte (Duke Energy)
- May 14–15, 2009 in Boulder City, NV (Bureau of Reclamation)
- June 17–18, 2009 in Manitoba (Manitoba Hydro)

Web meetings are scheduled approximately one week following each SDT meeting. Industry Webinar meetings are also planned to keep the industry informed on the progress of the Cyber Standards development.

The meeting was adjourned at 11 a.m. on January 9, 2009.

Appendix #1

Revised Meeting Agenda

Arizona Public Service Deer Valley Campus

Wednesday January 7, 2009

1:00 p.m. **Welcome and Opening Remarks — Jeri Domingo-Brewer and Kevin Perry**

a. Roll Call
b. NERC Antitrust Compliance Guidelines
c. FSU/FCRC Review of December meeting and adoption of December 4–5 Meeting Summary

1:15 **Review of Meeting Objectives and Agenda — Jeri Domingo and Bob Jones**

1:20 **Organizational Issues and Review of Phase 1 and early Phase II Schedule — Stuart Langton**

- Review of Phase 1 — Work-plan, January — May 2009 including small group proposal
- Review of Phase 2 — January–June, 2009 — including CIP-002 conceptual approach and industry input and feedback.

2:00 **Overview of Phase I Industry Responses — Number and Issues and Procedure Going Forward — Kevin Perry**

2:30 **Technical Feasibility Exception (TFE) — Briefing on NERC Review and Proposal Going Forward — Scott Mix**

3:00 **Break**

3:15 **TFE White Paper — Review of Changes and Additional Suggestions**

4:00 **Phase I Comment Review and Refinement — Full SDT Discussion of Cross Cutting Issues**

4:50 **Summary of Day One Outcomes and Review of Day Two Agenda**

5:00 **Recess**

Thursday January 8, 2009

8:00 **Welcome — Agenda Review and Review of Day One Results**

8:10 **Phase I Comment Review and Refinement- Plenary Discussion of Overall and Cross Cutting Issues**

9:00 **Break**

9:10 **Possible Small Group Breakouts — Review and Draft Responses**

12:00 **Working Lunch *(Return to plenary meeting at 12:45)***

12:45 **Initial Small Group Reports on Draft Responses and Full SDT Discussion**

2:45 **Break**

3:00	**Initial Small Group Reports on Draft Responses and Full SDT Discussion**
4:20	**Next Steps for Drafting Group WebEx Meetings in preparation for February 2–3, 2009 Meeting**
4:50	**Summary of Day Two Outcomes and Review of Day Three Agenda**
5:00	**Recess**

Friday January 9, 2009

8:00	**Welcome and Agenda Review**
8:10	**Learning from Other Initiatives — John Sykes, NERC System Protection and Control Task Force**
9:00	**SDT Discussion of Implications for Phase II 002 Critical Asset Identification**
10:00	**Break**
10:15	**Phase II White Paper Development — Early Thoughts and Preview and Questions of the SDT to aid in the drafting- Jackie Collette and William Winters**
11:30	**Assignments — Next Steps and Review of Work-plan**
12:00	**Adjourn**

Appendix # 2

Attendees List
January 7–9, 2009

Attending in Person — SDT Members

1 **Jeri Domingo-Brewer, Chair**	U.S. Bureau of Reclamation
2. Jackie Collett	Manitoba Hydro
3. Joe Doetzl	Manager, Information Security, Kansas City Power & Light Co. (Dec 4, in room, Dec 5 on phone)
4. Tom Hoffstetter	Midwest ISO, Inc
5. Scott Fixmer	Senior Security Analyst Exelon Corporate Security, Exelon Corp. (in room Dec 4, by phone Dec 5)
6. Gerald S. Freese	Director, Enterprise Information Security America Electric Power
7. Phillip Huff	Arkansas Electric Coop Corporation
8. Richard Kinas	Orlando Utilities Commission
9. John Lim	CISSP, Department Manager, Consolidated Edison Co. NY
10. David Norton	Policy Consultant, CIPEnergy Corporation
11. **Kevin B. Perry, Vice Chair**	Director, IT-Infrastructure, Southwest Power Pool
12. Christopher A. Peters	ICF International
13. David S. Revill	Georgia Transmission Corporation
14. Scott Rosenberger	Luminant Energy
15.Kevin Sherlin	Sacramento Municipal Utility District (Day 2)
16. Keith Stouffer	National Institute of Standards & Technology
17. John D. Varnell	Technology Director, Tenaska Power Services Co.
18.Michael Winters	Hydro One
19. William Winters	Arizona Public Service.
1. Roger Lampilla	NERC
2. David Taylor	NERC
3. Scott R. Mix	NERC
4. Todd Thompson	NERC
7. Robert Jones	FSU/FCRC Consensus Center Feb 3-4
8. Hal Beardall	FSU/FCRC Consensus Center Feb 2-4
9. Stuart Langton	FSU/FCRC Consensus Center
10. Joe Bucciero	Bucciero Consulting LLC

SDT Members Attending via WebEx and Phone

20. Jay S. Cribb	Southern Company Services, Inc.
21. Sharon Edwards	Project Manager, Duke Energy *Jan. 7.*
22.Jonathan Stanford	Bonneville Power Administration

SDT Members Not Attending

Bryan Singer	Kenexis Consulting Corp.

Appendix # 3

JANUARY — JUNE 2009 DRAFT SDT SCHEDULE

NOTE: Below are draft considerations developed by the facilitators in consultation with the Chair, Vice Chair and NERC staff and following the December SDT NERC Communication Plan briefing and Phase 1 Webinar on December 16. The facilitators also reviewed the SDT criteria for a "roadmap approach" to revising the CIP standards discussed and refined in Little Rock at its November, 2008 meeting (See pp 4 below for a list of the criteria) These considerations were used to construct a draft schedule for the SDT for the first half of 2009.

Short Term 2009 Schedule Draft Considerations

1. Follow the ANSI standard development process but use creative ways to efficiently secure input from the industry on emerging concepts and approaches to the CIP standards.
2. Seek creative ways to get advice and input to the SDT from experts in cyber security.
3. Seek creative ways to get focused input from industry stakeholders.
4. Take advantage of input opportunities from related NERC committees that will be meeting in the first half of 2009 (e.g. working with the NERC Members Representative Committee, CIPC, BOT, and industry committees such as the Electricity Sector Coordinating Council, etc.)
5. Seek, as soon as possible but no later than late Spring, 2009, to establish a consensus on the way forward for the SDT in its efforts to revise the CIP standards.
6. Track any follow up to the "Securing Cyberspace for the 44th Presidency" report of the Commission on Cyber security for the 44th President.

SDT Draft Schedule — January–June 2009

Overview

- 7 SDT Face-to-Face Meetings
- Multiple SDT subgroup and subcommittees WebEx Meetings
- 1 Cyber Expert Workshop (March 10 or 11, 2009)
- 1 NERC CIPC presentation? (Feb. 9, 2009)
- Industry Comments on CIP 002 White Paper (April 17–June 3)
- 1 NERC Members Representative Committee, May 1, 2009
- Other Meetings?

SDT Draft Schedule — January–June, 2009

1. January 7–9 SDT Meeting — Phoenix, AZ ½–1/½ day format — Wednesday–Friday

- Review of Technical Feasibility Exceptions white paper
- Review of Industry Comments on Phase 1 products- Establish and convene small groups
- Initial Review of Phase 2 White papers

January 15 — WebEx meeting(s)

- Small group draft responses to industry.

January 21 — WebEx meeting(s)

- Small group draft responses to industry.

2. February 2–4, 2009 SDT Meeting — Phoenix, AZ, ½–1/½ day format — Monday–Wednesday

- Review of Small Group responses and recommendations on Industry comments and adopt draft of Phase 1 products, as revised, for review by NERC/Maureen.
- Review of Phase 2 White papers and Testing of a Phase 2 CIP 002 concept going forward

February 9, 2009 — CIPC Meeting — Update on SDT Progress and Input?

February 11 — WebEx meeting?

- Phase 2 drafting concept group?

3. February 18–19, 2009 SDT Meeting — Boulder City, NV

- Review of Maureen's comments and adoption of Phase 1 products for balloting.
- Further discussion and adoption of a draft Phase 2 CIP 002 Concept for review by experts and stakeholders in March and beyond.

February 25 — WebEx meeting(s)

- Phase 2 drafting concept group?
- Development of Phase 2 CIP 002 Workshop for review by experts and stakeholders

4. March 10–11, 2009 SDT Meeting — Tampa, FL, 2-day format

- Invited Cyber Security Experts join SDT in a workshop to provide expert feedback to draft CIP 002 concept.
- Further SDT refinement of the CIP 002 proposed concept

March NERC Balloting on Phase 1 Products

March 18 — WebEx meeting(s)

- Phase 2 drafting concept group?

5. April 14–16, SDT Meeting, Charlotte NC — ½–1/½ day format. Wednesday-Friday

- Continue review and refinement of 002 concept and adopt White Paper on CIP 002 concept for Industry Comment

Industry Comment Period on White Paper — 45-days (April 17–June 3)

*May 1, **NERC Member Representative Committee**, Presentation of the Phase 2 CIP 002 Approach for MRC input. (Agenda item, Possible Workshop?)*

6. May 13–14 — SDT Meeting — Dallas, TX, 2-day format

- Review and respond to MRC input and further SDT refinement of the CIP 002 proposed concept and SDT CIP roadmap.
- Organize SDT in subcommittees to begin effort to draft revisions to CIP 003-008 or to address key issue areas.

June — following June 3 — WebEx meeting(s)

- SDT subcommittee meetings to review and draft responses to Industry comments on the CIP 002 concept.

7. June 17–18, SDT Meeting — Location TBD —2-day format

- Review Subcommittee responses to Industry comments on 002 approach
- Charge subcommittees and conduct organizational meetings
- Subcommittees meet to draft revisions to CIP 003-008

June — WebEx meeting

- SDT Subcommittee meetings

July–December, 2009 — SDT and subcommittees meet and continue CIP drafting

2nd DRAFT PHASE 2 ROADMAP APPROACH ASSESSMENT CRITERIA

(Presented, Revised, and Added to by SDT in its review on November 14, 2008)

1. The approach is consistent with the SDT purpose statement and is responsive to the FERC 706 directives and the SAR.
2. The approach is achievable given the SDT schedule and work plan.
3. The approach does most to advance and enhance cyber security in the BES.
4. The approach helps the SDT address the foundational issues with the current standards.
5. The approach is capable of implementation.
6. The approach is capable of improving compliance.
7. The approach helps protect the current investments and wherever possible builds on what has already been done.
8. The approach helps to identify and mitigate risk on an ongoing basis.
9. The approach balances a “systems” orientation with a “facilities” orientation to asset protection.
10. The approach is capable of being extended into related interests by others (distribution, AMI, Smart Grid, etc.).
11. The approach enables the industry to provide the appropriate level of security (i.e. not over securing nor under securing the BES cyber assets).

12. The approach allows for discrimination among and targeting the various types of infrastructure that support the BES

Appendix # 4

NERC Antitrust Compliance Guidelines

I. General

It is NERC's policy and practice to obey the antitrust laws and to avoid all conduct that unreasonably restrains competition. This policy requires the avoidance of any conduct that violates, or that might appear to violate, the antitrust laws. Among other things, the antitrust laws forbid any agreement between or among competitors regarding prices, availability of service, product design, terms of sale, division of markets, allocation of customers or any other activity that unreasonably restrains competition.

It is the responsibility of every NERC participant and employee who may in any way affect NERC's compliance with the antitrust laws to carry out this commitment.

Antitrust laws are complex and subject to court interpretation that can vary over time and from one court to another. The purpose of these guidelines is to alert NERC participants and employees to potential antitrust problems and to set forth policies to be followed with respect to activities that may involve antitrust considerations. In some instances, the NERC policy contained in these guidelines is stricter than the applicable antitrust laws. Any NERC participant or employee who is uncertain about the legal ramifications of a particular course of conduct or who has doubts or concerns about whether NERC's antitrust compliance policy is implicated in any situation should consult NERC's General Counsel immediately.

II. Prohibited Activities

Participants in NERC activities (including those of its committees and subgroups) should refrain from the following when acting in their capacity as participants in NERC activities (e.g., at NERC meetings, conference calls and in informal discussions):

- Discussions involving pricing information, especially margin (profit) and internal cost information and participants' expectations as to their future prices or internal costs.
- Discussions of a participant's marketing strategies.
- Discussions regarding how customers and geographical areas are to be divided among competitors.
- Discussions concerning the exclusion of competitors from markets.
- Discussions concerning boycotting or group refusals to deal with competitors, vendors or suppliers.

III. Activities That Are Permitted

From time to time decisions or actions of NERC (including those of its committees and subgroups) may have a negative impact on particular entities and thus in that sense adversely impact competition. Decisions and actions by NERC (including its committees and subgroups)

should only be undertaken for the purpose of promoting and maintaining the reliability and adequacy of the bulk power system. If you do not have a legitimate purpose consistent with this objective for discussing a matter, please refrain from discussing the matter during NERC meetings and in other NERC-related communications.

You should also ensure that NERC procedures, including those set forth in NERC's Certificate of Incorporation and Bylaws are followed in conducting NERC business. Other NERC procedures that may be applicable to a particular NERC activity include the following:

- Reliability Standards Process Manual
- Organization and Procedures Manual for the NERC Standing Committees
- System Operator Certification Program

In addition, all discussions in NERC meetings and other NERC-related communications should be within the scope of the mandate for or assignment to the particular NERC committee or subgroup, as well as within the scope of the published agenda for the meeting.

No decisions should be made nor any actions taken in NERC activities for the purpose of giving an industry participant or group of participants a competitive advantage over other participants. In particular, decisions with respect to setting, revising, or assessing compliance with NERC reliability standards should not be influenced by anti-competitive motivations.

Subject to the foregoing restrictions, participants in NERC activities may discuss:

- Reliability matters relating to the bulk power system, including operation and planning matters such as establishing or revising reliability standards, special operating procedures, operating transfer capabilities, and plans for new facilities.
- Matters relating to the impact of reliability standards for the bulk power system on electricity markets, and the impact of electricity market operations on the reliability of the bulk power system.
- Proposed filings or other communications with state or federal regulatory authorities or other governmental entities.
- Matters relating to the internal governance, management and operation of NERC, such as nominations for vacant committee positions, budgeting and assessments, and employment matters; and procedural matters such as planning and scheduling meetings.

Any other matters that do not clearly fall within these guidelines should be reviewed with NERC's General Counsel before being discussed.

Appendix # 5

Below is a link to all of the documents reviewed by the SDT during the full team discussions in Washington D.C. as well as Phase 1 SDT Products:

Adopted Unanimously, November 13, 2008

Cyber Security for Order 706 Standard Drafting Team

Consensus Guidelines

The Cyber Security for Order 706 Standard Drafting Team (team) will seek consensus on its recommendations for any revisions to the CIP standards.

General consensus is a participatory process whereby, on matters of substance, the members strive for agreements which all of the members can accept, support, live with or agree not to oppose. In instances where, after vigorously exploring possible ways to enhance the members' support for the final package of recommended revisions, and the team finds that 100 percent acceptance or support of the members present is not achievable, final consensus recommendations will require at least 75 percent favorable vote of all members present and voting. This super majority decision rule underscores the importance of actively developing consensus throughout the process on substantive issues with the participation of all members. In instances where the team finds that even 75 percent acceptance or support is not achievable, the team's report will include documentation of any differences as well as the options that were considered for which there was greater than 50 percent support from the team.

The team will develop its recommendations using consensus-building techniques with the leadership of the Chair and Vice Chair and the assistance of the facilitators. Techniques such as brainstorming, ranking and prioritizing approaches will be utilized. The team's consensus process will be conducted as a facilitated consensus-building process. Team members, NERC staff and facilitators will be the only participants seated at the table. Only team members may participate in consensus ranking or vote on proposals and recommendations. Observers or members of the public are welcome to speak when recognized by the Facilitator and all written comments submitted on the comment forms will be included in the Team and facilitators' summary reports.

The team will make decisions only when a quorum is present. A quorum shall be constituted by at least 51 percent of the appointed members being present (simple majority). The ream will utilize Robert's Rules of Order (as per the NERC Reliability Standards Development Procedure), as modified by the Team's adopted procedural guidelines, to make and approve motions;

however, the 75 percent supermajority voting requirement will supersede the normal voting requirements used in Robert's Rules of Order for decision making on substantive motions and amendments to motions. In addition, the Council will utilize their adopted meeting guidelines for conduct during meetings. The Council will make substantive recommendations using their adopted facilitated consensus-building procedures, and will use Robert's Rules of Order only for formal motions once a facilitated discussion is completed.

The presiding chair and/or Facilitator of the SDT, in general, should use parliamentary procedures set forth in Robert's Rules of Order, as modified by Council's adopted procedural guidelines.

To enhance the possibility of constructive discussions as members educate themselves on the issues and engage in consensus-building, members agree to refrain from public statements that may prejudge the outcome of the team's consensus process. In discussing the team process with the media, members agree to be careful to present only their own views and not the views or statements of other participants and/or may direct such inquiries to the team Chair and Vice Chair. In addition, in order to provide balance to the team process, members agree to represent and consult with their stakeholder interest group.

Meeting Guidelines for Participants

Participants' role in meetings:

- Explore possibilities
- Listen to understand (Respect) (limit sidebar conversations)
- Be focused and concise. (Avoid repetition. No need to offer comments in "strong agreement.")
- Focus on issues, not personalities.
- Offer options to address others' concerns.
- No sidebars.
- If participating by phone, indicate who is speaking.
- If participating by phone, please use the mute button. Do not put the phone on hold.

Facilitators/Staff role in meetings:

- Assist the Chair and Vice Chair in helping the Team stay on task
- Help the group follow agreed upon ground rules
- Design the meeting and problem solving process in consultation with the Chair and Vice Chair
- Facilitate discussion participation of the Team and other participants
- Prepare agenda packets and reports

Consensus Building Techniques

- Brainstorming (green light thinking – not judgmental) At certain points, the facilitator may ask the group to suspend judgment and get ideas onto the table before debating.

- Name Stacking in Team Discussions (use of name tents to seek attention)

- Acceptability Consensus Ranking Scale
  - Use a consensus acceptability scale to help focus discussion and test support in reviewing substantive issues.
  - Use to guide and focus discussion and as a poll to see where the Team stands, not used as a voting mechanism.
  - Must be prepared to offer refinements and suggestions to address serious concerns.

  4 = Proposal is acceptable as it is
  3 = Proposal is acceptable; I can live with it but there are minor concerns to address
  2 = Proposal is not acceptable. Proposal may be acceptable if the major concerns are addressed
  1 = Proposal is not acceptable

- Consensus Ranking Scale

  4. Comfortable—I support proposal as is ♥♥♥♥
  3. Minor Reservations— I can live with this; but would like to see changes as follows♥♥♥ Be prepared to offer specific refinements or changes to address your concerns.
  2. Major Reservations—I can't support this unless following changes are addressed to meet my serious concerns ♥♥ Be prepared to offer specific refinements or changes to address your concerns.
  1. Fatal Flaws—I can't support this ♥ Be prepared to offer alternatives and options that would address your own as well as other's concerns.

- Robert's Rules of Order and Facilitated Consensus Building Procedures

The Council will make substantive recommendations using their adopted facilitated consensus-building procedures, and will use Robert's Rules of Order only for formal motions once a facilitated discussion is completed.

Appendix # 6

FERC 706 Background References

Regarding NIST:

25. The Commission believes that the NIST standards may provide valuable guidance when NERC develops future iterations of the CIP Reliability Standards. Thus, as discussed below, we direct NERC to address revisions to the CIP Reliability Standards CIP-002-1 through CIP-009-1 considering applicable features of the NIST framework. However, in response to Applied Control Solutions, we will not delay the effectiveness of the CIP Reliability Standards by directing the replacement of the current CIP Reliability Standards with others based on the NIST framework.

232. As proposed in the CIP NOPR, the Commission will not at this time direct NERC to incorporate specific provisions of the NIST standards into the CIP Reliability Standards. While commenters provide compelling information that suggests that the NIST standards may provide superior measures for cyber security protection, the Commission is concerned that the immediate adoption of the NIST standards would result in unacceptable delays in having any mandatory and enforceable Reliability Standards that relate to cyber security.

233. The Commission continues to believe – and is further persuaded by the comments – that NERC should monitor the development and implementation of the NIST standards to determine if they contain provisions that will protect the Bulk-Power System better than the CIP Reliability Standards. Moreover, we direct the ERO to consult with federal entities that are required to comply with both CIP Reliability Standards and NIST standards on the effectiveness of the NIST standards and on implementation issues and report these findings to the Commission. Consistent with the CIP NOPR, any provisions that will better protect the Bulk-Power System should be addressed in NERC's Reliability Standards development process. The Commission may revisit this issue in future proceedings as part of an evaluation of existing Reliability Standards or the need for new CIP Reliability Standards, or as part of an assessment of NERC's performance of its responsibilities as the ERO.

Reliability Standards. In other cases, we note that some or all of the additional guidance could be placed in a reference document separate from the CIP Reliability Standards.

Regarding Risk Management

253. The Commission believes that the comments affirm that responsible entities need additional guidance on the development of a risk-based assessment methodology to identify critical assets. While we adopt our CIP NOPR proposal, we recognize that the ERO has already initiated a process to develop such guidance. The CIP NOPR proposed Docket No. RM06-22-000 - 71 -to direct that NERC modify CIP-002-1 to incorporate the guidance. However, we are persuaded by commenters that stress the need for flexibility and the need to take account of the individual

circumstances of a responsible entity. Thus, we modify our original proposal and in this Final Order leave to the ERO's discretion whether to incorporate such guidance into the CIP Reliability Standard, develop it as a separate guidance document, or some combination of the two. A responsible entity, however, remains responsible to identify the critical assets on its system.

254. Commenters raise a number of topics that they believe should be addressed in the NERC guidance, such as how to assess whether a generator or a blackstart unit is "critical" to Bulk-Power System reliability, the proper quantification of risk and frequency, facilities that are relied on to operate or shut down nuclear generating stations, and the consequences of asset failure and asset misuse by an adversary. We believe these are all appropriate topics to be addressed and direct the ERO to consider these commenter concerns when developing the guidance.

255. The Commission proposed in the CIP NOPR that the ERO and Regional Entities provide reasonable technical support to relatively smaller entities that may have difficulty determining whether a particular asset is critical because, for example, the impact of the facility may be dependent on their connection with a transmission owner or operator. While we believe that there is a need to assist entities that lack a wide-area view, we are mindful of the ERO's concern that it would place an undue burden on it and the Regional Entities. If the ERO believes that it and the Regional Entities do not have sufficient resources to take on this responsibility, it should designate another type of entity with a wide-area view, such as a reliability coordinator, to provide needed assistance. This approach is consistent with our determination (discussed later in this Final Rule) regarding the external review of critical asset lists. Accordingly, we direct either the ERO or its designees to provide reasonable technical support to assist entities in determining whether their assets are critical to the Bulk-Power System.

256. Regarding MidAmerican's comments on use of the N minus 1 criterion when applying a risk-based assessment methodology to the identification of critical assets, we agree with MidAmerican that an N minus 1 criterion is not an appropriate risk-based assessment methodology for identifying critical assets. While the N minus 1 criterion may be appropriate in transmission planning, use of an N minus 1 criterion for the risk based assessment in CIP-002-1 would result in the nonsensical result that no substations or generating plants need to be protected from cyber events. A cyber attack can strike multiple assets simultaneously, and a cyber attack can cause damage to an asset for such a time period that other asset outages may occur before the damaged asset can be returned to service. Thus, the fact that the system was developed to withstand the loss of any single asset should not be the basis for not protecting that asset. Also, we note that the definition of "critical assets" is focused on the criticality of the asset, not the Docket No. RM06-22-000 - 72 - likelihood of an outage. Based on this reasoning, in response to US Power, we clarify that a generator should not assume that none of its individual generating assets would be regarded "critical" to the Bulk-Power System.**84**

257. With regard to Xcel's request for clarification regarding the meaning of the phrase "used for initial system restoration," in CIP-002-1, Requirement R1.2.4, we direct the ERO to consider this clarification in its Reliability Standards development process.

258. As to Entergy's suggestion that the ERO provide a DBT profile of potential adversaries, the ERO should consider this issue in the Reliability Standards development process. Likewise, the ERO should consider Northern California's suggestion that the ERO establish a formal "feedback loop" to assist the industry in developing policies and procedures.**85**

FN84 Further, Requirement R.1.2.3 provides that the risk-based assessment must consider "generation resources that support the reliable operation" of the Bulk-Power System. This language indicates that certain generation facilities, and presumably some facilities within a region identified as critical, must be considered in an assessment. Beyond this, we leave it to the ERO to provide sufficient guidelines to inform generation owners and operators on how to determine whether it should identify a facility as a critical asset. As discussed later in the Final Rule, the Commission will monitor and evaluate the outcome of this endeavor – the list of critical assets.

FN85 Consistent with our approach in Order No. 693, the ERO should address NOPR comments suggesting specific new improvements to the CIP Reliability Standards. The Commission, however, does not direct any outcome other than that the comments receive consideration. See Order No. 693 at P 188.

272. Based on the range of comments received on this topic, the Commission is convinced that the consideration and designation of various types of data as a critical asset or critical cyber asset pursuant to CIP-002-1 is an area that could benefit from Docket No. RM06-22-000 - 76 -greater clarity and guidance from the ERO. Accordingly, the Commission directs the ERO, in developing the guidance discussed above regarding the identification of critical assets, to consider the designation of various types of data as a critical asset or critical cyber asset. In doing so, the ERO should consider Juniper's comments. Further, the Commission directs the ERO to develop guidance on the steps that would be required to apply the CIP Reliability Standards to such data and to consider whether this also covers the computer systems that produce the data.
273. The Commission also agrees with ISO-NE that experience in the implementation of the CIP Reliability Standards may indicate a need to further address this topic in a future proceeding.

Regarding an additional guidance/reference document

61. The Commission received comments on both sides of the issue of specificity. Some commenters caution against the CIP Reliability Standards being too specific, while others request more guidance to help them comply. In general, the Commission believes it is

appropriate to provide sufficient guidance to explain Requirements so that responsible entities have a high degree of certainty that they understand what is necessary to comply with a Requirement. More guidance will allow responsible entities to implement measures adapted to their specific situations more consistently and effectively. Additional guidance need not be included in a specific Requirement, but could be in the form of examples. The Commission is not directing that the ERO establish a specific end result. Our concern is simply that responsible entities have guidance on how to achieve an appropriate result in individual cases, which can vary on a case-by-case basis. Therefore, in several instances throughout this Final Rule, the Commission gives the ERO direction to provide additional guidance. In some cases, we require that the guidance be placed in modifications to the CIP

355. The Commission believes that responsible entities would benefit from additional guidance regarding the topics and processes to address in the cyber security policy required pursuant to CIP-003-1. While commenters support the need for guidance, many are concerned about providing such guidance through a modification of the Reliability Standard. We are persuaded by these commenters. Accordingly, the Commission directs the ERO to provide additional guidance for the topics and processes that the required cyber security policy should address. However, we will not dictate the form of such guidance. For example, the ERO could develop a guidance document or white paper that would be referenced in the Reliability Standard. On the other hand, if it is determined in the course of the Reliability Standards development process that specific guidance is important enough to be incorporated directly into a Requirement, this option is not foreclosed. The entities remain responsible, however, to comply with the cyber security policy pursuant to CIP-003-1.

356. In response to ISO/RTO Council, Ontario Power and other commenters, the Commission's intent in the CIP NOPR – as well as the Final Rule – is not to expand the scope of the CIP Reliability Standards. Requirement R1 of CIP-003-1 requires a responsible entity to document and implement a cyber security policy "that represents management's commitment and ability to secure its Critical Cyber Assets." The Requirement then states that the policy, "at a minimum," must address the Requirements in CIP-002-1 through CIP-009-1. The Commission believes that there are other topics, besides those addressed in the Requirements of the CIP reliability Standards, which are relevant to securing critical cyber assets. The Commission identified examples of such topics in the CIP NOPR. Thus, the Commission, in directing the ERO to develop guidance on additional topics relevant to securing critical cyber assets, is not expanding the scope of the CIP Reliability Standards.

408. The Commission agrees with FirstEnergy on the importance of flexibility in developing a mutual distrust posture, but does not see a conflict between the need for flexibility and what it is proposing, which is simply more guidance. More guidance will allow responsible entities to implement measures adapted to their specific situations more consistently and effectively. Additional guidance need not be included in a specific Requirement, but could be in

the form of examples. We will leave it to the Reliability Standards development process and the ERO to decide whether some or all of the guidance can be contained in separate guidance documents referenced in the Reliability Standard. In response to Entergy, the Commission is not directing that the ERO establish a specific end result. Our concern is simply that responsible entities have guidance on how to achieve an appropriate result in individual cases, which can vary on a case-by case basis. We disagree that providing useful guidance affects the scope of the Reliability Standards.

502. In response to APPA/LPPC, the Commission clarifies that it does not intend to create an inflexible rule calling for redundant electronic security in all cases. While the Commission directs that a responsible entity must implement two or more distinct security measures when constructing an electronic security perimeter, the specific requirements should be developed in the Reliability Standards development process. This would include whether or not the second security measure must be "on par" with the first. The Commission also directs the ERO to consider, based on the content of the modified CIP-005-1, whether further guidance on this defense in depth topic should be developed in a reference document outside of the Reliability Standards.

511. The Commission adopts the CIP NOPR's proposal to direct the ERO to identify examples of specific verification technologies that would satisfy Requirement R2.4, while also allowing compliance pursuant to other technically equivalent measures or technologies. In response to commenters, in discussing digital certificates and two-factor authentication, the Commission was providing examples of strong authentication, not limiting authentication to those options. The Commission is not prescribing the specific methods as an exclusive solution pursuant to Requirement R2.4. The ERO can propose an alternative solution that it believes is equally effective and efficient. If the ERO believes it would be helpful to responsible entities, additional guidance beyond the examples that are eventually included in Requirement R2 can be given in a separate reference document. Since we are directing the ERO to provide guidance on what constitutes strong authentication, it is not necessary for the Commission to respond to ISO-NE's request that digital certifications or two-factor authentication are acceptable methods of authentication. In identifying examples or categories of specific verification technologies that would satisfy Requirement R2.4, the ERO should take into account the specific comments raised in this proceeding. Similarly, while encryption is one method to accomplish two-factor authentication, and is an effective process for ensuring authenticity of the accessing party, for some facilities, we leave it to the ERO in the Reliability Standards development process to evaluate whether and how to address the use of encryption. In the alternative, the ERO may identify verification technologies or categories of verification technologies in a reference document.

547. In sum, we direct the ERO to modify Requirement R4 to require these representative active vulnerability assessments at least once every three years, with subsequent annual paper

assessments in the intervening years. The ERO should develop the details of how to determine what constitutes a representative system and what modifications require an active vulnerability assessment in the Reliability Standards development process. The revised Reliability Standard should contain the essential requirement that an active assessment must be performed at least once every three years. Based on the amount of guidance contained in the modified Reliability Standard, the ERO should consider at that time whether additional guidance should be provided in a reference document.

575. In response to commenters' questions regarding specific physical access controls, the Commission clarifies that it does not intend to create an inflexible rule calling for redundant physical security. While the Commission continues to believe that a responsible entity must implement two or more distinct and complimentary physical access controls at a physical access point of the perimeter, the specific requirements should be developed in the Reliability Standards development process when the ERO develops its modifications in response to this Final Rule. The Commission also directs the ERO to consider, based on the content of the modified CIP-006-1, whether further guidance on this defense in depth topic should be developed in a reference document outside of the Reliability Standards.

609 . The Commission has discussed issues related to testing environments in CIP-005-1. In that context, the Commission clarifies the CIP NOPR proposal to require differences between the test environment and the production system to be documented. As stated with respect to CIP-005-1, the Commission understands that test systems do not need to exactly match or mirror the production system in order to provide useful test results. However, to perform active testing, the responsible entities should be required at a minimum to create a "representative system" – one that includes the essential equipment and adequately represents the functioning of the production system. We therefore direct the ERO to develop requirements addressing what constitutes a "representative system" and to modify CIP-007-1 accordingly. The Commission directs the ERO to consider providing further guidance on testing systems in a reference document.

621. While we agree that no safeguard will protect against all malicious or unintentional acts, this does not mean that systems should not be protected against such acts. In response to MidAmerican, the Commission believes that details regarding how to safeguard systems against personnel introducing, maliciously or unintentionally, viruses or malicious software to a cyber asset are best developed in the Reliability Standards development process. The revised Reliability Standard does not need to prescribe a single method for protecting against the introduction of viruses or malicious software to a cyber asset by personnel. However, how a responsible entity does this should be detailed in its cyber security policy so that it can be audited for compliance with the Reliability Standard. The Reliability Standards development process should decide the degree to which the revised CIP-007-1 describes how an entity should protect

against personnel introducing viruses or malicious software to a cyber asset. The ERO could also provide additional guidance in a reference document.

629. For the reasons discussed in CIP-005-1, in directing manual log review, the Commission does not require that every log be reviewed in its entirety. Instead, the Commission will allow a manual review of a sampling of log entries or sorted or filtered logs. The Commission recognizes that how a responsible entity determines what sample to review may not be the same for all locations. Therefore, the revised Reliability Standard does not need to prescribe a single method for producing the log sampling. However, how a responsible entity performs this sample review should be detailed in its cyber security policy so that it can be audited to determine compliance with the Reliability Standards. The Reliability Standards development process should decide the degree to which the revised CIP-007-1 describes acceptable log sampling. The ERO could also provide additional guidance on how to create the sampling of log entries, which could be in a reference document. The final review process, however, must be rigorous enough to enable the entity to detect intrusions by attackers.

644. For the reasons discussed in CIP-005-1, in directing manual log review, the Commission does not require that every log be reviewed in its entirety. Instead, the Commission will allow a manual review of a sampling of log entries or sorted or filtered logs. The Commission recognizes that how a responsible entity determines what sample to review may not be the same for all locations. Therefore, the revised Reliability Standard does not need to prescribe a single method for producing the log sampling. However, how a responsible entity performs this sample review should be detailed in its cyber security policy so that it can be audited to determine compliance with the Reliability Standards. The Reliability Standards development process should decide the degree to which the revised CIP-007-1 describes acceptable log sampling. The ERO could also provide additional guidance on how to create the sampling of log entries, which could be in a reference document. The final review process, however, must be rigorous enough to enable the entity to detect intrusions by attackers.

660. The Commission adopts the CIP NOPR proposal to direct the ERO to provide guidance regarding what should be included in the term reportable incident. In developing the guidance, the ERO should consider the specific examples provided by commenters, described above. However, we direct the ERO to develop and provide guidance on the term reportable incident. The Commission is not opposed to the suggestion that the ERO create a reference document containing the reporting criteria and thresholds and requiring responsible entities to comply with the reference document in the revised Reliability Standard CIP-008-1, but will allow the ERO to determine the best method to accomplish the goal of better defining reportable incident.

725. The Commission adopts, with modifications, the CIP NOPR proposal to develop modifications to CIP-009-1 through the Reliability Standards development process to require an

operational exercise once every three years (unless an actual incident occurs, in which case it may suffice), but to permit reliance on table-top exercises annually in other years. Consistent with our goals and discussion of CIP-005-1, the Commission will not at this time require responsible entities to perform full operational exercises. Instead, the Reliability Standard should require the demonstrated recovery of critical cyber assets in a test environment, with the requirements for representative test environments and for addressing differences between the test environment and the production environment, similar to the conditions discussed for live testing in CIP-005-1. Given the range of views presented in comments regarding live testing, as the Reliability Standard development process forms the details of this "demonstrated recovery" concept, it should consider offering guidance beyond the actual Requirements of the Reliability Standard in separate reference documents. The Commission believes this alleviates commenters' concerns about the risks associated with such testing.

PROJECT 2008-06 CYBER SECURITY ORDER 706
JANUARY 7-9, 2009 PHOENIX AZ

NAME	COMPANY
DAVID TAYLOR	NERC
SCOTT MIX	NERC
ROGER LAMPILA	NERC
TODD THOMPSON	NERC
Keith Stouffer	NIST
DAVE NORTON	ENTERGY
KEVIN B. PERRY	SPP
Philip Huff	AECC
Joe Doetzl	KCP&L
JERRY FREESE	AEP
JOHN D. VARNELL	TENASKA
Scott Rosenberger	Luminant
RICH KINAS	OUC
DAVID REVILL	GTC
TOM HOFSTETTER	MISO
CHRIS PETERS	ICF INTERNATIONAL
Mike Winters	Hydro One Networks
Jackie Collett	Manitoba Hydro
KEVIN SHERLIN	SMUD
HAL BEARDALL	FCRC
STU LANGTON	FCRC
John Lim	Con Edison
Jeri D Brewer	US Bureau of Reclamation
Scott Fixmer	Exelon
BILL WINTERS	ARIZONA PUBLIC SERVICE
STUART LANGTON	FLORIDA STATE UNIVERSITY
JOE BUCCIERO	Bucciero Consulting, LLC

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Revised Meeting Agenda

Cyber Security Order 706 SDT — Project 2008-06

January 7, 2009 | 1–5 p.m. PST
January 8, 2009 | 8 a.m.–5 p.m. PST
January 9, 2009 | 8 a.m.–noon PST
Arizona Public Service Deer Valley Campus
Black Canyon 3 Building (BC-3)
2133 W. Peoria Ave.
Phoenix, AZ (609-250-1117)

Wednesday January 7, 2009

1:00 p.m. **Welcome and Opening Remarks — Jeri Domingo-Brewer and Kevin Perry**

a. Roll Call
b. NERC Antitrust Compliance Guidelines
c. FSU/FCRC Review of December meeting and adoption of December 4–5 Meeting Summary

1:15 **Review of Meeting Objectives and Agenda — Jeri Domingo and Bob Jones**

1:20 **Organizational Issues and Review of Phase 1 and early Phase II Schedule — Stuart Langton**

- Review of Phase 1 — Work-plan, January — May 2009 including small group proposal
- Review of Phase 2 — January—June, 2009 — including CIP-002 conceptual approach and industry input and feedback.

2:00 **Overview of Phase I Industry Responses — Number and Issues and Procedure Going Forward — Kevin Perry**

2:30 **Technical Feasibility Exception (TFE) — Briefing on NERC Review and Proposal Going Forward — Scott Mix**

3:00 **Break**

3:15 **TFE White Paper — Review of Changes and Additional Suggestions**

4:00	**Phase I Comment Review and Refinement — Full SDT Discussion of Cross Cutting Issues**
4:50	**Summary of Day One Outcomes and Review of Day Two Agenda**
5:00	**Recess**

Thursday January 8, 2009

8:00	**Welcome — Agenda Review and Review of Day One Results**
8:10	**Phase I Comment Review and Refinement- Plenary Discussion of Overall and Cross Cutting Issues**
9:00	**Break**
9:10	**Possible Small Group Breakouts — Review and Draft Responses**
noon	**Working Lunch *(Return to plenary meeting at 12:45)***
12:45	**Initial Small Group Reports on Draft Responses and Full SDT Discussion**
2:45	**Break**
3:00	**Initial Small Group Reports on Draft Responses and Full SDT Discussion**
4:20	**Next Steps for Drafting Group WebEx Meetings in preparation for February 2–3, 2009 Meeting**
4:50	**Summary of Day Two Outcomes and Review of Day Three Agenda**
5:00	**Recess**

Friday January 9, 2009

8:00	**Welcome and Agenda Review**
8:10	**Learning from Other Initiatives — John Sykes, NERC System Protection and Control Task Force**
9:00	**SDT Discussion of Implications for Phase II 002 Critical Asset Identification**
10:00	**Break**

10:15	**Phase II White Paper Development — Early Thoughts and Preview and Questions of the SDT to aid in the drafting- Jackie Collette and William Winters**
11:30	**Assignments — Next Steps and Review of Work-plan**
noon	**Adjourn**

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Cyber Security Order 706 SDT — Project 2008-06
JANUARY — JUNE 2009 DRAFT SDT SCHEDULE

NOTE: Below are draft considerations developed by the facilitators in consultation with the Chair, Vice Chair and NERC staff and following the December SDT NERC Communication Plan briefing and Phase 1 Webinar on December 16. The facilitators also reviewed the SDT criteria for a "roadmap approach" to revising the CIP standards discussed and refined in Little Rock at its November, 2008 meeting (See pp 4 below for a list of the criteria) These considerations were used to construct a draft schedule for the SDT for the first half of 2009.

Short Term 2009 Schedule Draft Considerations

1. Follow the ANSI standard development process but use creative ways to efficiently secure input from the industry on emerging concepts and approaches to the CIP standards.
2. Seek creative ways to get advice and input to the SDT from experts in cyber security.
3. Seek creative ways to get focused input from industry stakeholders.
4. Take advantage of input opportunities from related NERC committees that will be meeting in the first half of 2009 (e.g. working with the NERC Members Representative Committee, CIPC, BOT, and industry committees such as the Electricity Sector Coordinating Council, etc.)
5. Seek, as soon as possible but no later than late Spring, 2009, to establish a consensus on the way forward for the SDT in its efforts to revise the CIP standards.
6. Track any follow up to the "Securing Cyberspace for the 44th Presidency" report of the Commission on Cybersecurity for the 44th President.

SDT Draft Schedule — January–June 2009

Overview

- 7 SDT Face-to-Face Meetings
- Multiple SDT subgroup and subcommitees WebEx Meetings
- 1 Cyber Expert Workshop (March 10 or 11, 2009)
- 1 NERC CIPC presentation? (Feb. 9, 2009)
- Industry Comments on CIP 002 White Paper (April 17–June 3)
- 1 NERC Members Representative Committee, May 1, 2009

- OTHER MEETINGS?

SDT Draft Schedule — January–June, 2009

1. January 7–9 SDT Meeting — Phoenix, AZ ½–1/½ day format — Wednesday–Friday

- Review of Technical Feasibility Exceptions white paper
- Review of Industry Comments on Phase 1 products- Establish and convene small groups
- Initial Review of Phase 2 White papers

January 15 — WebEx meeting(s)

- Small group draft responses to industry.

January 21 — WebEx meeting(s)

- Small group draft responses to industry.

2. February 2–4, 2009 SDT Meeting — Phoenix, AZ, ½–1/½ day format — Monday–Wednesday

- Review of Small Group responses and recommendations on Industry comments and adopt draft of Phase 1 products, as revised, for review by NERC/Maureen.
- Review of Phase 2 White papers and Testing of a Phase 2 CIP 002 concept going forward

February 9, 2009 — CIPC Meeting — Update on SDT Progress and Input?
February 11 — WebEx meeting

- Phase 2 drafting concept group?

3. February 18–19, 2009 SDT Meeting — Boulder City, NV

- Review of Maureen's comments and adoption of Phase 1 products for balloting.
- Further discussion and adoption of a draft Phase 2 CIP 002 Concept for review by experts and stakeholders in March and beyond.

February 25 — WebEx meeting(s)

- Phase 2 drafting concept group?
- Development of Phase 2 CIP 002 Workshop for review by experts and stakeholders

4. March 10–11, 2009 SDT Meeting — Tampa, FL, 2-day format

- Invited Cyber Security Experts join SDT in a workshop to provide expert feedback to draft CIP 002 concept.
- Further SDT refinement of the CIP 002 proposed concept

March NERC Balloting on Phase 1 Products

March 18 **—** WebEx meeting(s)

- Phase 2 drafting concept group?

5. April 14–16, SDT Meeting, Charlotte NC — ½–1/½ day format. Wednesday-Friday

- Continue review and refinement of 002 concept and adopt White Paper on CIP 002 concept for Industry Comment

Industry Comment Period on White Paper **—** 45-days (April 17–June 3)

*May 1, **NERC Member Representative Committee**, Presentation of the Phase 2 CIP 002 Approach for MRC input. (Agenda item, Possible Workshop?)*

6. May 13–14 — SDT Meeting — Dallas, TX, 2-day format

- Review and respond to MRC input and further SDT refinement of the CIP 002 proposed concept and SDT CIP roadmap.
- Organize SDT in subcommittees to begin effort to draft revisions to CIP 003-008 or to address key issue areas.

June **—** following June 3 — WebEx meeting(s)

- SDT subcommittee meetings to review and draft responses to Industry comments on the CIP 002 concept.

7. June 17–18, SDT Meeting — Location TBD —2-day format

- Review Subcommittee responses to Industry comments on 002 approach
- Charge subcommittees and conduct organizational meetings
- Subcommittees meet to draft revisions to CIP 003-008

June **—** WebEx meeting

- SDT Subcommittee meetings

July–December, 2009 — SDT and subcommittees meet and continue CIP drafting

2nd DRAFT PHASE 2 ROADMAP APPROACH ASSESSMENT CRITERIA

(Presented, Revised, and Added to by SDT in its review on November 14, 2008)

1. The approach is consistent with the SDT purpose statement and is responsive to the FERC 706 directives and the SAR.

2. The approach is achievable given the SDT schedule and workplan.
3. The approach does most to advance and enhance cyber security in the BES.
4. The approach helps the SDT address the foundational issues with the current standards.
5. The approach is capable of implementation.
6. The approach is capable of improving compliance.
7. The approach helps protect the current investments and wherever possible builds on what has already been done.
8. The approach helps to identify and mitigate risk on an ongoing basis.
9. The approach balances a “systems” orientation with a “facilities” orientation to asset protection.
10. The approach is capable of being extended into related interests by others (distribution, AMI, Smart Grid, etc.).
11. The approach enables the industry to provide the appropriate level of security (i.e. not over securing nor under securing the BES cyber assets).
12. The approach allows for discrimination among and targeting the various types of infrastructure that support the BES

Working Group Assignments

CIP Standard No.	Questions Nos.	Assignments/Volunteers
002 & 003	Q1 & Q2	Jeri Brewer/Gerald Freese/Dave Norton/Dave Revill
004 & 007	Q3 & Q6	Chris Peters/Keith Stouffer/Mike Winters/William Winters
005 & 006	Q4 & Q5	John Varnell/ John Lim/ Rich Kinas/Scott Fixmer/Scott Rosenberger
008 & 009	Q7 & Q8	Tom Hofstetter/Joe Doetzel/Kevin Sherlin
Compliance	ALL Qs	Roger Lampila/Todd Thompson/Jackie Collett
Implementation	Q9, Q10, Q11, Q12	Kevin Perry/Scott Mix/Phil Huff
Q13	Q13	

Phase I Schedule of Activities

Jan 7-9, 2009 Meeting (Phoenix): General Consensus

Jan 15 WebEx I: Harry will run this WebEx (Joe will attend)

Move toward specific comments responses to the questions and comments from industry

Jan 21 Webex II: Joe will run the WebEx

Move toward producing final responses to industry comments and other ballotting documents

Prepare for ballotting: Comments and Summaries; Clean and revised versions of the CIP Standards, Implementation Plan (redline and new clean copy), Implementation Plan for Newly Identified Cyber Assets

Seek input from Maureen to finalize responses

February 2-4, 2009 (Phoenix): Meeting to **approve** comments back to the industry

Meeting is likely to be a 2 ½ day meeting (Half-day; Full-day; Full-day)

February 5, 2009 Target: Post document for pre-ballot review

February 18-19, 2009 (ICFI-Fairfax, VA): Meeting to finalize and approve comments back to industry including any changes or comments from Maureen

February 25 WebEx: Follow up with action items from February 18-19 meeting.

March 9-19, 2009: Initial Ballot

March 10-11, 2009 Meeting (Orlando): Deliver the Industry Workshop (Day 1); Discuss outcome of Workshop and Phase 2 (Day 2)

March 20 - April 3: Respond to Comments

March 25 WebEx: Respond to comments received during Initial Ballot

April 14-16, 2009 Meeting (Charlotte): Hold first day for possible Industry Workshop (Alternate to March 10); Prepare MRC Presentation for May MRC Meeting

April 29 WebEx: Finalize the MRC Presentation (Mike Assante participation)

May 13-14, 2009 Meeting (Boulder City, NV): TBD

May 21 WebEx:

June 17-18, 2009 Meeting (Manitoba): TBD

June 25 WebEx:

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Meeting Summary
Cyber Security Order 706 SDT — Project 2008-06

January 7–9, 2009
Arizona Public Service
Phoenix, AZ

1. **Attendance and Roll Call**
   See attached attendance sheet, plus 12 participants on the WebEx and conference call.

2. **Antitrust Compliance**
   NERC Antitrust Compliance statement was read

3. **Meeting Agenda and Objectives**
   The agenda and objectives for this meeting were reviewed and no changes were made (see attached document).

   Stu introduced the revised process schedule for Phase I as it reflects adjustments to original schedule and includes flexibility leading up to June 2009, when we can pause and assess the best way to move forward from there with Phase II taking into account the ANSI process (see Assessment Criteria listed at the end of the schedule).

   Jonathan Sykes from SRP was invited to provide the SDT with a briefing from the NERC System Protection and Control Subcommittee describing Protection System Redundancy on Friday, January 9th. The Subcommittee's engineering approach to equipment redundancy and protection may be useful in helping the SDT to identify criteria for determining critical electric system assets.

   The upcoming Phase I SDT Meeting schedule from January to June 2009 was also reviewed. (See the attached schedule "SDT Draft Schedule – January—June 2009")

   Preparations for the upcoming NERC Member Representative Committee (MRC) meeting scheduled for May 1, 2009 were also discussed.

   A Cyber Security SDT workshop was also discussed and is planned for March 2009. The idea of this workshop is to bring in cyber experts from the electricity industry

and a variety of other industries and companies to obtain additional input that can be used to augment and/or validate the SDT's approaches.

Some preliminary thoughts and discussion on the preparation of white papers by Jackie Collett and William Winters concerning Phase II SDT Standards Development approach will be explored on Friday, January 9th.

4. Review of Phase I Comments on the SDT Standards

Kevin Perry provided a preliminary overview of the 119 pages of comments received from the 46 industry respondents. The comments were organized by NERC staff, and the latest set of comments was released to the SDT on January 7th. In summary, there were:

- No show stoppers
- Lots of duplication in the comments received
- Some comments cross multiple standards with common concerns such as :
  - Compliance Enforcement Authority
  - "a" vs. "the" senior manager and the delegation of authority
- New compliance language received lots of comments and maybe confusing to industry
- Confusion regarding data retention requirements warrants further discussion

Kevin recommended that the Compliance Team pay close attention to the new compliance wording so as to avoid the possibility of impact on all of the cyber security standards.

a. Approaches for Reviewing Phase I Comments

A couple of approaches to reviewing the Phase I Comments on the cyber security standards were discussed:

- *Option 1*: Form various small groups to review and respond to subsets of the comments received. Possibly begin Phase II work in parallel.
- *Option 2*: All comments would be reviewed by all SDT members and those present at the meeting.

The preferred approach was to break up into small working groups to review an assigned grouping of standards in parallel, but not to begin Phase II activities. Following the review period, the full group would meet to discuss the findings and responses from each of the small working groups. Any cross references or duplicative responses should be found during this group review session. The

small working groups and their assignments are identified in the attachment labeled *"Working Group Assignments"*.

b. Schedule for Reviewing Phase I Comments

The Industry Comments need to be addressed and responses prepared in January 2009. The plan is to have the responses ready by the February 2–4, 2009 meeting for group adoption and eventual posting.

c. Response Strategy and Process

a. Many comments could be contentious and caution should be taken such that we answer comments at face value and not be drawn into the arguments.
b. Avoid getting drawn into discussing the Aurora incident; it is out of scope for the SDT.
c. A lot of the issues will be considered in Phase II; our response needs to indicate that the commenter should review their concern when Phase II documents are published for industry review and comment. An appropriate response may be "we will consider the comment in Phase II".
d. We will receive comments during the ballot period that we will need to respond to — hopefully the highly contentious issues are identified now before sending out the Phase I standards for ballot.
e. A "significant" change to a standard versus a "minor" change is a judgment call made by the NERC standards manager (Maureen Long).
f. If we make a significant change to what's already been published, we'll have to seek comments again. If we do not change the requirement but move it to a different standard, is that a significant change? Some clarification is needed.
g. The plan is to issue the responses to the industry comments without requiring another round of comments. If we receive a particularly contentious comment, consider removing the item for further consideration in Phase II.
h. Compliance comments and issues should be addressed by the NERC compliance folks, not the SDT.
i. Keep responses short and concise; don't water it down or get involved in long explanations; take the issue on in the appropriate language.
j. Point to reference documents, where appropriate, to address confusion about what some requirements mean.
k. Put the background material into the responses and refer to it, if needed.
l. A suggestion was made to include an introduction to the standards comments response document that describes the approach and what is being accomplished in Phase I and that the major issues will be addressed in Phase II.

d. Small Working Group Logistics

Some of the logistical items that were discussed included:

a. Logistically how and where will we meet? Should groups go off on their own? Should we meet at individual group tables so we can address cross-cutting issues as needed?
b. Can WebEx participants be included in the discussions?
c. CIP-002 and CIP-003 should be considered together.
d. Compliance requirements should be carved out of each standard for review and comment.
e. Each working group needs a scribe to document the responses. The industry comments are simply arranged by the thirteen questions that were asked and in the ordered they were received.
f. If a "yes" response is received and no comment is provided, then no response is needed. If a comment is provided, then an appropriate response is needed.
g. Address the most contentious issues first.
h. Work with the Word version of the comment document.

5. Technical Feasibility Exception Discussion

The Technical Feasibility Exception (TFE) process is based on discussion with utility management. The process is not about the technical requirements and standards that the SDT tends to address, but it is more about whether compliance has been met; compliance is more than just the audit process.

Technical feasibility was meant to address the issues where compliance could not be met quickly, thereby allowing for good reason to be technically out of compliance while significant issues can be addressed.

The TFE White Paper is being reviewed by NERC management. Compliance and Legal counsel were sought concerning how the white paper should be positioned and what it would mean to enforcement. It needs its own vetting process within NERC, and it may require modification to the Compliance Monitoring and Evaluation Program (CMEP). Changes to the CMEP are applicable across all of NERC's standards, so the TFE needs to well thought through and vetted within NERC.

Mike Assante, Chief Security Officer at NERC, has agreed to sponsor the TFE through the compliance process at NERC. Scott Mix will work with NERC Management to determine the best approach for getting this done.

6. Small Working Groups

Six small working groups were formed to review the industry comments and to develop the SDT's responses. The six groups were created to craft the SDT's responses and to make appropriate edits to the text of the CIP Standards. The six groups were:

1. CIP 2 and 3 (Questions 1 & 2)
2. CIP 4 and 7 (Questions 3 & 6)
3. CIP 5 and 6 (Questions 4 & 5)
4. CIP 8 and 9 (Questions 7 & 8)
5. Implementation (Questions 9, 10, 11, and 12)
6. Compliance Issues (all questions)

Question 13 was reviewed by the entire group.

WebEx and teleconference participants were advised that members would be breaking into small groups for the afternoon; they were welcome to join again when the full group reconvened to review the responses and edits prepared by the working groups.

The plan was to begin the review of the formal responses to the comments on a WebEx to be held on January 15th, and complete the initial reviews during a WebEx scheduled for Wednesday, January 21st.

a. Small Working Groups — Initial Report Out

The members of each small working group were asked to consider the following in presenting their findings to the full group:

- Present substantive issues/responses from most to least contentious (10-15 total minutes for each small group report)
- The full SDT will focus on most contentious issues to confirm response
- Small groups may reconvene to refine responses

At 1:00, the WebEx was re-initiated. Bob Jones reviewed the expectations for the group reports with a focus on the most contentious or substantive issues that will need full group input for possible additional refinement. The reports were brief with an opportunity for groups to revise their work.

b. Questions 1 and 2 (CIP 002 & 003)

Three sets of substantive issues

1. Concern about assigning a senior manager in CIP-003 rather than in CIP-002
2. Clarify delegation of senior manger responsibilities
3. Industry concern about the responsibility of a senior manager vs. a responsible entity (accountability issue?)

Confusion over how to delegate responsibilities. Does the Senior Manager have the authority to:

a. Assign specific actions
b. Identify which responsibilities will be delegated
c. Document only those delegations assigned to each delegate
d. Delegate authority for specific actions (added) "assigned to the senior manager" to a named delegate or delegates.

Other items to change include:

i. Delete "business phone" information
ii. Use "calendar days" throughout CIP 002 to 009

Poll was taken to test support for adding the above language: (Result: 7 for; 10 against)
Respond back to those offering the language in the comments?

c. Questions 3 & 6 (CIP 004 & 007)

Substantive issues were the following:

a. Addressing ambiguity in "specified circumstances" – answer that the language was included as directed in FERC Order 706
(Comment: we need to be specific in our responses, not necessarily clarifying, but more explicit about what the drafting team will do with this)
b. Don't change any language, but specify where the wording came from – Phase II will not change the language either
c. Careful what you are promising to do in Phase II
d. Leave first sentence as is and refine second sentence into a shorter version without promising future action
e. Need to avoid any linkages between guidance and standards

Highlighted key items for discussion:

i. For R3 – need to specify critical assets
ii. Added access "to critical cyber assets" - much the same reference in R2 – consistency issue
iii. Added "all" in front of "other" to remove any potential ambiguity
iv. Need to be consistent across the different standards – use the same terminology

Poll to test securing "all" Cyber Assets within an ESP: (10 yes; 8 no)
Rather make the necessary changes in Phase II

Exception to taking out "acceptance of risk" – did not make a substantive change – but review response for group support

Recommendation is to consider language modification – residual risk analysis would demonstrate that an entity has exercised due diligence when compensation measures have been applied.
Response should be that the analysis will be considered in development of the technical feasibility (TFE) process.

Within the measures – initially agreed with changing M2 to make it consistent with other measures, but suggest alternative language to add "and records" to M2 – (make available documentation "and records of its ports and services process" as specified in Requirement R2)
Conclusion was to remove "and records" to limit the heartburn
The SDT could revisit in Phase 2?
Are we changing more than we should?

Poll taken to test if there is any problem in adding the language? (7 – Yes - that's enough to remove it)

Need to re-explain the need for Phase I to meet the June deadline set by FERC when the response document is sent out for comment.

d. Questions 4 & 5 (CIP 005 & 006)

Substantive Issues:

a. Substitute "subsequent" phases for Phase II; "subsequent" phases anticipate significant changes
b. Intent is to include only devices that perform access control or monitioring, not those devices that are receiving alerts
c. Only a few real changes suggested:
    i. Change "maintain and implement" to "implement and maintain"
    ii. Agree that R1.4 should reference R4 and not R3
    iii. Competing authorities is outside the scope of the SDT – offer to refer it to appropriate entity (NERC)
    iv. Reliability standards only prescribe what and not how
    v. "Continuous" is a clarification of active escort – SDT is not agreeing to remove it
d. Is there a more positive way of asking commenters to resubmit during the next phase?
e. Apologize for not clearly red-lining the changes; it added to the confusion

f. In Phase II, the SDT will need to address differences between logging and monitoring
g. Use of "documents" versus "documentation" – need to be consistent in use

e. Questions 7 & 8 (CIP 008 & 009)

Substanfive issues:

a. Concern with the addition of the word "dated" into the measures
b. CIP 009-02 R3 missed the mark
c. CIP 008-02 confusing wording

Actions:

a. "Dated": Remove the word dated from the measures.

b. CIP-009-02 R3:
- Rewrite to meet intent of FERC Order 706 (P731)
- Change control — updates shall be completed within 30 days and communicated within 90 calendar days (What is meant by "completed"?)
- *Subsequent discussions led to the decision to wait to make any changes until Phase II development of the CIP Standards.*

c. CIP-008-02 R1.3 to R1.6:
- Remove "process for" from each requirement
- R1.5 and R1.6 add annual testing of the response plan
- *Comments:*
  - Add to the compliance section as additional guidance?
  - Is this a major change requiring submittal for further comments?
  - Putting it in as additional compliance guidance - is it a major or minor modification to the standard?
  - This comment is not related to a change made in the last revision to the standards, but rather is a new additional item. These changes should be addressed as part of Phase II
  - Do we need to weigh the number of commenters making the comment that this section is confusing?
- *Subsequent discussion to accept these comments or pull them for consideration in Phase II led to the conclusion to wait until Phase II. A good strawman will be needed to start the process at that time.*

f. Questions 9 to 12 (Implementation)

Actions to be taken:

1. Update Implementation Tables
2. Modify the SDT implementation plan to clarify emergency provision

3. Change category 3
4. Change #3 to add "cyber"
5. Reference "other" CA rather than "non-critical" CA
6. Modify timeframe to 18 months after the new CCA is identified
7. Update Table 2 to reflect the addition of two new requirements
8. Any further updates to Table 2

Decisions:

a. Implementation plan as a separate document – consider incorporating in subsequent revisions
b. Guidelines for identifying CA and CCA are being developed
c. Six months is reasonable – not changing to nine months
d. Nuclear facilities are out of the scope of this SDT group

Explanations:

- "In the event of a merger or acquisition of a company, … allow one year for the programs to be harmonized." If one party has a program then continue it while merging, if they have competing programs, then take a year to sort it out – this is a response to a comment, not making any changes to standard.
- Concern about how this applies when a holding company owns separately registered entities – will address by revising language here
- Reviewed items "tossed over the wall" to Compliance small group

Proposed effective date in implementation plan– add "compliant" to clarify from "auditably compliant" – Poll to test for opposition: Any opposed? None
Test to leave without "compliant" – no objection. Why does title include "proposed"? Not adopted yet and consistent with other implementation plans

g. Compliance Issues (All CIPs)

Substantive Compliance issues identified were:

1. The wording in Compliance Section 1.1.1 does not specify who is responsible for the enforcement – not changing it at this time but probably will need to – have sent it to NERC (Maureen) for possible clarification
2. Do the terms ERO and Compliance Enforcement Authority need to be defined in the glossary? They are already defined in the Rules of Procedure of NERC, which is hierarchically higher in terms of precedence of documentation, and therefore governs the definition - is not needed in the standards glossary
3. Can we just add the same definition to the glossary? Keep response simple here that definition is already covered in the Rules of Procedure.

4. "Dated" – do we revise the measures for all standards to include "dated"? (Comment: - In phase I, leave it like it is – revisit in Phase II)
5. Reinstate "duly authorized exceptions will not result in non-compliance"? Referring back to NERC for follow up
6. "In conjunction" leaves open possible interpretation – referred back to NERC

Jackie will review the rest of the compliance issues, but expects most new comments will be repeats from responses covered above. Jackie will flag any additional issues that the group may need to address.

h. Question 13 (All CIPs)

Tom Hofstetter described how he assigned many of the comments to the appropriate small group. The small groups will need to tag or segregate their responses to Question 13 items so they can be pulled out to include as a set of responses under Question 13.

Tom reviewed a few basic responses that he proposes to comments that are not related to other questions or small groups.

7. NERC System Protection and Control Presentation (Jon Sykes)

Scott Mix introduced John Sykes – Vice Chair of the NERC System Protection and Control Subcommittee, which is looking at redundancy in control and protection systems, as an aspect of critical asset protection. They are early in their process of review.

The NERC SPCS has written a technical white paper, a proposed working paper for a standard, and has prepared the presentation. It took two an a half years to get to this point, and the SPCS need lots of industry input because of the high potential cost to the industry.

The major topic of discussion was on the methods for determining risk. Do we write a prescriptive standard or a performance based standard? Key initial question, helped decide on the performance based approach.

Defined "redundancy", and reviewed protection system performance requirements Methodology to determine adequate redundancy of a Protection System

- Determine redundancy of the PS
- Ascertain the performance of the PS
- Compare protection systems performance with electric system performance requirements in the TPL standards

- Mitigate all performance shortfalls

8. White Paper Discussions for Phase II

Stu introduced a review of the Phase II White Paper process. He reviewed discussion from the previous SDT meeting in Washington where we came away with proposal to prepare and review two straw proposals, one starting from the CIP standards perspective and the other starting from the NIST standards perspective

Jackie Collett took a look at the NIST 800-53 standard and sees promise, but she also sees aspects of the standard that may cause concern for electric power systems. Jackie reviewed her take on the original intent of the NERC CIP 002 Standard.

William Winters offered initial thoughts on his approach from NIST, and how he might address some of the gaps in the standards but recognizing the concerns the industry may have with the NIST risk assessment approach, particularly cost.

William will look at what NIST does regarding asset identification, focusing on CIP 002, not CIP 003. Some of the items addressed were:

- Concerns expressed by members about the disincentive for including critical assets, particularly for purposes of audits
- NIST may allow for gradations of identification, but that can complicate compliance – will the NIST approach work in the end?
- Energy Act 2005 and FERC announcements have come subsequent to the drafting of the standards which were written for data centers - industry concern about the cost and need for the identification of the critical assets
- Understand where and why we are where we are today to help figure out how to avoid potential industry refection – if industry does not accept, then FERC will do something because they now have clear Congressional support to do something
- Change in administration attitude about the need for industry regulation – we need to do a better job of educating the industry on the cyber risk in order to get their support for changes and limit the gaming – people want to do the right thing, if they understand why
- NERC SDT is focused on critical assets for the bulk power system, but the NIST framework covers the whole spectrum of systems used by the federal system.
- Generation aspect does not necessarily include transmission – we need to understand the different needs but be sure to include both – one size will not fit all for different systems
- Homeland Security list exists – need to resolve how industry list supports this other broader list –

- ISA 99 takes a multi-level approach to security
- Identify the cyber assets that do x, y and z – then if it fails what bad happens – that identifies critical cyber assets system wide – is the information flow essential, follow out to find boundary, even where it crosses company boundaries – need to get away from applying physical engineering to the flow of information
- How do we reorganize what we consider critical?

This discussion provided guidance to Jackie and William to develop their approaches for review in February. Should the approaches be combined now for review next time? Or parallel approaches to be merged later?

Jackie envisioned parallel approaches to then be compared, and William agreed. Also they agreed that the items/issues identified are the starting points to be addressed. William will look at how NIST can be tailored to fit with the CIP standards, while Jackie will look at how the CIP Standards can be adopted into the NIST framework. Both will be brought together to see if and how a hybrid might work effectively.

Both products will be circulated before the next face-to-face meeting in February. Some manner of blending will occur — just a matter of how much — no one is saying start over from scratch. They will review and discuss the balance and trade-offs especially from an audit perspective. Five issue areas will be used by Jackie and William as part of the problem statement. Are there possibly other areas that need to be added to the list of five?

9. Wrap-Up

The SDT must sign off on the edits by the end of the next meeting to meet the proposed schedule for Phase I.

Next Meeting is scheduled at the downtown Phoenix Hyatt Regency — please plan on staying the full meeting time, especially try to stick around for the afternoon of the third day.

Beyond the February 2–4, 2009 meeting in Phoenix:

- February 14–15, 2009 meeting is in Fairfax, VA (ICFI Offices)
- March workshop
    - Progress at the next few meeting will help move us toward preparations for that workshop. Need to work in February to prepare for the workshop, which is preliminarily scheduled in conjunction with the March 10–12, 2009 SDT Meeting in the Orlando or Tampa area.

  - Purpose of the Workshop is to broaden our outreach and enlist review and input from cyber security experts in other industries as well as the electric industry.
  - The workshop will lead to a presentation to the NERC MRC on or about May 1, 2009.
- April 14–16, 2009 meeting in Charlotte (Duke Energy)
- May 14–15, 2009 meeting in Boulder City, NV (Bureau of Reclamation)
- June 17–18, 2009 meeting in Manitoba (Manitoba Hydro)

Web meetings are scheduled approximately one week following each SDT meeting. Industry Webinar Meetings are also planned to keep the industry informed on the progress of the Cyber Standards development.

Meeting Adjourned at 11 a.m. on January 9, 2009.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Meeting Summary
Cyber Security Order 706 SDT — Project 2008–06

February 2, 2008 | 1–5 p.m. MST
February 3, 2008 | 8 a.m.–5 p.m. MST
February 4, 2008 | 1–5 p.m. MST

Adopted Unanimously February 19, 2009

Robert Jones and Stuart Langton, Facilitation and Meeting Design

FCRC Consensus Center, Florida State University

Thanks to team members Sharon Edwards, Tom Hofstedler and Kevin Perry for sharing their meeting notes.

http://www.nerc.com/filez/standards/Project_2008–06_Cyber_Security.html

116-390 Village Blvd.
Princeton, NJ 08540
609.452.8060 | www.nerc.com

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Cyber Security Order 706 Standard Drafting Team
Sixth Meeting Summary,
February 2–4, 2009
Phoenix, AZ

Meeting Summary Contents

116-390 Village Blvd.
Princeton, NJ 08540
609.452.8060 | www.nerc.com

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Cyber Security Order 706 Standard Drafting Team
Sixth Meeting Summary,
February 2–4, 2009
Phoenix, AZ

EXECUTIVE SUMMARY

The Chair and Vice Chair welcomed the members and welcomed Rob Antonishen, Ontario Power Generation as the team's newest member. NERC staff David Taylor conducted a roll call of members and participants in the room and on the conference call. They then reviewed with the team and participants the proposed meeting agenda. David Taylor reviewed with the team the need to comply with NERC's Antitrust Guidelines**.** The facilitators reviewed with the team the consensus guidelines adopted at the SDT November 2008 Little Rock meeting.

Scott Mix, NERC staff provided the team with an update on the status of the Technical Feasibility Exception white paper and the effort to convert it into a compliance document under NERC Rules of Procedure. On Wednesday, Scott Mix provided an additional update on the TFE process noting he had received an e–mail from the NERC Assistant General Counsel that outside counsel started to review the white paper and that nothing had been identified as a show stopper e.g. "good faith efforts".

In introducing the Phase II presentations and discussions, the facilitator reviewed related FERC 706 provisions noting they direct the SDT to consider "applicable features" of the NIST framework (Paragraph 25, 232, 233).

Bill Winters presented his paper, "Independent assessment of FISMA and related NIST documents for adoption for Electric Sector Critical Infrastructure Protection," and an additional section, "Thoughts for Discussion of NIST/CIP Opportunities" noting his assignment was to review the NIST/FISMA framework and suggest CIP features that represented strengths that might be incorporated into NIST/FISMA. His approach was to ask and try to answer the question: could my company apply the NIST/FISMA security framework approach? He suggested two approaches going forward: Heavy alignment vs. Integration Light:

1. *Heavy alignment* — replace/expand CIP 002 require assessment of: systems used in control and monitoring BES/BPS; systems directly connected and/or exchange data with; and systems which transport data used in control and monitoring.
2. *Light alignment* — develop a set of controls using NIST controls as starting points.

Members discussed topics that included: Address gaps in both NIST and CIP; Common Controls and Auditing; Outcomes Based Framework; Other Approaches; How prescriptive should controls be; Standards vs. Frameworks; and Certification Methodology.

John Lim presented the team's paper on Phase II approach from a CIP perspective on behalf of Jackie Collett, Scott Rosenberger and John Varnell. He noted that CIP standards are intended to be a baseline for cyber security for bulk power assets with a focus on assets with the highest impact. One of the issues with the current NERC standards which the team discussed the most was the "all or nothing" approach of the current CIP standards, i.e. if an asset is not defined as "critical" under CIP, there are no controls required. Perhaps additional systems and/or functions need to be identified to address this gap.

The team identified the following five issues with CIP 002 and for each offered comments on shortcomings, gaps, challenges and options: Piecemeal Approach; Not protecting assets needing protection; Gaming; All or Nothing Approach; and Loss of Asset Integrity and Misuse. John Lim noted that a multi–level protection scheme will have to identify high, medium and low. It will be necessary to study which assets are most critical. Look at the function of system and the connection to the BES.

Following the presentation there was a discussion about whether vulnerabilities in common systems should be addressed in the next version of standards. There was also discussion concerning the protection of defined Critical Assets versus protection of all SCADA systems. Several members stated that priority should be given to CIP 002 and the all or nothing view of defining Critical Infrastructure which is in scope as a result of CIP 002 current logic. Several members expressed that at least a minimum level of protection must be prescribed for additional assets.

Scott Mix took on the task of trying to conceptualize what would a NERC FISMA process look like to apply while maintaining the status quo in terms of the scope of the current CIP standards. He created a "straw man" which was presented in a power point format. He noted that he started with a mission focus on the bulk electric system (BES) vs. the bulk power system (BPS). The law and FERC say BPS whereas NERC has historically used the BES. He then noted that extending the scope into the distribution system will take an act of Congress because the bulk power system does not include distribution. The bulk power system consists of the 8 regional bulk electric systems. Characteristics are identified for 3 categories: confidentiality; integrity and availability. Then a high water mark is applied to the highest ranking of the 3 aspects. The electric system is bisected into Transmission and Distribution. Distribution is off the table by law. The portion of Transmission dealing with Marketing is also off the table. Transmission is then divided into High, Medium and low impact to the BES. If we applied that methodology to the standards this would classify all transmission assets by impact (high, medium, low, none). Then the SDT could go through CIP-003 through CIP-009 and determine what the implications are from a reliability standpoint. 800–53 is a good catalog that can be used for an approach excluding the sections that deal with financial, etc, which are not applicable. There are significant implications for the workload for SDT, the workload for education, and the workload for industry implementation. Scott suggested the SDT could have a healthy debate as to whether or not this approach is what the Team agrees is the right approach.

SDT member Michael Winter drafted these overarching principles for consideration by the SDT based on the team's previous review and discussion. He introduced them making the following points: these principles are intended to be complementary and not mutually exclusive; the SDT should modify in order

get the best of both worlds; CIP and NIST. The concept is to offer protection for all but to different degrees based on the risk.

The top 3 most acceptable principles based on the SDT's initial ranking are:

1. Create clear standards and employ a technical exception/compensating controls reporting and guidance process that accommodates deviations (3.6 of 4)
2. A mapping similar to NIST 800–53 Appendix G to CIPs will help quantify and assess the gap, if any. (3.6 of 4)
3. Use a consistent risk–based model to classify all assets (i.e. facilities, sites, physical perimeters) (i.e. not cyber assets at this point) as critical/high impact, moderate impact, low impact.

The following draft principles are in order of acceptability:

4. An entity's Asset classification would be open to scrutiny by regional entities and ERO. The extent of scrutiny to be defined and tightly controlled. (3.1 of 4)
5. Use the minimum security controls for high, moderate, low within NIST 800–53 to help model the CIP controls for each level. Address any gaps at the same time but keep the same CIP-002 to CIP-0XX general format. Industry knows this format, is building policies and programs around it, has commented on it and has voted on it. (3.0 of 4)
6. Any IT devices beyond the perimeter, including telecom, are not part of the CIPs — the CIPs remain perimeter–based where devices on and within the perimeter are protected and everything beyond is considered untrusted. (2.9 of 4)
7. As part of a power system (non–corporate IT) inventory of cyber assets, add an attribute to each device that associates the high, moderate, or low classification of the physical perimeter, facility, or site within which it resides. Apply security controls based on the classification. (2,8 of 4)
8. Protect all cyber assets related to power system; not just the Critical Cyber Assets but to different degrees of protection/controls depending on their classification. (2.8 of 4)

The facilitators noted that the authors of the draft papers and principles would be asked to refine them and be prepared to present them at the February 18–19 SDT meeting.

For the Phase I review, the SDT reviewed all of the responses drafted to date for consistency and content. The team also looked at each of the additional industry comments that were not available at the January 7–9, 2009 Phoenix meeting. They then broke into the small groups that had been formed and worked together at the January meeting to complete the task of refining the responses. The SDT then reconvened and reviewed and agreed on the final responses.

On Wednesday, the SDT reviewed all of the proposed changes to the Phase I documents posted for industry review in light of the SDT responses and discussion. The SDT unanimously agreed to:

- Adopt the SDT Response Document (reflecting Tuesday's agreed on changes)
- Adopt the Proposed Changes to the Phase I Documents (reflecting Wednesday's review)
- Agree to post the documents for the 30–day pre-ballot period.
- However, the Phase I balloting will only commence after the NERC TFE proposal has been posted for industry comment for at least 14 days.

The SDT reviewed a draft set of Violation Severity Levels for the current CIP 003 through CIP-009 that a separate team (Project 2008–14) has developed. The SDT members expressed concerns with the likely confusion with the VSL team and in the industry posting both of these VSL changes (i.e. current CIP and Phase I proposed changes). Mr. Taylor noted that the draft SAR that directed the VSL SDT to only review the current CIP standard was open for comment until February 10, 2009. Members again expressed concerns that two SDTs revising the same documents is sure to cause confusion in the industry. Following straw polls, (the SDT to take on drafting VSLs for current CIP, Phase I, and Phase II standards 0–18; for the SDT to take on VSLs for Phase I and II, 7–11 in support; and for SDT addressing only Phase 2 VSLs, 16–2 in support, the SDT adopted the following approach:

The following statement will be forwarded to the SAR Committee as an SDT comment for its consideration with only the names of those SDT members voting in support of the motion:

> "The Phase I changes ("Version 2") to the CIP standards are expected to be balloted coincident with the development of the VSLs for "Version 1" of the CIP standards. The Project 2008–06 drafting team will not be in a position to include the VSLs with the revised standards due to the timing of the two projects. The VSL drafting team is best positioned to recommend VSLs in support of the Version 2 standards."

The motion was approved by more than 75 percent of the SDT members present and voting. The facilitators reviewed adjustments to the schedule including:

- A SDT comment on the VSL SAR by the deadline (February 10, 2009)
- February 18–19 in Fairfax, Virginia — advance the Phase II review and discussion
- March 10–12 in Orlando, Florida — seek a Phase II framework going forward.
- April 14–16 in Charlotte, NC — test the Phase II framework in a workshop with cyber experts and refine the framework for presentation at the MRC on May 1.
- May 1 — Members Representative Committee presentation of Phase II framework
- May 18–19 — Refinement to Phase II framework based on MRC comments and determination of whether to issue a white paper for industry comment. Review proposed SDT sub–committee and drafting group structure
- June–December, 2009 — SDT meetings along with SDT drafting groups.

The team then evaluated the meeting in terms of what worked and what could be improved. The meeting adjourned at 11:30 a.m.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Cyber Security Order 706 Standard Drafting Team

Sixth Meeting Summary,
February 2–4, 2009
Phoenix, AZ

I. INTRODUCTIONS, AGENDA REVIEW, PROCEDURES AND OPENING REMARKS

The Chair and Vice Chair welcomed the members and welcomed Rob Antonishen, Ontario Power Generation as the team's newest member. NERC staff David Taylor conducted a roll call of members and participants in the room and on the conference call *(See appendix #2*). They then reviewed with the team and participants the proposed meeting agenda *(See appendix #1*).

David Taylor reviewed with the team the need to comply with NERC's Antitrust Guidelines *(See, appendix #3).* He urged the team and other participants in the process to carefully review the guidelines as they would cover all participants and observers. He urged all to avoid behaviors or appearance that would be anti–competitive nature and also reminded the group of the sensitive nature of the information under discussion.

The facilitators reviewed with the team the consensus guidelines (Appendix #5) adopted at the SDT November, 2008 Little Rock meeting.

II. TECHNICAL FEASIBILITY EXCEPTION UPDATE

Scott Mix, NERC staff provided the team with an update on the status of the Technical Feasibility Exception white paper and the effort to convert it into a compliance document under NERC Rules of Procedure. He offered the following points:

- NERC's outside legal counsel is reviewing and helping to convert the whitepaper into a formal compliance document under NERC Rules of Procedure.
- The SDT needs to take into account all of the FERC rules regarding the NERC Rules of Procedure.
- Expect to see a short formal version in the ROP (400 series) and an appendix with greater detail.
- Being prioritized with all other filings. Unlikely to hear more by Wednesday, February 4, 2009. There is a large compliance filing in queue ahead of this tasking and we do not know if other work is ahead of the TFE document.
- Once the proposed procedure is ready, it will have a 45–day posting period for industry comments. Similarity to standards review, comment, and vote process is not yet clear. It must be adopted by the NERC BOT.
- NERC and the SDT understand that the Industry needs something now. Need to be able to process TFE by the end of the second quarter of 2009.

- Need to circle around on Wednesday to see if there is more information for the SDT prior to its approval to post the Phase I revisions for review and balloting.
- Dave Taylor noted that in Sacramento the SDT decided TFE was a separate process from Phase 1. He noted the Rules of Procedure process is likely to happen more quickly than the Phase 1 Standards process

SDT Member Comments

- TFE is a big gap that may impact the Phase 1 posting schedule.
- The schedule was to post the responses to comments and revisions to standards on February 5, 2009.
- The Standards Committee meets next week and would be expected to approve for pre–ballot posting.
- A lot of utilities will need to use TFE beginning July 1; they're asking members often what's going to be needed. As soon as possible, they need to know something for them to begin the process.
- Scott Mix added that he is not sure exactly what it will look like, but the SDT can assume the fields that appear in the white paper (standard referenced, etc.) that the SDT reviewed in December won't get stripped out. Some other entries may or may not be acceptable from a legal perspective. The key information that is likely to stay is the information that will take the longest time to develop.
- Entities are counting on the availability of technical feasibility.
- Once posted, can balloting be delayed?
- Are we going to let the clock drive us or are we going to do what is right?
- When will there be industry notice of what is happening?
- Large NERC and FERC compliance filing ahead of this.
- The industry has to be understanding of generation and substation devices. Implementing during the last half of this year.
- Industry needs to understand how this fits with standards development.
- Starts July 1 — need the TFE. Impact on response to industry of Phase 1 products?
- Need to get information, even if it is not in final form.
- Need process in place on July 1. Normally compliance processes take several months.
- If remove reasonable business judgment, must have TFE piece.
- We separated TFE from the standards and handled through compliance and rules of procedure. Industry hasn’t separated this in their understanding. Without clarity and certainty about how this is going to be handled, industry may reject phase 1 changes.
- The SDT is ready to help and also not advisable to post Phase 1 standards for balloting until something is out on the TFE process as well so the industry has what it needs.
- SDT shouldn’t authorize until TFE process is out in some form.

- The Chair and Vice Chair sent a memo to Mike Assante at NERC and copied Dave Cook, NERC General Counsel and Dave Taylor last week and he is aware of the SDT concerns about the importance of moving quickly so that the Phase 1 changes and the TFE process is known.
- Whenever it occurs, the industry wants to know what the TFE process will be and what it will need it by the end of the year. There may be a compliance issue and the industry needs to know how TFE fits into compliance, especially with CIP–007.
- If we get thru the comment response during this meeting, we may want to follow up on Wednesday.
- The Chair and Vice Chair suggested that perhaps a few of us can come up with an interim solution that we can review on Wednesday and will allow us to move forward.

On Wednesday, Scott Mix provided an update on the TFE process noting he had received an e-mail from the NERC Assistant General Counsel that outside counsel started to review the white paper and that nothing had been identified as a show stopper e.g. "good faith efforts". In the SDT discussion the following points were made:

- One new point that they raised concerned "What can you claim a TF for?" Is it only what is called out in the standard, or is the subject broader that defined in the standard?
- Scott cautioned that we will have to wait for the outside counsel to complete their review.
- The majority of comments on such rules of procedure typically come from legal and upper management. The good news is that the process seems to be proceeding more quickly. He expects approval around the middle of the first round of ballots on standard changes. It is possible that the ballot should be delayed in order to ensure the opportunity of review if the SDT believes it is warranted.

III. SDT 706 PHASE II FRAMEWORK REVIEW AND DISCUSSION

A. FERC 706 Order Provisions

The facilitator reviewed related FERC 706 provisions noting they direct the SDT to consider "applicable features" of the NIST framework that might be applied to the CIP:

- "…we direct NERC to address revisions to the CIP Reliability Standards CIP–002–1 through CIP–009–1 considering **applicable features** of the NIST framework. However, in response to Applied Control Solutions, we will not delay the effectiveness of the CIP Reliability Standards by directing the replacement of the current CIP Reliability Standards with others based on the NIST framework." *FERC Order 706, Paragraph 25*

- "…As proposed in the CIP NOPR, the Commission will not at this time direct NERC to incorporate specific provisions of the NIST standards into the CIP Reliability Standards." *FERC Order 706, Paragraph 232*
- "…NERC should monitor the development and implementation of the NIST standards to determine if they contain provisions that will protect the Bulk–Power System better than the CIP Reliability Standards. Moreover, we direct the ERO to consult with federal entities that are required to comply with both CIP Reliability Standards and NIST standards on the effectiveness of the NIST standards and on implementation issues and report these findings to the Commission." *FERC Order 706, Paragraph 233*

B. White Paper Presentation — NIST/FISMA and CIP, Bill Winters

Bill presented his paper, "Independent assessment of FISMA and related NIST documents for adoption for Electric Sector Critical Infrastructure Protection," and an additional section, "Thoughts for Discussion of NIST/ CIP Opportunities" and noted his assignment was to review the NIST/FISMA framework and suggest CIP features that represented strengths that might be incorporated into NIST/FISMA. His approach was to ask and try to answer the question: could my company apply the NIST/FISMA security framework approach? Below are points he made in his presentation:

1. One of the CIP problems is that it is a one size fits all approach. It doesn't distinguish between different big and small facilities and their relative security risks. NIST/FISMA with its focus on life cycle methodology, risk assessment methodology and matching the "controls." It offers more in bringing the electric industry forward in information and system security knowledge and application.
2. "Controls" are most common set of information to provide to industry as a common basis for implementation and protection and 853 represent a "hell of a body of controls." 853A is an assessment process for those controls.
3. The NIST/FISMA approach offers a good educational potential as its series of documents could easily be put together for a curriculum that could be offered industry wide to teach and get everyone up to an equivalent level of understanding of the NIST/FISMA framework which provides capability.
4. The NIST/FISMA framework is not currently targeted towards our kind of control systems (CIP based). But the industry can bridge that gap to meet our needs. You may not have to use only the controls presented in 853 as these could be augmented.
5. All gaps in CIP are largely covered in NIST/FISMA regarding controls regarding any entity type. Even where technical feasibility is limited.
6. The closer and sooner we can get to NIST framework, the faster we will get to a common set of controls across various entities; a framework then that vendors, and industry, will produce an infrastructure grounded in a common set of expectations.

SDT Member Comments

- "Frequently asked questions" may answer some of the NIST questions. Did the FAQ with the standards make it on the NERC Web site yet? The Standards Committee asked for more information on that and its posting is pending the SCs review.
- Most SDT members indicated they have seen questions.
- What was Bill's "plan of attack" in his review and drafting? He indicated he started with 853, FIPS 199 and 200, looked at the FISMA site, with all other documents (about 12 in number). They are voluminous but practical for drafting team to use this process. Bill's second paper addresses this. Is the SDT doing it or is it guidance to industry to do it?
- 853 caveat for control systems — Appendix J. NIST published white paper on control systems speaking to general architecture. How much is 853 applicable to control systems?
- SDT would have to tailor controls to fit our systems. The largest gap in the NIST/FISMA is that they don't address reliability.
- Review the FISMA appendix that addresses how to tailor the controls.
- NIST Draft 2 of 82 goes to next step and addresses control systems. Similarity between process control systems and BES control systems.
- CIP standards may need to be broken apart into: commercial computing environment; different standards in generation plants, etc.
- A plus is that the NIST/FISMA framework is developed and already paid for with tax payer dollars. We can leverage that expertise and apply and tailor it to our industry.
- He thought he would find a disjointed set of documents but was surprised to see the logic and connection of the framework. The SDT could get behind or alongside NIST/FSMA to further documents for the BES.

Thoughts for Discussion of CIP/NIST Opportunities

Bill Winters offered the following thoughts for the CIP/NIST/FISMA SDT discussion that were contained in a second paper he handed out to members:

1. He noted there are some controls in CIP but they are not related together.
2. A possible transition approach could be to walk through CIP standards and tie to NIST guidelines (e.g. analyze system, risk assessment process, etc). The SDT could do this relatively easily. The question would be how much detail we should go to.
3. The SDT could put together controls and break into small working groups to align controls to CIP standards.
4. SDT might recommend letting federal agencies subject to FISMA be able to use it to satisfy CIP requirements.
5. It may be better to create separate set of documents that serve as parallels for control systems vs. creating appendices for things like control systems.

6. Offers two approaches going forward: Heavy alignment vs. Integration Light.
7. *Heavy alignment* — replace/expand CIP-002 requires assessment of: systems used in control and monitoring BES/BPS; systems directly connected and/or exchange data with; and systems which transport data used in control and monitoring.
8. *Light alignment* — develop a set of controls using NIST controls as starting points.
9. Common controls would serve as the basis for certification. How proscriptive they are written will be debated.
10. The industry should be trying to get to a common set of protections and the controls are the fastest route there. Hard work up front, but down the road, there will be less work under a new NIST/FISMA system.
11. The NIST/FISMA framework will enable a more open discussion across the industry of the controls unlike today's CIP discussion.
12. Options in developing and implementing/phasing in over time: e.g. on vendor–by–vendor, system by system etc.

Member Comments

- **Address gaps in both NIST and CIP.** There are gaps for control systems that still need to be addressed in NIST. CIP has benefits for addressing these gaps.
- NIST needs an overarching document that provides step by step. "A read me first" document with an FAQ. There is a 36 pp Guide to NIST information security docs that serves as a roadmap for all docs on the NIST/FISMA website.
- Replace all CIP standards with one requirement? Implement a NIST based protection program to protect critical cyber assets. Would that be close to what the current CIPs provide? May not be close at all. Moving NIST into CIP — care has to be taken; we may end up with more holes
- Moving to be more strongly associated with NIST/FISMA might be better than sticking with where we are with CIP.
- Nothing precludes you from using NIST as basis for building standards. There is a small percent within the industry have to use NIST. A much larger percent can use CIP standards and come up with their own methodology and document in procedures how to do that.
- **Common Controls and Auditing.** You can do it however if you want to in CIP; some struggle with this. When it comes to auditing, what is the outcome? Most prevalent feature in NIST is that you can audit across the entities through the existence of common controls.
- How much reworking would be required to convert to a NIST/FISMA compliant program? There are many ways to meet requirements.
- The SDT's work and output will be roundly criticized if we adopt a narrow scope and basically leave the CIP as is it is now.
- **Outcomes Based Framework.** The SDT should remember the challenge Mr. Assante made to seek to develop an "outcomes based approach and standards". Standards that are

more prescriptive are presumably easier for auditors, but harder for industry to protect assets.

- Let the industry use tools out there as long as the end goal of protecting critical infrastructure is achieved. We are caught between multiple masters. NERC Compliance wants black and white standards requirements audited with a Yes or No.
- **Other Approaches?** In DC all we heard was NIST/FISMA. Are there other standards? Look across all to determine how to build guidelines to have protection. What would be entry to these? 199 document. E.g. all cyber assets in CIP-002 fit in high category. How we categorize systems?
- What would an outcome based standard look like? A "senior manager" outcome entity will put into place a governance program to ensure that an appropriate program is in place to maintain a good security program. Why should CIP mandate a single senior manager. Will FERC buy off? Outcomes may be hard to measure.
- Guideline about the types of people and roles for good practice. Let them figure out who will do. Somebody is responsible for all (1 or 10 different).
- SDT should be trying to move people in direction of NIST framework over the long term. This is "a" methodology.
- **How prescriptive should controls be?** What is the body of controls? Should we be prescriptive and identify a minimum set of protections for each type of system? CIP-002 through CIP-009 does it here and there but leaves a lot for interpretation.
- Trying to be as non–prescriptive in order to preserve choices in implementing security as long as certain goals are met.
- Standards should be telling you "what" to do not "how" to do. CIP may have stepped over the line on the "how" end. In order to make it auditable we may be forced to cross the line again with the "how". 199 and 200 are the standards and 853 a guide.
- If we put anything in a standard it becomes mandatory and enforceable; specifically if we put controls as to what we tell industry they must be doing. E.g. look at kinds of industry comments on the proposal to find a single person who will have to take responsibility. This will be nothing compared to 200–400 pp we will receive on this path.
- **Standards vs. Frameworks.** We need to be clear of difference between standards vs. framework. NIST is a framework that was not intended nor designed to be standards to be certified.
- **Certification Methodology.** We should focus on a framework and then what is the certification methodology we will use. How do we get to that so we are able to have a consistent set of protections?
- Current CIP based on 1200, which was based on ISO 17799. The SDT should pick a framework and develop the adaptation as they can all work. Then consistently implement that framework. All frameworks have provisions for certification.
- Should the SDT propose continuing down the ISO 17799 path? Or go to some other framework?

C. Phase II — CIP and NIST/FISMA — CIP–002–1 Discussion Document, 1–29–09

John Lim presented the team's paper on behalf of Jackie Collett, Scott Rosenberger and John Varnell. He presented a discussion paper for the Phase 2 approach. He noted that the CIP standards are intended to be a baseline for cyber security for bulk power assets with a focus on assets with the highest impact. One of the issues with the current NERC standards which the team discussed the most was the "all or nothing" approach of the current CIP standards, i.e. if an asset is not defined as "critical" under CIP, there are no controls required. Perhaps additional systems and/or functions need to be identified to address this gap.

The team identified the following five issues with CIP-002 and for each offered comments on shortcomings, gaps, challenges and options:

1. Piecemeal Approach.
2. Not protecting assets needing protection. Description, comments, and options.
3. Gaming
4. All or Nothing
5. Loss of Asset Integrity and Misuse

John Lim noted that a multi–level protection scheme will have to identify high, medium, and low. It will be necessary to study which assets are most critical. Look at the function of system and the connection to the BES.

Following the presentation there was a discussion about whether vulnerabilities in common systems should be addressed in the next version of standards. There was also discussion concerning the protection of defined Critical Assets versus protection of all SCADA systems. Several members stated that priority should be given to CIP-002 and the all or nothing view of defining Critical Infrastructure which is in scope as a result of CIP-002 current logic. Several members expressed that at least a minimum level of protection must be prescribed for additional assets.

Member Discussion Points

- All or nothing. Definition of a cyber asset. "Something that is programmable." It is in the NERC glossary. What about network connectivity? Formal definition from NERC. How is programmable being defined?
- What about analogue?
- Programmable or programmed?
- Include anything with firmware. What about subclasses in security environment. Very few of those are left.

- **Focus on High Impact Assets.** Commonality of vulnerabilities — perhaps looking at functionality will address issue. Will focusing on high impact assets address common vulnerability?
- Should this be addressed in standards or in the vulnerability assessment and response system? E.g. "Zero day exploits" problem — the risk of acts that take systems down before we realize vulnerability. Apply good basic security standards and you can deal with this. But if we only look at high impact systems, we may not be addressing this.
- **System Approach.** Industry can/may use a system approach. However, won't do this voluntary. Whatever is not critical asset. This approach doesn't conform with information security. Can we redefine some of these things in standards? No just programmable devices. CIP standards may not be sufficient.
- Many in industry are protecting others even though standard doesn't require. Put critical asset in because that is what they are going to get fined for. You can keep off the CA books but still protect.
- Already addressed/protected in CIP-005
- If this involved anything except critical infrastructure I would trust that people will do the right thing. Don't call cyber security call them reliability.
- System perspective approach — today people only admit to 30 percent of what they have. However, FERC's jurisdiction to BES is tied to interstate commerce moving of power. Bulk power assets is a limited portion of what falls under FERC's jurisdiction. Critical asset list. N– 1, 2, 3 and extreme contingencies. Cyber event — could be in an N–4, 5, 6. From a system perspective, this increases which assets are 'critical"
- Dump CIP-002 and start over again?
- From a NERC standpoint we need to focus on potential attack vectors and will increase in the future.
- Have to study the criticality of the systems we are doing.
- Look at NERC charter — BES doesn't cover every device — agree, but we need to be looking far enough forward to be able to protect that. The end goal is to protect BES, but extent to which the distribution affects BES, we need to be considering whether or not distribution can impact BES and if so, what to do at that level what needs to happen.

D. Strawman — NERC/FISMA Asset Selection Process — Scott Mix

Scott Mix took on the task of trying to conceptualize what would a NERC/FISMA process look like to apply while maintaining the status quo in terms of the scope of the current CIP standards. He created a "strawman" which was presented in a PowerPoint format. He noted that he started with a mission focus on the bulk electric system (BES) vs. the bulk power system (BPS). The law and FERC say BPS whereas NERC has historically used the BES. He noted that some standards have drawn line at various levels and the CIP standards focus only on high impact systems. Most of NIST framework deals with technical protections once assets have been identified.

Scott noted that the FISMA approach requires that all computer assets be included in scope. Using FIPS–199, systems are in scope if needed to accomplish the assigned mission.

He then noted that extending the scope into the distribution system will actually take an act of Congress because the bulk power system does not include distribution. The bulk power system consists of the eight regional bulk electric systems. Characteristics are identified for 3 categories: confidentiality; integrity and availability. Then a high water mark is applied to the highest ranking of the 3 aspects.

Electric system is bisected into Transmission and Distribution. Distribution is off the table by law.

The portion of Transmission dealing with Marketing is also off the table. Transmission is then divided into High, Medium, and Low impact to the BES. Perhaps there needs to be a fourth category that is "ignore" or no impact to reliability. If we applied that methodology to the standards this would classify all transmission assets by impact (high, medium, low, or none). Then the SDT could go through CIP-003 through CIP-009 and determine what the implications are from a reliability standpoint. 800–53 is a good catalog that can be used for an approach excluding the sections that deal with financial, etc, which are not applicable. A key question is would this meet all mandated changes for FERC 706? There are significant implications for the workload for SDT, the workload for education, and the workload for industry implementation. Scott suggested the SDT could have a healthy debate as to whether or not this approach is what the team agrees is the right approach.

SDT Member discussion

- Mainly affect CIP 5, 6 7? Yes but also others.

E. Overarching Principles Presentation and Review — Mike Winters

SDT member Michael Winters drafted these principles for consideration by the SDT. He introduced them making the following points:

- Hoping principles are complementary
- Modify existing standards and get the best of both worlds– CIP and NIST.
- Risk of scrapping and starting over.
- Consider the amount of IT introduced to distribution systems.
- These principles are not mutually exclusive.
- #1, 3 and 5 are consistent with Scott Mix's strawman.
- The concept is to offer protection for all cyber assets associated to operating the interconnected power system but to different degrees based on the risk.

SDT Member Comments before Ranking

- Why not use guideline by Risk Development Working Group?
- Pick a framework. Apply it consistently. 800–53 catalogue – 003–009.
- All cyber assets "Power system". There is not a nice line around generation systems. [Note to Draft: Generation is a critical component to power systems]
- The term Power System IT is simply intended to differentiate from corporate IT.
- Potential for causing someone to make a decision to shut down a plant?
- E.g. continuous emissions monitoring. Fuel supply and multiple infrastructure interdependencies. This is a big issue. SDT can't get to this point for a long time.
- Approach for #1 — catalogue your SCADA, (EMS systems, etc.) and then look at those systems essential to operation of inner circle.
- What is the list of critical assets minimum to perform our mission? Why protect anything else? Or the reverse — identify which assets are critical in order to meet mission. Determine which assets, if turned off, would prove to be critical to meet mission.

Phase II Overarching Principles (Michael Winters)
February 2 SDT Initial Rankings

The Overarching Principles have been re–ordered to reflect the ranking of each principle and their average acceptability from higher to lower. The Strikethrough #s reflect the initial numbering.

1. **(2) Create clear standards and employ a technical exception and compensating controls reporting and guidance process that accommodates deviations.**

Acceptability Ranking Scale	*4 = acceptable, I agree*	*3 = acceptable, I agree with minor reservations*	*2 = not acceptable unless major reservations addressed*	*1 = not acceptable*	*Avg.*
2–2–09 rank	**11** (10/1)	**5**	**1**	**0**	**3.6 of 4**

Author's clarifying comments before SDT initial ranking

- #2 outcome based, not too prescriptive — Exception based standards. Need a clear process with clear standards and TFE process and guidance to accommodate deviations.

2. **(8) A mapping similar to NIST 800–53 Appendix G to CIPs will help quantify and assess the gap, if any.**

Acceptability Ranking Scale	*4 = acceptable, I agree*	*3 = acceptable, I agree with minor reservations*	*2 = not acceptable unless major reservations addressed*	*1 = not acceptable*	*Avg.*
2–2–09 rank	**11**(10/1)	**2**	**2**	**0**	**3.6 of 4**

Author's clarifying comments before SDT initial ranking

- #8 Mapping — refers to NIST 800–53 Appendix G.

3. **(3)Use a consistent risk–based model to classify all assets (i.e. facilities, sites, physical perimeters) (i.e. not cyber assets at this point) as critical/high impact, moderate impact, low impact.**

Acceptability Ranking Scale	*4 = acceptable, I agree*	*3 = acceptable, I agree with minor reservations*	*2 = not acceptable unless major reservations addressed*	*1 = not acceptable*	*Avg.*
2–2–09 rank	**9 (**8/1 ph)	**6**	**2**	**0**	**3.4 of 4**

Author's clarifying comments before SDT initial ranking

- Principle #3 strike/delete from principle reference to going below 100kV. This should be considered "evolution" vs. "revolution."

4. **(4)An entity's Asset classification would be open to scrutiny by regional entities and ERO. The extent of scrutiny to be defined and tightly controlled.**

Acceptability Ranking Scale	*4 = acceptable, I agree*	*3 = acceptable, I agree with minor reservations*	*2 = not acceptable unless major reservations addressed*	*1 = not acceptable*	*Avg.*
2–2–09 rank	**4** (3/1)	**11**	**2**	**0**	**3.1 of 4**

Author's clarifying comments before SDT initial ranking

- #4 allows for scrutiny — "open up the kimono" and have peer reviews or have asset classifications scrutinized by RRO and ERO. Will need and effective arbitration/mediation mechanism.

5. **(7)Use the minimum security controls for high, moderate, low within NIST 800–53 to help model the CIP controls for each level. Address any gaps at the same time but keep the same CIP002 to CIP0XX general format. Industry knows this format, is building policies and programs around it, has commented on it and has voted on it.**

Acceptability Ranking Scale	*4 = acceptable, I agree*	*3 = acceptable, I agree with minor reservations*	*2 = not acceptable unless major reservations addressed*	*1 = not acceptable*	*Avg.*
2–2–09 rank	**5** (4/1)	**8**	**4**	**0**	**3.0 of 4**

Author's clarifying comments before SDT initial ranking

- #7 Use guideline to figure out the controls at different levels. Some customization, reference NIST, Use as starting point.

6. **(6) Any IT devices beyond the perimeter, including telecom, are not part of the CIPs – the CIPs remain perimeter–based where devices on and within the perimeter are protected and everything beyond is considered untrusted.**

Acceptability Ranking Scale	*4 = acceptable, I agree*	*3 = acceptable, I agree with minor reservations*	*2 = not acceptable unless major reservations addressed*	*1 = not acceptable*	*Avg.*
2–2–09 rank	**4** (3/1)	**6**	**6**	**0**	**2.9 of 4**

Author's clarifying comments before SDT initial ranking

- #6 — logistics — interfacing devices and perimeters. Keep perimeter based or trusted zones, still accomplish.

7. **(5) As part of a power system (non–corporate IT) inventory of cyber assets, add an attribute to each device that associates the high/moderate/low classification of the physical**

perimeter/facility/site within which it resides. Apply security controls based on the classification.

Acceptability Ranking Scale	*4 = acceptable, I agree*	*3 = acceptable, I agree with minor reservations*	*2 = not acceptable unless major reservations addressed*	*1 = not acceptable*	*Avg.*
2–2–09 rank	**4** (3/1)	**6**	**7**	**0**	**2.8 of 4**

Author's clarifying comments before SDT initial ranking

- #5. This is logistical and is related to principles #1 (8) and #3 (3)

8. (1)Protect all cyber assets related to power system – not just the Critical Cyber Assets – but to different degrees of protection/controls depending on their classification.

Acceptability Ranking Scale	*4 = acceptable, I agree*	*3 = acceptable, I agree with minor reservations*	*2 = not acceptable unless major reservations addressed*	*1 = not acceptable*	*Avg.*
2–2–09 rank	**3** (2/1)	**8**	**6**	**0**	**2.8 of 4**

The facilitators noted that the authors of the draft papers and principles would be asked to refine them and be prepared to present them at the February 18–19 SDT meeting. That meeting would be devoted to making progress on the SDT's development of a Phase II framework around which the team could organize its work and begin more detailed review of the CIP and the applicability of the NIST.

IV. PHASE I INDUSTRY COMMENT/ SDT RESPONSES

The Chair proposed that the SDT review all of the responses and then, as needed, break into the small groups that had been formed and worked together at the January meeting to complete the task of drafting the responses. The SDT then would reconvene and review and agree on the final response. Following that the SDT would review any changes made in the Phase 1 documents that were out for comment based on the SDT's responses.

Joe Bucciero presented the draft Response Text noting where there were additional responses needed. (See, Appendix #4 for link to a power point presentation). The team looked at each of the additional industry comments that were not available at the January 7–9, 2009 Phoenix meeting. The SDT reviewed and made suggestions related to consistency and content for the small working groups to consider keeping in mind the goal of "good enough to post" the responses. The six small working groups were re-formed to review the industry comments and to refine the SDT's responses. The six groups were created to craft the SDT's responses and to make appropriate edits to the text of the CIP standards.

The small groups reported the results of their drafting later in the afternoon to the full SDT which approved them pending the development of the complete text that was to be developed

overnight by Joe Bucciero along with a redline draft of the Phase I documents with changes made as a result of the industry comments.

On Wednesday, the SDT reviewed all of the proposed changes to the Phase I documents posted for industry review in light of the SDT responses and discussion. The final SDT response document reflecting all of the changes agreed to by the SDT on Tuesday was not ready in final form for the team's review. The Chair asked Mr. Bucciero to distribute the final Response document to the SDT as soon as it was ready.

Kevin Perry made a motion which was seconded by Tom Hofstedder that the SDT will:

- Adopt the SDT Response Document (reflecting Tuesday's agreed on changes)
- Adopt the Proposed Changes to the Phase I Documents (reflecting Wednesday's review)
- Agree to post the documents for the 30 day pre-ballot period.
- However, the Phase I balloting will only commence after the NERC TFE proposal has been posted for industry comment for at least 14 days.

The motion was unanimously adopted by all SDT members present and voting.

V. VSL PROCESS AND DISCUSSION

Dave Taylor, NERC staff reminded SDT members that under the FERC Order 706 the Violation Severity Levels needed to be applied to the CIP 002 through CIP-009. The Standards Committee made a decision to have a separate team assign VSLs to the standards rather than incorporating into the 706 SDT. Project 2008–14 is creating the VSLs. An initial draft of the VSLs is complete, but still needs to be posted for comment. These draft VSLs will ultimately need to be compatible with CIP Phase I efforts of the SDT.

There were questions concerning the relationship of measures vs. VSLs. Mr. Taylor reminded the group that the only thing which is required is the requirements and not the measures.

The SDT discussed the fact that a separate team created the VSL. Mr. Taylor suggested that the original VSLs be posted and then revisions related to this SDT Phase I work could also be posted for comment. The SDT members expressed concerns with the likely confusion with the VSL team and in the industry posting both of these VSL changes (i.e. current CIP and Phase I proposed changes). Mr. Taylor noted that the draft SAR that directed the VSL SDT to only review the current CIP standards was open for comment until February 10, 2009. Members again expressed concerns that two SDTs revising the same documents is sure to cause confusion in the industry. There was discussion regarding whose responsibility it is to create VSLs for the CIP original and Phase I revisions to CIP. There was also discussion concerning the changes and timing or Phase I changes.

The facilitators suggested straw polling to determine the SDT's views on several options going forward.

- **Poll 1**: This team should take on both the CIP current VSLs (Version 1) and Phase 1 (Version 2) and Phase 2 (Version 3) CIP VSLs — **0–18 members supported** this approach.
- **Poll 2**: The VSL team should do both current CIP VSLs (Version 1) and the Phase I VSLs (Version 2) — **16–2 in support of this approach.**

Member Comments following Poll 2

- One member expressed concern about the amount of time it will take for this SDT to agree on comments to be sent on the other team's SAR. That member suggested that individual utilities should comment on the SAR, but consensus is not needed.
- **Poll 3:** The SDT should be responsible for VSL's for both Version 2 (Phase I) and Version 3 (Phase II) of VSL's — **7–11 in support** of proposal.

Following the polls and further discussion, a motion was made by Kevin Perry and seconded by Sharon Edwards as follows:

The following statement, if approved by the SDT, will be forwarded to the SAR Committee as an SDT comment for its consideration with only the names of those SDT members voting in support of the motion:

> **"The Phase I changes ("Version 2") to the CIP standards are expected to be balloted coincident with the development of the VSLs for "Version 1" of the CIP standards. The Project 2008–06 drafting team will not be in a position to include the VSLs with the revised standards due to the timing of the two projects. The VSL drafting team is best positioned to recommend VSLs in support of the Version 2 standards."**

The motion was approved by more than 75 percent of the SDT members present and voting.

The following SDT members voted in favor of sending the following SDT comment to the VSL SAR Committee with their names appended: Jeri Domingo Brewer; Kevin Perry; Jon Stanford; Rob Antonishen; Sharon Edwards; Jay Cribb; Joe Doetzl; Scott Fixmer; David Revill; Phil Huff; Tom Hofstetter; Chris Peters; Keith Stoffer; and Gerry Freeze

The following SDT members voted against the motion: Rich Kinas; John Lim; John Varnell; and Kevin Sherlin.

VI. NEXT STEPS

The facilitators reviewed adjustments to the schedule including:

- A SDT comment on the VLS SAR by the deadline (February 10, 2009)
- February 18–19 in Fairfax, Virginia — advance the Phase II review and discussion
- March 10–12 in Orlando, Florida — seek a Phase II framework going forward.
- April 14–16 in Charlotte, NC — test the Phase II framework in a workshop with cyber experts and refine the framework for presentation at the MRC on May 1.
- May 1 — Members Representative Committee presentation of Phase II framework
- May 18–19 — Refinement to Phase II framework based on MRC comments and determination of whether to issue a white paper for industry comment. Review proposed SDT sub–committee/drafting group structure
- June–December, 2009 — SDT meetings along with SDT drafting groups.

The team then evaluated the meeting

- **What worked?**
  - Small group breakout
  - Papers for Monday's presentation available for advanced review
  - Rapid parking lot

- **What could be improved?**
  - Meeting announcement/agenda versus actual schedule — try to clarify and establish starting and ending times so people can book appropriate travel.
  - 4–3–2–1 vote language needs to be a bit tighter and clearer. Need to allow sufficient time in the session to understand proposals that will be ranked.
  - Underestimation of level of effort to get updated documents available on the last day.
  - Hard to keep track of where we were in the comments list. Needed unique identifier for reference purposes when we do this again.

- **Suggestions for next meeting**
  - Earlier agenda posting (with caveat that there are only two weeks separating meeting on February 18–19).
  - Possible pre–meeting SDT agenda review for future meetings?
  - Consider ways to survey experts

The SDT adjourned at 11:30 a.m.

Appendix # 1

Meeting Agenda — February 2–4, 2009

Draft Meeting Objectives:

- To receive an update on the NERC Technical Feasibility Exception process;
- To complete and adopt the SDT's responses to comments and any changes to the Phase I documents for posting;
- To initiate a SDT review of Phase II principles and potential approaches to integrating CIP and NIST/FISMA; and
- To agree on next steps and the work plan going forward.

Monday	**February 2, 2009**
1:00 p.m.	Welcome and Opening Remarks — Jeri Domingo–Brewer and Kevin Perry • Roll Call • NERC Antitrust Compliance Guidelines • Facilitator Review of January meeting and adoption of January 7–9, 2009 Meeting Summary
1:15	Review of Meeting Objectives and Agenda — Jeri Domingo and Bob Jones
1:20	Organizational Issues and Review of Phase I and early Phase II Schedule — Stuart Langton • Overview of Phase I Work–plan, January– May 2009 • Overview of Phase II Work plan– January–June, 2009– including CIP 002 conceptual approach and workshop and industry input and feedback.
1:40	Update on Phase I SDT Responses to Comments and Procedure Going Forward for Day Two — Jeri Domingo–Brewer
1:50	Update on Technical Feasibility Exception (TFE) Process — Scott Mix
2:00	Introduction to Phase II Review Process — Stuart Langton
2:10	Initial Review of Phase II Principles — Michael Winters
3:00	Break
3:15	Initial Presentation and Discussion of the Phase II White Papers — John Lim (Jackie Collett, Scott Rosenberg, and John Varnell) Bill Winters
4:55	Summary of Day One Outcomes and Review of Day Two Agenda
5:00	Recess
Tuesday	**February 3, 2009**
8:00	Welcome, Agenda Review and Review of Day One Results

8:05	Review of Proposed Procedure/Guidelines for Phase I Comment Review
8:10	Phase I Comment Review and Refinement — Plenary Discussion of Comments
10:15	Phase I Comment Review and Refinement — Plenary Discussion of Comments
12:00	Working Lunch (Return to plenary meeting at 2:00) Small Group Breakouts — Review and Draft Final Responses (As needed)
2:00	Small Group Reports on Draft Responses and Plenary SDT Discussion and Decisions
3:30	Break
3:15	Small Group Reports on Draft Responses and Full SDT Discussion and Decisions
4:50	Summary of Day Two Outcomes and Review of Day Three Agenda
5:00	Recess

Wednesday February 4, 2009

8:00	Welcome and Agenda Review
8:10	Review and Adoption of Phase I Responses and Proposed Changes to Phase I Products
10:00	Review of Work plan for Phase I and Phase II
10:30	(If time permits) Continue Review and Discussion of the Phase II Approach to Integrating CIP and NIST/FISMA.
11:15	Next Steps on Phase II Approach Development
11:30	Technical Feasibility Exception Process Going Forward — Scott Mix
11:45	Meeting Evaluation — What Worked and What Could be Improved?
11:55	Assignments, Next Steps and Review of February and March SDT Agendas
12:00	Adjourn
12:15	Working Lunch and Opportunity for SDT Small Groups to Continue Development of Phase II Products
3:00	Conclude

Appendix # 2

Cyber Security for Order 706 SDT Attendees List
Phoenix AZ
February 2–4, 2009

Attending in Person — SDT Members

1.Rob Antonishen,	Ontario Power Generation
2. **Jeri Domingo–Brewer, Chair**	U.S. Bureau of Reclamation
3. Jay S. Cribb	Information Security Analyst, Principal, Southern Company Services, Inc.
4. Joe Doetzl	Manager, Information Security, Kansas City Power & Light Co.
5. Sharon Edwards	Project Manager, Duke Energy
6. Tom Hoffstetter	Midwest ISO, Inc
7. Scott Fixmer	Senior Security Analyst Exelon Corporate Security, Exelon Corp.
8. Gerald S. Freese	Director, Enterprise Information Security America Electric Power
9. Richard Kinas	Orlando Utilities Commission
10. John Lim	CISSP, Department Manager, Consolidated Edison Co.NY
11. **Kevin B. Perry, Vice Chair**	Director, IT–Infrastructure, Southwest Power Pool
12. Christopher A. Peters	ICF International
13. David S. Revill	Georgia Transmission Corporation
14. Kevin Sherlin	Sacramento Municipal Utility District
15. Keith Stouffer	National Institute of Standards & Technology
16. John D. Varnell	Technology Director, Tenaska Power Services Co.
17. William Winters	Hydro One Networks, Inc. *(Monday only)*
1. Roger Lampilla	*NERC*
2. David Taylor	*NERC*
3. Scott R. Mix	*NERC*
4. Joe Bucciero	*NERC/Bucciero Assoc.*
7. Robert Jones	*FSU/FCRC Consensus Center*
8. Stuart Langton	*FSU/FCRC Consensus Center*

SDT Members Attending via WebEx and Phone

18.Phillip Huff	Arkansas Electric Coop Corporation
19.Jonathan Stanford	Bonneville Power Administration
20.Michael Winters	Hydro One

SDT Members Unable to Attend

1. Jackie Collett	Manitoba Hydro
2. David Norton	Policy Consultant, CIPEnergy Corporation
3. Scott Rosenberger	Luminant Energy
4. Bryan Singer	Kenexis Consulting Corp.

Appendix # 3

NERC Antitrust Compliance Guidelines

I. General

It is NERC's policy and practice to obey the antitrust laws and to avoid all conduct that unreasonably restrains competition. This policy requires the avoidance of any conduct that violates, or that might appear to violate, the antitrust laws. Among other things, the antitrust laws forbid any agreement between or among competitors regarding prices, availability of service, product design, terms of sale, division of markets, allocation of customers or any other activity that unreasonably restrains competition.

It is the responsibility of every NERC participant and employee who may in any way affect NERC's compliance with the antitrust laws to carry out this commitment.

Antitrust laws are complex and subject to court interpretation that can vary over time and from one court to another. The purpose of these guidelines is to alert NERC participants and employees to potential antitrust problems and to set forth policies to be followed with respect to activities that may involve antitrust considerations. In some instances, the NERC policy contained in these guidelines is stricter than the applicable antitrust laws. Any NERC participant or employee who is uncertain about the legal ramifications of a particular course of conduct or who has doubts or concerns about whether NERC's antitrust compliance policy is implicated in any situation should consult NERC's General Counsel immediately.

II. Prohibited Activities

Participants in NERC activities (including those of its committees and subgroups) should refrain from the following when acting in their capacity as participants in NERC activities (e.g., at NERC meetings, conference calls and in informal discussions):

- Discussions involving pricing information, especially margin (profit) and internal cost information and participants' expectations as to their future prices or internal costs.
- Discussions of a participant's marketing strategies.
- Discussions regarding how customers and geographical areas are to be divided among competitors.
- Discussions concerning the exclusion of competitors from markets.
- Discussions concerning boycotting or group refusals to deal with competitors, vendors or suppliers.

III. Activities That Are Permitted

From time to time decisions or actions of NERC (including those of its committees and subgroups) may have a negative impact on particular entities and thus in that sense adversely impact competition. Decisions and actions by NERC (including its committees and subgroups)

should only be undertaken for the purpose of promoting and maintaining the reliability and adequacy of the bulk power system. If you do not have a legitimate purpose consistent with this objective for discussing a matter, please refrain from discussing the matter during NERC meetings and in other NERC–related communications.

You should also ensure that NERC procedures, including those set forth in NERC's Certificate of Incorporation and Bylaws are followed in conducting NERC business. Other NERC procedures that may be applicable to a particular NERC activity include the following:

- Reliability Standards Process Manual
- Organization and Procedures Manual for the NERC Standing Committees
- System Operator Certification Program

In addition, all discussions in NERC meetings and other NERC–related communications should be within the scope of the mandate for or assignment to the particular NERC committee or subgroup, as well as within the scope of the published agenda for the meeting.

No decisions should be made nor any actions taken in NERC activities for the purpose of giving an industry participant or group of participants a competitive advantage over other participants. In particular, decisions with respect to setting, revising, or assessing compliance with NERC reliability standards should not be influenced by anti–competitive motivations.

Subject to the foregoing restrictions, participants in NERC activities may discuss:

- Reliability matters relating to the bulk power system, including operation and planning matters such as establishing or revising reliability standards, special operating procedures, operating transfer capabilities, and plans for new facilities.
- Matters relating to the impact of reliability standards for the bulk power system on electricity markets, and the impact of electricity market operations on the reliability of the bulk power system.
- Proposed filings or other communications with state or federal regulatory authorities or other governmental entities.
- Matters relating to the internal governance, management and operation of NERC, such as nominations for vacant committee positions, budgeting and assessments, and employment matters; and procedural matters such as planning and scheduling meetings.

Any other matters that do not clearly fall within these guidelines should be reviewed with NERC's General Counsel before being discussed.

Appendix # 4

Below is a link to all of the Phase I documents and the Draft SDT Response Document and PowerPoint presentations by Joe Bucciero (Phase I review), Scott Mix (Phase II Strawman) and David Taylor (Phase I VSLs) reviewed by the SDT during the small group and full team discussions in Phoenix, AZ:

http://www.nerc.com/filez/standards/Project_2008–06_Cyber_Security–RF.html

Appendix #5

Background, Principles, and White Paper and Strawman Documents

FERC 706 Background References

Regarding NIST:

25. The Commission believes that the NIST standards may provide valuable guidance when NERC develops future iterations of the CIP Reliability Standards. Thus, as discussed below, we direct NERC to address revisions to the CIP Reliability Standards CIP–002–1 through CIP–009–1 considering applicable features of the NIST framework. However, in response to Applied Control Solutions, we will not delay the effectiveness of the CIP Reliability Standards by directing the replacement of the current CIP Reliability Standards with others based on the NIST framework.

232. As proposed in the CIP NOPR, the Commission will not at this time direct NERC to incorporate specific provisions of the NIST standards into the CIP Reliability Standards. While commenters provide compelling information that suggests that the NIST standards may provide superior measures for cyber security protection, the Commission is concerned that the immediate adoption of the NIST standards would result in unacceptable delays in having any mandatory and enforceable Reliability Standards that relate to cyber security.

233. The Commission continues to believe – and is further persuaded by the comments – that NERC should monitor the development and implementation of the NIST standards to determine if they contain provisions that will protect the Bulk–Power System better than the CIP Reliability Standards. Moreover, we direct the ERO to consult with federal entities that are required to comply with both CIP Reliability Standards and NIST standards on the effectiveness of the NIST standards and on implementation issues and report these findings to the Commission. Consistent with the CIP NOPR, any provisions that will better protect the Bulk–Power System should be addressed in NERC's Reliability Standards development process. The Commission may revisit this issue in future proceedings as part of an evaluation of existing Reliability Standards or the need for new CIP Reliability Standards, or as part of an assessment of NERC's performance of its responsibilities as the ERO.

Phase II Overarching Principles (*Michael Winters)*

***NOTE**: The principles below were drafted and submitted by SDT member Michael Winters. He notes they are applicable to both the 'NIST approach' and the 'CIPs modification' approach and suggests that the approaches may be one and the same. He requests that SDT members "Don't get hung up on any specific term as this is a concept. Terms and definitions can be refined."*

***Note from Michael Winters**: The approach suggested uses an example of facilities/sites being Critical Assets. Consider this a case study where we could then make the 'CA=System' model also work. These principles represent a collection of ideas voiced by several members at previous SDT meetings. It focuses on building upon existing CIPs for improvement rather then starting at the beginning. The foundation for the principles consists of: existing CIPs; NIST 800–53/82; SDT discussion and debate to–date. We have all observed that the SDT has made a few different attempts at finding the starting point for the next phase of changes and the overarching principles to be applied to those changes. It may be time to attempt an approach and then assess its effectiveness at an interim checkpoint. Even if we end up abandoning a main concept, some of the learning's will prove useful for future iterations. Leveraging the existing CIPs instead of a wholesale re–write will still accomplish an incorporation of NIST 800–53/82 where applicable without losing all the good work that has already gone into the CIPs or it being perceived by Industry that their investments in becoming CIP compliant to–date will be stranded.*

1. Protect all cyber assets related to power system — not just the Critical Cyber Assets — but to different degrees of protection/controls depending on their classification.

Acceptability Ranking Scale	*4 = acceptable, I agree*	*3 = acceptable, I agree with minor reservations*	*2 = not acceptable unless major reservations addressed*	*1 = not acceptable*	*Avg.*
2–2–09 rank					

2. Resist creating exception–based standards to accommodate every possible business and operations scenario. Instead, create clear standards and employ a technical exception/compensating controls reporting and guidance process that accommodates deviations.

Acceptability Ranking Scale	*4 = acceptable, I agree*	*3 = acceptable, I agree with minor reservations*	*2 = not acceptable unless major reservations addressed*	*1 = not acceptable*	*Avg.*
2–2–09 rank					

3. Use a consistent risk–based model to classify all assets (i.e. facilities, sites, physical perimeters) (i.e. not cyber assets at this point) as critical/high impact, moderate impact, low impact. Risk Assessment Working Group may be providing a good start and perhaps concepts from FIPS 199 impact analysis can also be

incorporated. This will allow for expansion of standards beyond Critical and to Distribution networks (i.e. below 100 kV – accommodates AMI, Dx automation, etc). Classifying at the physical perimeter level would allow different classifications to exist within a building or at a site (e.g. control room, computer rooms, dev and testing rooms, and back–office at a control centre).

Acceptability Ranking Scale	*4 = acceptable, I agree*	*3 = acceptable, I agree with minor reservations*	*2 = not acceptable unless major reservations addressed*	*1 = not acceptable*	*Avg.*
2–2–09 rank					

4. An entity's Asset classification would be open to scrutiny by regional entities and ERO. The extent of scrutiny to be defined and tightly controlled.

Acceptability Ranking Scale	*4 = acceptable, I agree*	*3 = acceptable, I agree with minor reservations*	*2 = not acceptable unless major reservations addressed*	*1 = not acceptable*	*Avg.*
2–2–09 rank					

5. As part of a power system (non–corporate IT) inventory of cyber assets, add an attribute to each device that associates the high/moderate/low classification of the physical perimeter/facility/site within which it resides. Apply security controls based on the classification.

Acceptability Ranking Scale	*4 = acceptable, I agree*	*3 = acceptable, I agree with minor reservations*	*2 = not acceptable unless major reservations addressed*	*1 = not acceptable*	*Avg.*
2–2–09 rank					**of 4**

6. Interfaces between ESPs/PSPs of two different classifications will take on the controls of the higher classification. Any routers, switches, firewalls, secure FTP, ICCP, DMZ that connects corporate admin networks or external entities to your power system IT (cyber) devices/perimeters get included as a CIP protected device. Any IT devices beyond the perimeter, including telecom, are not part of the CIPs – the CIPs remain perimeter–based where devices on and within the perimeter are protected and everything beyond is considered untrusted.

Acceptability Ranking Scale	*4 = acceptable, I agree*	*3 = acceptable, I agree with minor reservations*	*2 = not acceptable unless major reservations addressed*	*1 = not acceptable*	*Avg.*
2–2–09 rank					**of 4**

7. Use the minimum security controls for high, moderate, low within NIST 800–53 to help model the CIP

controls for each level. Address any gaps at the same time but keep the same CIP002 to CIP0XX general format. Industry knows this format, is building policies and programs around it, has commented on it and has voted on it.

Acceptability Ranking Scale	*4 = acceptable, I agree*	*3 = acceptable, I agree with minor reservations*	*2 = not acceptable unless major reservations addressed*	*1 = not acceptable*	*Avg.*
2–2–09 rank					**of 4**

8. A mapping similar to NIST 800–53 Appendix G to CIPs will help quantify and assess the gap, if any.

Acceptability Ranking Scale	*4 = acceptable, I agree*	*3 = acceptable, I agree with minor reservations*	*2 = not acceptable unless major reservations addressed*	*1 = not acceptable*	*Avg.*
2–2–09 rank					

DRAFT **01/29/09**

Independent assessment of FISMA and related NIST documents for adoption for Electric Sector Critical Infrastructure Protection.

William Winters, Arizona Public Service
*(Distributed before the Meeting)_*

What

First, I have to commend the NIST staff responsible for the development of the guidelines and standards documents that form the FISMA framework. This body of work provides an incredibly comprehensive background and framework for information security.

To a limited degree, the current version of CIP standards at least attempted to capture the essence of fundamental cyber security implementation and management however, as is evidenced by the creation of the SDT, the full extent of what is required was missed. In the years since the CIP standards were conceived, NIST expanded and refined the cyber security framework and standards documents required for FISMA. These documents embody the essence and the detail required for Information Security Management. In fact, the NIST FISMA documents go beyond a framework by providing the narrative background at a fundamental level necessary to develop a clear understanding of the framework, intent and method of implementation to non–cyber security professionals. A clarity that is largely lacking in the CIP standards.

To date the SDT 706 Phase II discussions have largely centered on NIST 800–53 and integration with the CIP standards. To a lesser degree, FIPS–199, NIST 800–53A and FISMA have been discussed.

I feel at this time expanding the discussion to FISMA and the full body of associated NIST standards and guidelines is warranted. Not simply should or how NIST 800–53 can be integrated but to what degree should or can CIP integrate or parallel FISMA.

After review of FISMA as documented and the supporting NIST documents, I count myself an advocate of integration and, to a significant degree, adoption of the FISMA/NIST approach to Information Security Management for electric sector CIP standard.

Why

The FISMA/NIST framework provides a consistent methodology to install a set of security protections appropriate to the criticality of an information system and the associated information.

It is well thought out, documented and based on the fundamentals of cyber security and SDLC. The guidelines provide the fundamental security background as well as the guidance for application.

It is a body of work that is easily accessible by all industries and sectors and all sizes of entities, service providers, vendors, auditors, etc. It is a requirement for federal agencies including those in the electric sector. As such, it represents a common framework. Ambiguity is minimized. Knowledge sharing is maximized.

The use of a common framework will provide the greatest opportunity for uniform application of cyber security controls to protect our Critical Infrastructure. Fundamentally, it provides a common basis for assessment, implementation and audit regardless of sector or service entity.

As much as the existing CIP standards may get most entities to the point of implementing appropriate cyber security controls, it will not have been done in a consistent manner with clear mutual understanding of the objectives.

Though the body of NIST documents is of significant volume, the effort required to understand and apply is in no way more difficult than the effort that has been expended to understand and apply the CIP standards. The most significant difference is that after the NIST process is assimilated, security controls may be implemented consistently, monitored consistently, changed consistently and, assessed consistently.

Protecting our cyber managed supply of electricity in a consistent manner across all entities is the best thing to do.

It's paid for.

How

Integration approaches can range from drawing on individual elements in the NIST documents to fill in the CIP gaps requirement by requirement to wholesale adoption of FISMA.

My recommendation is that we take an approach that establishes a strong parallel to FISMA, utilizing the NIST standards and guidelines as much as possible.

In its most pervasive manifestation, this would entail a combination of adopting the FISMA/NIST documents directly and/or creating parallel documents/supplements tailored to the electric sector. This would likely result in an overhaul of the current CIP requirement layout and require transition education.

At a minimum, this would entail developing a set of controls (800–53), related assessment procedures (800–53A) and FIPS 200 Minimum Security Requirements equivalent specific to BES entities, creation of FIPS 199 Security Categorization equivalent that integrates to CIP 002 and other CIP requirements to relevant NIST documents.

The degree to which the FISMA/NIST framework should be adopted will need to be discussed and debated.

A couple of fundamental questions:

- Does FERC feel that adoption of FISMA/NIST framework will meet all the concerns in Order 706?
- What were the concerns with adopting the FISMA/NIST framework as the basis for the existing CIP standards and do those concerns still exist?

W Winters 02/02/09
Thoughts for discussion of CIP/NIST opportunities
(Handed out at the meeting)

- Develop set of controls for each area/entity which could be done regionally
- Entities can create control extensions. This is currently allowed in the NIST method
- Allow option for federal entities currently subject to FISMA and CIP to use FISMA/NIST to satisfy CIP
- Encourage use of FISMA/NIST today. Entities have the option today to use FISMA/NIST as a basis for meeting CIP requirements.

- Develop a process for application of FISMA/NIST (e.g. Develop as an overlay of CIP or Develop as standalone)

Controls Development Approach

- SDT sub–team(s) could develop initial minimum controls (they could be entity tailored controls and/or "exception" based controls)
- Create clearinghouse for sharing of controls amongst entities as different organizations develop control extensions
- Develop controls using working group model at the regional level. This could be extended to development of educational framework and more effective open information sharing.
- Lifecycle management of controls for improvement/refinement and adoption
- Regional controls could feed to national and periodic update with regional, national and NIST representation.
- NIST and/or SDT team create initial draft of documents for "CIP" (e.g. appendices to existing or separate set of docs,)
- Build transition education program based on mapping of CIP to NIST.
- As body of controls are refined and standardized, auditors, developers of compliance programs (internal, consultant/vendor), developers of applications, support personnel, etc. have common reference and interpretation of the standards

Heavy alignment:

1. Expand/replace CIP 002 to require assessment of:

   a) Systems used in control and monitoring of BES/BPS
   b) Systems directly connected and/or exchange data with
   c) Systems which transport data used in control and monitoring

2. Develop equivalent FIPS 199, FIPS 200
3. Develop Risk Assessment process (800–37 equivalent/appendix) tailored to industry.

Integration light (in the beginning):

1. Develop set of controls (can use existing NIST controls as starting point) for each of the CIP requirements. Some of these exist within the CIP standards today but not consistently.
2. Systems that are determined in CIP 002 to be CCA are classified as high, as are all systems within the same ESP and form the ESP. Monitoring systems get medium?
3. 3Map CIP requirements to NIST docs as guidelines particularly for Risk Assessment

CIP–002–1 Discussion Document, 1–29–09

Jackie Collett, John Lim, Scott Rosenberger, and John Varnell

I. Original Intent of the CIP–002 Version 1 Standard

- **Starting Point**: A "reasonable" initial attempt to applying cyber security to the electric infrastructure.
  - Initial Baseline – starting from zero
- High Impact Focus: Reduces the scope of implementation to the transmission and generation assets which have the highest impact on the reliability and operability of the BES.
- Cyber Assets: directly linked to the BES elements *FAQ Q2*
- Cyber Asset Scope: limited to control centers, remote access and "jumping–off" points, which may not be evident in the standard *FAQ 2*
- What to Do: Not How to Do
- Non–prescriptive: Allows flexibility for a wide range of scenarios

- **Key Decisions**:
  - Create "trusted zones"
  - Exclude communications outside of "trusted zones": often external carriers and indeterminate paths

- **Assumptions**: Not explicit in the standard, but required for good security
  - **Redundancy**: Critical Asset / Cyber Asset redundancy does not eliminate the requirement for cyber protection. *FAQ Q5*
    - Need to protect common modes of failure.
    - Multiple attacks / compromises are possible electronically.
  - **"Systems approach"**: A systems approach to identifying Critical Assets / Critical Cyber Assets can and should be used. CIP–002 does not preclude a systems approach, but does not explicitly require it.
  - **"Consider"**: Consider means include if at all applicable.
  - **"Essential to operation":** Critical Assets and Critical Cyber Assets should be identified and protected to ensure sustainable and reliable operation indefinitely. Loss or compromise of the Control Centre or other critical functions is not sustainable.
  - **Critical Assets**: Critical Assets may include sites, elements and systems.
  - **CCA Compromise**: In addition to the BES impact due to loss of the Critical Asset or Critical Cyber Asset, compromise of the Critical Cyber Asset must be included in the risk assessment (Integrity).
- FERC conditionally approved the Version 1 standards, and directed changes for a "final" version

- The "gap" is what is currently under discussion

II. Important Aspects of CIP–002–1

1. **Relationship to BES**: There is a very clear relationship between the BES assets required for reliability and the cyber assets essential for their operation. The reliability and operations segments of the electric industry are structured upon BES assets. This includes processes, procedures, inventories and terminology.
2. **High Impact Focus**: CIP–002–1 focuses the efforts and resources for protection to the most important BES assets and associated cyber assets, recognizing that resources are not unlimited. Assets which do not affect the reliability and operability of the BES are not considered. As a result, the majority of the BES assets are not included for protection under the CIP standards.
3. **Industry Acceptance**: The electric industry has invested thousands of hours and millions of dollars to meet CIP–003–1 through CIP–009–1 based on CIP–002–1. The industry would not favor a significant or radical change to the asset identification method, and could reject it.

III. Issues identified with the current CIP–002 + Standards

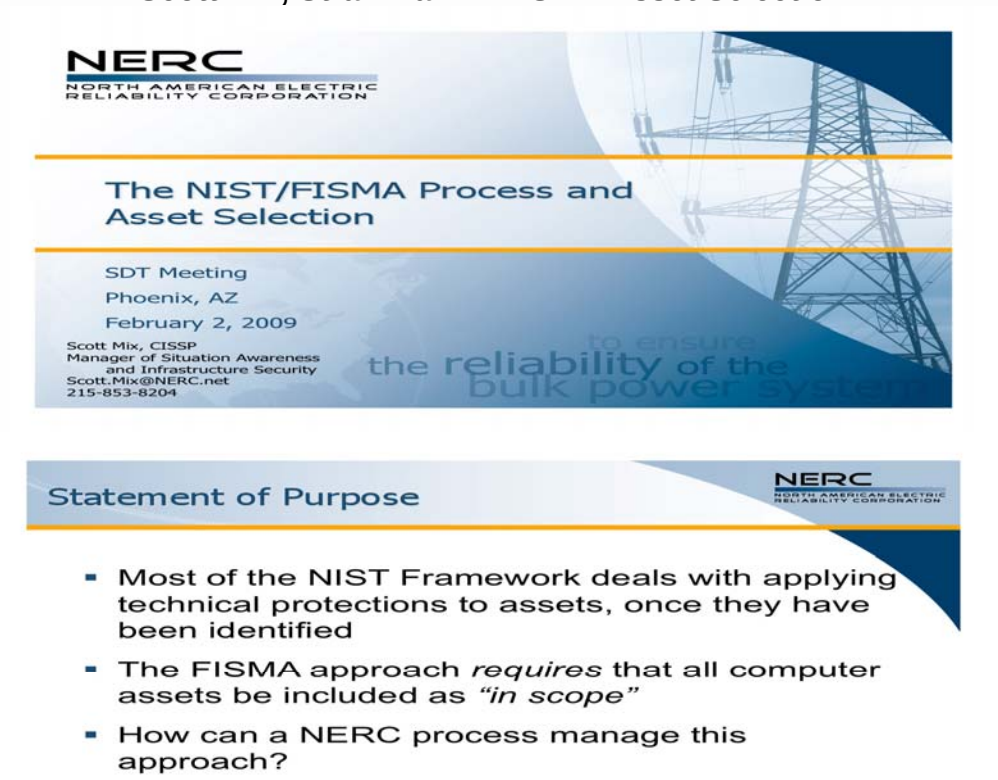
A		**Piecemeal Approach**
	Description	By identifying individual Critical Cyber Assets, security gaps exist when the CCAs operate in a system. (E.g. data integrity impact for a cyber asset outside of the ESP)
	Comment	• The identification of Critical Cyber Assets does not preclude a systems approach, but does not explicitly require it. • A Critical Cyber Asset may be part of a system or network, including other cyber assets, which is currently addressed somewhat by the ESP. • The standards do not address interdependent functions across ESP boundaries, which may be essential to the Critical Cyber Asset and/or the BES.
	Options	1. Need to include both Critical Cyber Assets and critical functions. 2. Need to include an impact assessment of the components required for the critical function. 3. Need to include consideration and protection for interfaces into the Critical Cyber Assets – may be at a different risk level. Protection may be required outside of the ESP.
B		**Not Protecting Assets Needing Protection**
	Description	Assets which may have an impact on the BES, either singly or in conjunction with other assets are not being identified under CIP–002.
	Comment	• Compliance with the NERC cyber security standards is onerous.

		• There are large penalties for non–compliance. • Criticality based on BES system planning models (e.g. PSSE) are not adequate. BES interconnectivity and interdependencies are very different from cyber connectivity and interdependencies. • Area requirements or impacts may not be available or considered in the identification of Critical Assets and Critical Cyber Assets (e.g. generation units' impact on the reliability and operability of the BES in a geographical area). • Perception of "missing Critical Assets" creates a lack of confidence in the industry to self–manage.
	Options	1. Include some responsibility for the BA in determining Critical Assets based on area impact (area overview). 2. Single largest contingency must be included in the impact / Critical Asset identification. 3. The Identifying Critical Assets Guideline1 provides detailed guidance for Critical Asset evaluation. 4. Targeting specific risks / impacts can help focus the protection requirements.
C	**Gaming**	
	Description	Entities are striving to create minimal or null Critical Asset Lists to avoid the effort and expense of complying with the standards.
	Comment	• Some entities are taking a very literal interpretation of the standards, and some oppose guidance that is not explicitly included in the standards. • Asset identification by some entities has been perceived as "unreasonable" and generated criticism of the industry. • All compliance avoidance (gaming) cannot be completely anticipated or eliminated. • Gaming will occur regardless of the methodology or framework applied. These issues can be addressed over time through the audit and compliance enforcement process. • "Zero tolerance" for non–compliance: self–report a violation and possibly be fined (compliance culture vs. good security practice)
	Options	1. Improve clarification of the intent of the standards and the requirements.
D	**All or Nothing**	
	Description	Assets or cyber assets are either critical and require protection, or not critical and do not require any protection.
	Comment	• Conducted diligently, including the interdependencies of systems required for essential functions, the asset identification can provide an adequate level of security for the BES. • NERC's mandate is to protect the BES. This does not include distribution and the related assets.

[1] The NERC Guideline "Identifying Critical Assets" is presently under development by the Critical Infrastructure Protection Committee Risk Assessment Working Group. The development of this guidance document was directed by FERC in its NOPR, and reconfirmed in FERC Order 706 p253.

		• There are no graduations or levels of assets, and no levels of protection for cyber assets. ***Options*** 1. The fundamental tenet of the NERC reliability standards is to protect the reliable operation of the BES; therefore the focus of cyber protection, for both BES assets and cyber assets, should be on their impact to the reliable operation of the BES. 2. The Identifying Critical Assets Guideline1 provides some criteria to help define impact to the BES. 3. There may be a need to define what systems beyond the current Critical Assets need protection. 4. Required protection of cyber assets may be related to some characteristics (contains an operating system / purpose–written software / no software). 5. Multiple levels of protection do exist in the standards: critical cyber asset vs. non–critical cyber asset in an ESP vs. cyber asset outside an ESP. May want to provide a different granularity. 6. Define the breadth and depth of protection.
5	**Loss of Asset – Integrity / Misuse**	
	Description	Determining the criticality of BES assets tends to focus on a loss (outage) of the asset. Loss of data integrity or misuse of the cyber assets may not be considered.
	Comment	– Loss of an asset is a traditional risk analysis approach which may be incomplete for cyber impacts. – Can be combined with other system or cyber events, increasing the impact – Need to include the analysis of intentional and unintentional misuse.
	Options	1. Consider magnitude of impact of loss of data integrity / misuse: o Generation or Transmission Control Centre – possible impact. o Transmission Substation or Generation Assets – little or no impact depending upon the size or function of the facility. May be related to the single largest contingency. o ISO – possible impact. 2. Need to educate industry to consider intentional and unintentional misuse

Scott Mix, Strawman — FISMA Asset Selection

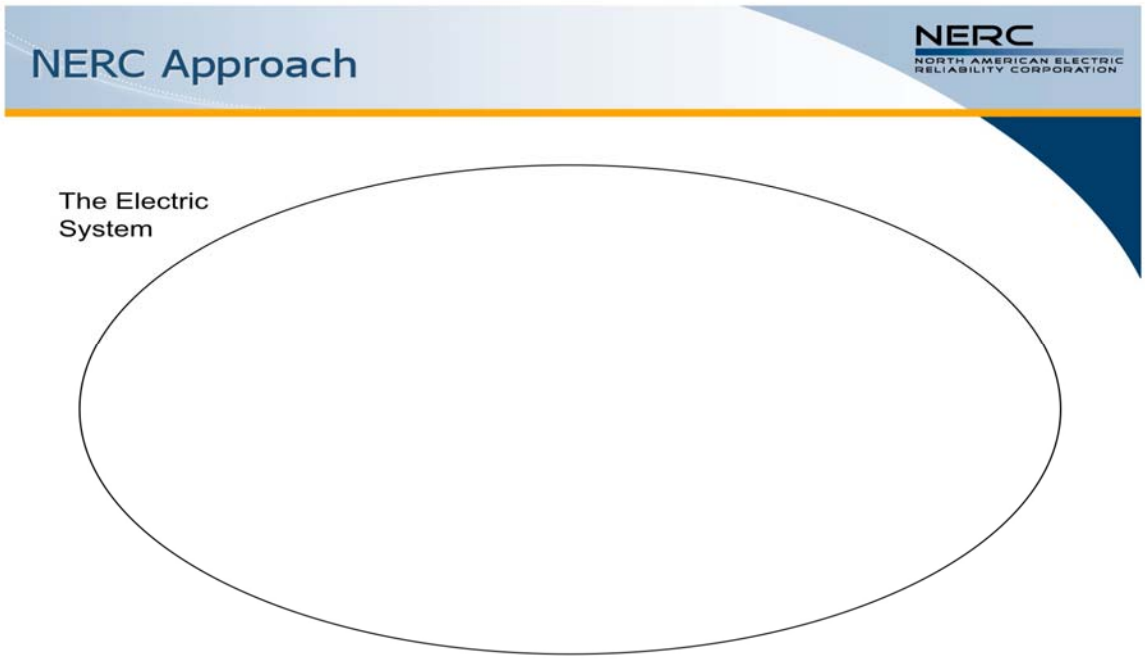


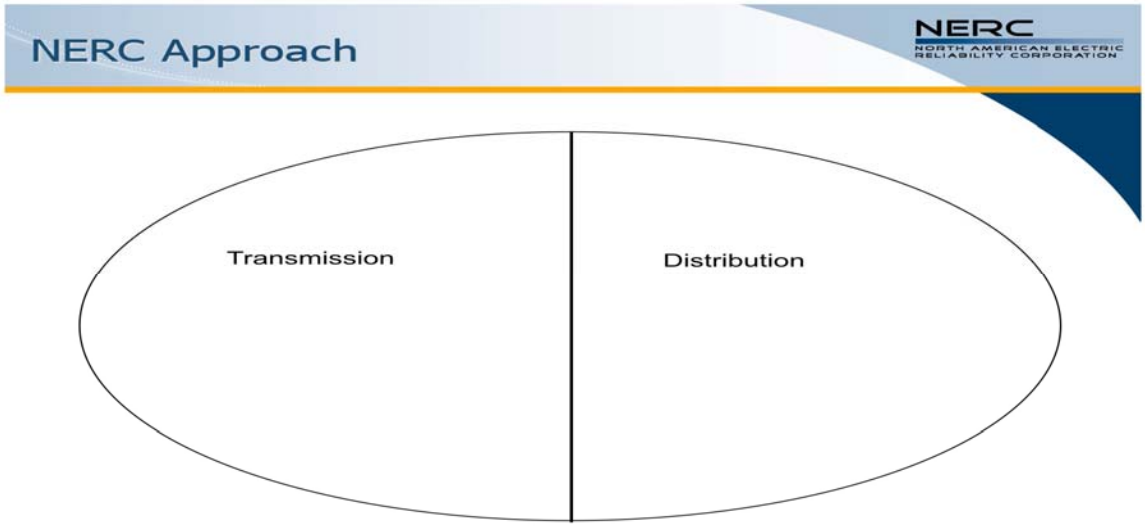
Categorization of Assets

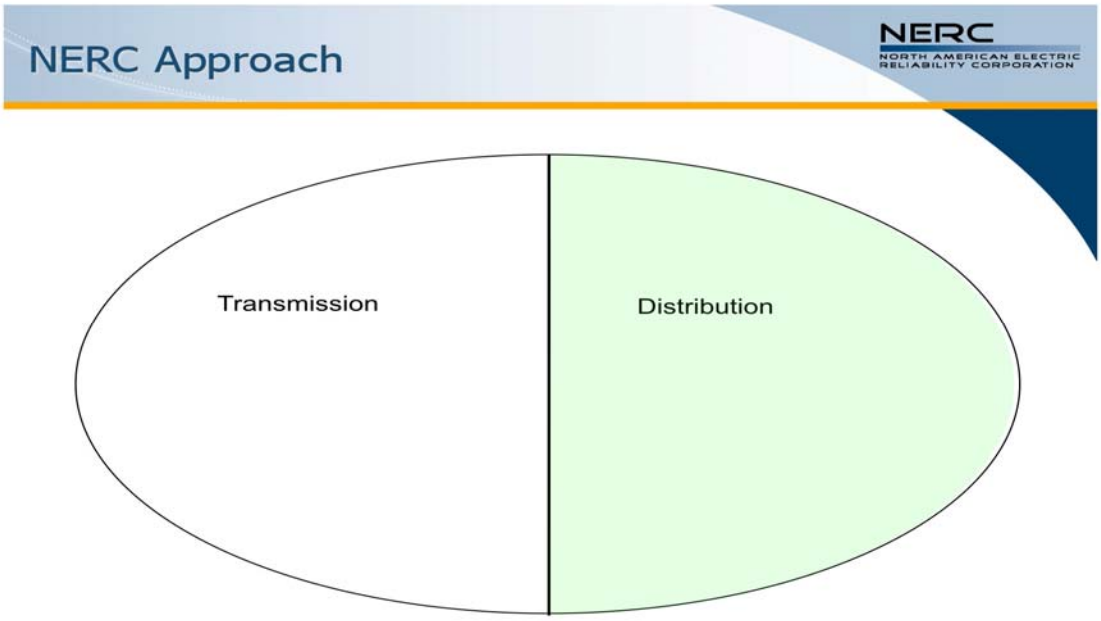
- FIPS-199:
  - Mission Focus:
    - "The security categories are based on the potential impact on an organization should certain events occur which jeopardize the information and information systems needed by the organization to accomplish its assigned mission, protect its assets, fulfill its legal responsibilities, maintain its day-to-day functions, and protect individuals." (emphasis added)
    - "Security categories are to be used in conjunction with vulnerability and threat information in assessing the risk to an organization."

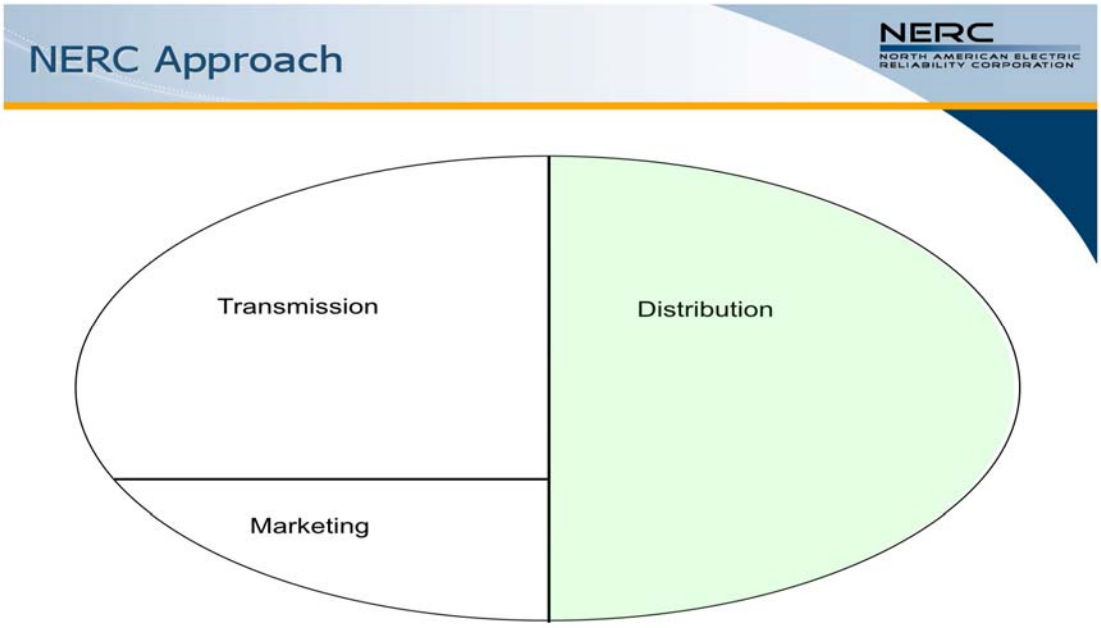
Categorization of Assets

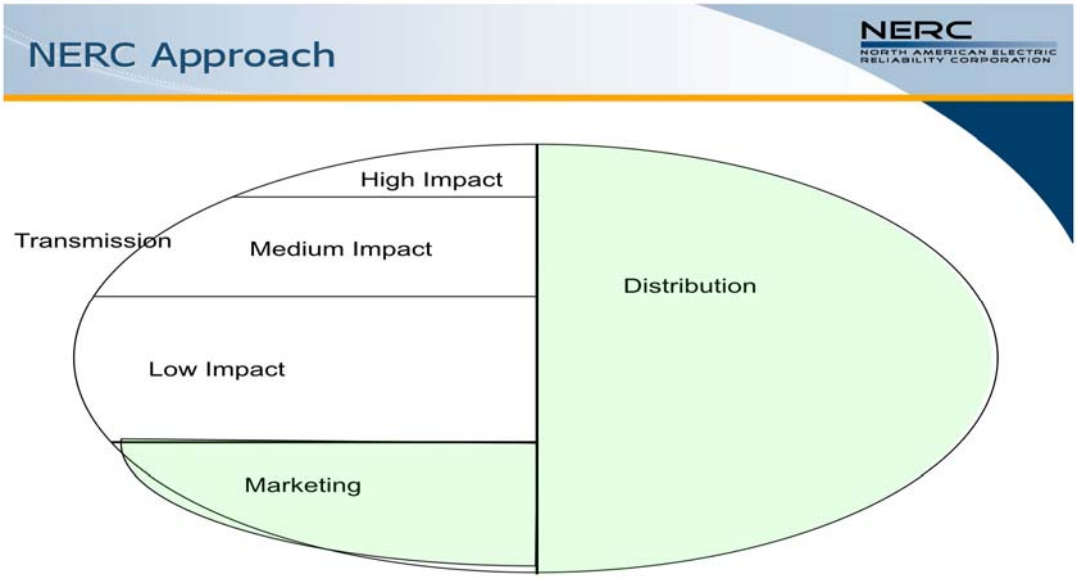
- FIPS-199:
  - Characterize in 3 categories:
    - Confidentiality
    - Integrity
    - Availability
  - Assign level to each category:
    - Low
    - Medium
    - High
  - High Water Mark
  - Customize controls (later)

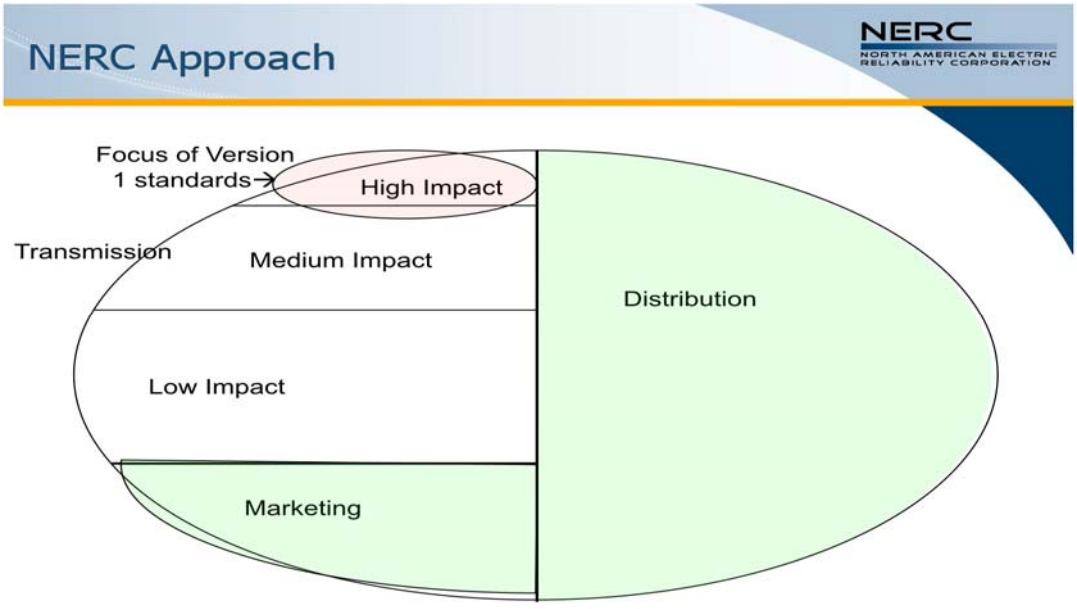

NERC Approach
NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION
The Electric System


NERC Approach
NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION
Transmission
Distribution

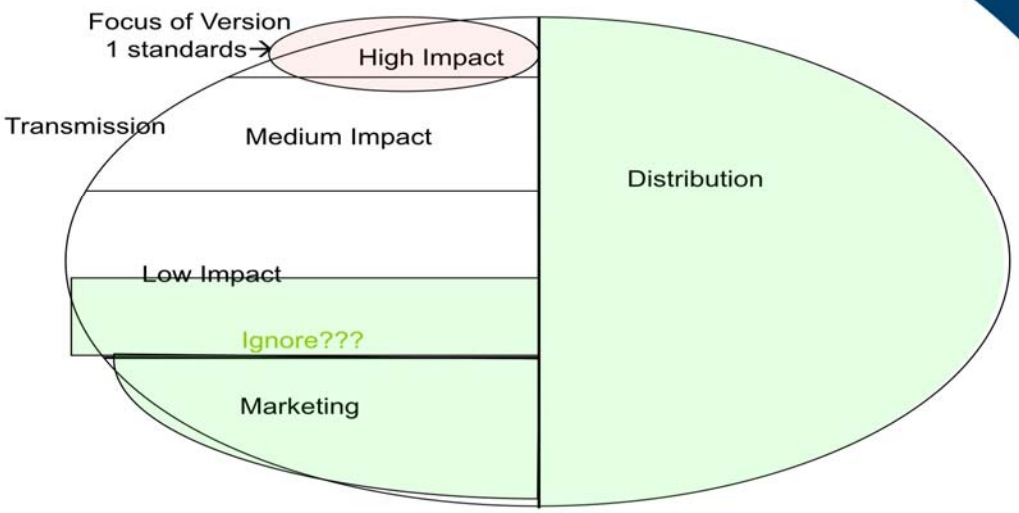

NERC Approach
NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION
Transmission
Distribution


NERC Approach
NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION
Transmission
Distribution
Marketing


NERC Approach
NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION
High Impact
Transmission
Medium Impact
Distribution
Low Impact
Marketing


NERC Approach
NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION
Focus of Version 1 standards
High Impact
Transmission
Medium Impact
Distribution
Low Impact
Marketing

NERC Approach



NERC Approach

- This would require changes:
  - CIP-002 to classify ALL transmission assets by impact category
  - CIP-003 to CIP-009 – requirement-by-requirement specificity for obligations at each impact category level
    - SP800-53 Catalog as an example

NERC Approach

- Separate set of standards for:
  - Control Centers
  - Transmission Facilities
  - Generation Facilities
- Each with 3 levels of requirements
  - Not every requirement would expand – but most would
  - Essentially expanding current requirement set by practically a factor of 9 just to maintain *status quo* with requirement scope

NERC Approach

- Would this meet all the mandated (ordered) changes from FERC Order 706???
  - Probably not by itself
  - Would require significant additional work on top of what was just described.

Appendix # 6

SDT Consensus Guidelines
Adopted Unanimously, November 13, 2008

The Cyber Security for Order 706 Standard Drafting team (team) will seek consensus on its recommendations for any revisions to the CIP standards.

General consensus is a participatory process whereby, on matters of substance, the members strive for agreements which all of the members can accept, support, live with or agree not to oppose. In instances where, after vigorously exploring possible ways to enhance the members' support for the final package of recommended revisions, and the team finds that 100 percent acceptance or support of the members present is not achievable, final consensus recommendations will require at least 75 percent favorable vote of all members present and voting. This super majority decision rule underscores the importance of actively developing consensus throughout the process on substantive issues with the participation of all members. In instances where the team finds that even 75 percent acceptance or support is not achievable, the team's report will include documentation of any differences as well as the options that were considered for which there was greater than 50 percent support from the team. The team will develop its recommendations using consensus–building techniques with the leadership of the Chair and Vice Chair and the assistance of the facilitators. Techniques such as brainstorming, ranking and prioritizing approaches will be utilized. The team's consensus process will be conducted as a facilitated consensus–building process. team members, NERC staff and facilitators will be the only participants seated at the table. Only team members may participate in consensus ranking or vote on proposals and recommendations. Observers/members of the public are welcome to speak when recognized by the Facilitator and all written comments submitted on the comment forms will be included in the team and facilitators' summary reports.

The team will make decisions only when a quorum is present. A quorum shall be constituted by at least 51 percent of the appointed members being present (simple majority). The team will utilize Robert's Rules of Order *(as per the NERC Reliability Standards Development Procedure)*, as modified by the team's adopted procedural guidelines, to make and approve motions; however, the 75 percent supermajority voting requirement will supersede the normal voting requirements used in Robert's Rules of Order for decision making on substantive motions and amendments to motions. In addition, the Council will utilize their adopted meeting guidelines for conduct during meetings. The Council will make substantive recommendations using their adopted facilitated consensus–building procedures, and will use Robert's Rules of Order only for formal motions once a facilitated discussion is completed.

The presiding chair and/or Facilitator of the SDT, in general, should use parliamentary procedures set forth in Robert's Rules of Order, as modified by Council's adopted procedural guidelines.

To enhance the possibility of constructive discussions as members educate themselves on the issues and engage in consensus–building, members agree to refrain from public statements that may prejudge the outcome of the team's consensus process. In discussing the team process with the media, members agree to be careful to present only their own views and not the views or statements of other participants and/or may direct such inquiries to the team Chair and Vice Chair. In addition, in order to provide balance to the team process, members agree to represent and consult with their stakeholder interest group.

Meeting Guidelines for Participants

Participants' role in meetings:

- Explore possibilities
- Listen to understand (Respect) (limit sidebar conversations)
- Be focused and concise. (Avoid repetition. No need to offer comments in "strong agreement.")
- Focus on issues, not personalities.
- Offer options to address others' concerns.
- No sidebars.
- If participating by phone, indicate who is speaking.
- If participating by phone, please use the mute button. **Do not** put the phone on hold.

Facilitators/Staff role in meetings:

- Assist the Chair and Vice Chair in helping the team stay on task
- Help the group follow agreed upon ground rules
- Design the meeting and problem solving process in consultation with the Chair and Vice Chair
- Facilitate discussion participation of the team and other participants
- Prepare agenda packets and reports

Consensus Building Techniques

- **Brainstorming** (green light thinking – not judgmental) At certain points, the facilitator may ask the group to suspend judgment and get ideas onto the table before debating.

- **Name Stacking in Team Discussions** (use of name tents to seek attention)

- **Acceptability Consensus Ranking Scale**
  - Use a consensus acceptability scale to help focus discussion and test support in reviewing substantive issues.

- Use to guide and focus discussion and as a poll to see where the team stands, not used as a voting mechanism.
- Must be prepared to offer refinements and suggestions to address serious concerns.

4 = Proposal is acceptable as it is
3 = Proposal is acceptable; I can live with it but there are minor concerns to address
2 = Proposal is not acceptable. Proposal may be acceptable if the major concerns are addressed
1 = Proposal is not acceptable

o **Consensus Ranking Scale**

4. Comfortable—I support proposal as is ♥♥♥♥
3. Minor Reservations— I can live with this; but would like to see changes as follows♥♥♥ Be prepared to offer specific refinements or changes to address your concerns.
2. Major Reservations—I can't support this unless following changes are addressed to meet my serious concerns ♥♥ Be prepared to offer specific refinements or changes to address your concerns.
1. Fatal Flaws—I can't support this ♥ Be prepared to offer alternatives and options that would address your own as well as other's concerns.

o **Robert's Rules of Order and Facilitated Consensus Building Procedures**

The Council will make substantive recommendations using their adopted facilitated consensus–building procedures, and will use Robert's Rules of Order only for formal motions once a facilitated discussion is completed.

Standard Development Roadmap

This section is maintained by the drafting team during the development of the standard and will be removed when the standard becomes effective.

Development Steps Completed:

1. The Standards Committee (SC) accepted the Standards Authorization Request (SAR) for Project 2008-06 Cyber Security Order 706 on March 10, 2008.
2. The SAR for Project 2008-06 Cyber Security Order 706 was posted for industry comment March 20–April 19, 2008.
3. Nominations for the SAR drafting team members were solicited March 20–April 4, 2008.
4. The Executive Committee of the SC appointed the SAR drafting team for Project 2008-06 Cyber Security Order 706 on April 25, 2008 and the full SC ratified the Executive Committee's action on May 8.
5. The SC accepted the SAR and approved moving forward with Project 2008-06 Cyber Security Order on July 10, 2008.
6. Nominations for the standard drafting team (SDT) for Project 2008-06 Cyber Security Order 706 were solicited July 15–28, 2008.
7. The Executive Committee of the SC appointed the SDT for Project 2008-06 Cyber Security Order 706 on August 7, 2008.

Proposed Action Plan and Description of Current Draft:

The standard drafting team for Project 2008-06 Cyber Security Order 706 (SDT CSO706) has been assigned the responsibility to review each of the following reliability standards to ensure that they conform to the latest version of the ERO Rules of Procedure, including the Reliability Standards Development Procedure, and also address all of the directed modifications identified in the FERC Order 706:

CIP–002–1 — Cyber Security — Critical Cyber Asset Identification
CIP–003–1 — Cyber Security — Security Management Controls
CIP–004–1 — Cyber Security — Personnel and Training
CIP–005–1 — Cyber Security — Electronic Security Perimeter(s)
CIP–006–1 — Cyber Security — Physical Security
CIP–007–1 — Cyber Security — Systems Security Management
CIP–008–1 — Cyber Security — Incident Reporting and Response Planning
CIP–009–1 — Cyber Security — Recovery Plans for Critical Cyber Assets

Because of the extensive scope of Project 2008-06 Cyber Security Order 706 the SDT CSO706 is implementing a multiphase approach for revising this set of standards.

Phase I of the project includes necessary modifications to CIP-002-1 through CIP-009-1 to comply with the near term specific directives included in FERC Order 706. In particular, the SDT addressed the directive in FERC Order 706 that the "... ERO modify the CIP Reliability Standards through its Reliability Standards development process to remove references to reasonable business judgment before compliance audits begin in 2009." In addition, a number of other directives included in FERC Order 706, which apply to specific standards are also addressed in Phase I. More contentious issues to be addressed by the SDT associated with the modification of this set of standards will be addressed in a later phase(s) of Project 2008-06 Cyber Security Order 706.

This posting of the cyber standards for industry comment only relates to Phase I of the project. Specifically, SDT CSO706 produced a revised version of Standard CIP–002–2 — Cyber Security — Critical Cyber Asset Identification and is posting the proposed modifications for a 45-day comment period.

Future Development Plan:

Anticipated Actions	Anticipated Date
1. Develop and post reply comments to initial posting of standard for industry comment	January 7–February 17, 2009
2. Post for 30-day pre-ballot period.	February 18–March 31, 2009
3. Conduct initial ballot	April 2–11, 2009
4. Post response to comments on first ballot	April 20–May 12, 2009
5. Conduct recirculation ballot	May 13–22, 2009
6. Board adoption date.	To be determined.

A. Introduction

1. Title: Cyber Security — Critical Cyber Asset Identification

2. Number: CIP-002-2

3. Purpose: NERC Standards CIP-002-2 through CIP-009-2 provide a cyber security framework for the identification and protection of Critical Cyber Assets to support reliable operation of the Bulk Electric System.

These standards recognize the differing roles of each entity in the operation of the Bulk Electric System, the criticality and vulnerability of the assets needed to manage Bulk Electric System reliability, and the risks to which they are exposed.

Business and operational demands for managing and maintaining a reliable Bulk Electric System increasingly rely on Cyber Assets supporting critical reliability functions and processes to communicate with each other, across functions and organizations, for services and data. This results in increased risks to these Cyber Assets.

Standard CIP-002-2 requires the identification and documentation of the Critical Cyber Assets associated with the Critical Assets that support the reliable operation of the Bulk Electric System. These Critical Assets are to be identified through the application of a risk-based assessment.

4. Applicability:

4.1. Within the text of Standard CIP-002-2, "Responsible Entity" shall mean:

4.1.1 Reliability Coordinator.

4.1.2 Balancing Authority.

4.1.3 Interchange Authority.

4.1.4 Transmission Service Provider.

4.1.5 Transmission Owner.

4.1.6 Transmission Operator.

4.1.7 Generator Owner.

4.1.8 Generator Operator.

4.1.9 Load Serving Entity.

4.1.10 NERC.

4.1.11 Regional Entity.

4.2. The following are exempt from Standard CIP-002-2:

4.2.1 Facilities regulated by the U.S. Nuclear Regulatory Commission or the Canadian Nuclear Safety Commission.

4.2.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

5. Effective Date: The first day of the third calendar quarter after applicable regulatory approvals have been received (or the Reliability Standard otherwise becomes effective the first day of the third calendar quarter after BOT adoption in those jurisdictions where regulatory approval is not required)

B. Requirements

R1. Critical Asset Identification Method — The Responsible Entity shall identify and document a risk-based assessment methodology to use to identify its Critical Assets.

R1.1. The Responsible Entity shall maintain documentation describing its risk-based assessment methodology that includes procedures and evaluation criteria.

R1.2. The risk-based assessment shall consider the following assets:

R1.2.1. Control centers and backup control centers performing the functions of the entities listed in the Applicability section of this standard.

R1.2.2. Transmission substations that support the reliable operation of the Bulk Electric System.

R1.2.3. Generation resources that support the reliable operation of the Bulk Electric System.

R1.2.4. Systems and facilities critical to system restoration, including blackstart generators and substations in the electrical path of transmission lines used for initial system restoration.

R1.2.5. Systems and facilities critical to automatic load shedding under a common control system capable of shedding 300 MW or more.

R1.2.6. Special Protection Systems that support the reliable operation of the Bulk Electric System.

R1.2.7. Any additional assets that support the reliable operation of the Bulk Electric System that the Responsible Entity deems appropriate to include in its assessment.

R2. Critical Asset Identification — The Responsible Entity shall develop a list of its identified Critical Assets determined through an annual application of the risk-based assessment methodology required in R1. The Responsible Entity shall review this list at least annually, and update it as necessary.

R3. Critical Cyber Asset Identification — Using the list of Critical Assets developed pursuant to Requirement R2, the Responsible Entity shall develop a list of associated Critical Cyber Assets essential to the operation of the Critical Asset. Examples at control centers and backup control centers include systems and facilities at master and remote sites that provide monitoring and control, automatic generation control, real-time power system modeling, and real-time inter-utility data exchange. The Responsible Entity shall review this list at least annually, and update it as necessary. For the purpose of Standard CIP-002-2, Critical Cyber Assets are further qualified to be those having at least one of the following characteristics:

R3.1. The Cyber Asset uses a routable protocol to communicate outside the Electronic Security Perimeter; or,

R3.2. The Cyber Asset uses a routable protocol within a control center; or,

R3.3. The Cyber Asset is dial-up accessible.

R4. Annual Approval — The senior manager or delegate(s) shall approve annually the risk-based assessment methodology, the list of Critical Assets and the list of Critical Cyber Assets. Based on Requirements R1, R2, and R3 the Responsible Entity may determine that it has no Critical Assets or Critical Cyber Assets. The Responsible Entity shall keep a signed and dated record of the senior manager or delegate(s)'s approval of the risk-based assessment methodology, the list of Critical Assets and the list of Critical Cyber Assets (even if such lists are null.)

C. Measures

M1. The Responsible Entity shall make available its current risk-based assessment methodology documentation as specified in Requirement R1.

M2. The Responsible Entity shall make available its dated list of Critical Assets as specified in Requirement R2.

M3. The Responsible Entity shall make available its dated list of Critical Cyber Assets as specified in Requirement R3.

M4. The Responsible Entity shall make available its dated approval records of annual approvals as specified in Requirement R4.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

1.1.1 Regional Entity for Responsible Entities that do not perform delegated tasks for their Regional Entity.

1.1.2 ERO for Regional Entity.

1.1.3 Third-party monitor without vested interest in the outcome for NERC.

1.2. Compliance Monitoring Period and Reset Time Frame

Not applicable.

1.3. Compliance Monitoring and Enforcement Processes

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints

1.4. Data Retention

1.4.1 The Responsible Entity shall keep documentation required by Standard CIP-002-2 from the previous full calendar year unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

1.4.2 The Compliance Enforcement Authority in conjunction with the Registered Entity shall keep the last audit records and all requested and submitted subsequent audit records.

1.5. Additional Compliance Information

1.5.1 None.

2. Violation Severity Levels (Under Development by the CIP VSL Drafting Team)

E. Regional Variances

None identified.

Version History

Version	Date	Action	Change Tracking
1	01/16/06	R3.2 — Change "Control Center" to "control center"	03/24/06
2		Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	

Standard Development Roadmap

This section is maintained by the drafting team during the development of the standard and will be removed when the standard becomes effective.

Development Steps Completed:

1. The Standards Committee (SC) accepted the Standards Authorization Request (SAR) for Project 2008-06 Cyber Security Order 706 on March 10, 2008.
2. The SAR for Project 2008-06 Cyber Security Order 706 was posted for industry comment March 20–April 19, 2008.
3. Nominations for the SAR drafting team members were solicited March 20–April 4, 2008.
4. The Executive Committee of the SC appointed the SAR drafting team for Project 2008-06 Cyber Security Order 706 on April 25, 2008 and the full SC ratified the Executive Committee's action on May 8.
5. The SC accepted the SAR and approved moving forward with Project 2008-06 Cyber Security Order on July 10, 2008.
6. Nominations for the standard drafting team (SDT) for Project 2008-06 Cyber Security Order 706 were solicited July 15–28, 2008.
7. The Executive Committee of the SC appointed the SDT for Project 2008-06 Cyber Security Order 706 on August 7, 2008.

Proposed Action Plan and Description of Current Draft:

The standard drafting team for Project 2008-06 Cyber Security Order 706 (SDT CSO706) has been assigned the responsibility to review each of the following reliability standards to ensure that they conform to the latest version of the ERO Rules of Procedure, including the Reliability Standards Development Procedure, and also address all of the directed modifications identified in the FERC Order 706:

CIP–002–1 — Cyber Security — Critical Cyber Asset Identification
CIP–003–1 — Cyber Security — Security Management Controls
CIP–004–1 — Cyber Security — Personnel and Training
CIP–005–1 — Cyber Security — Electronic Security Perimeter(s)
CIP–006–1 — Cyber Security — Physical Security
CIP–007–1 — Cyber Security — Systems Security Management
CIP–008–1 — Cyber Security — Incident Reporting and Response Planning
CIP–009–1 — Cyber Security — Recovery Plans for Critical Cyber Assets

Because of the extensive scope of Project 2008-06 Cyber Security Order 706 the SDT CSO706 is implementing a multiphase approach for revising this set of standards.

Phase I of the project includes necessary modifications to CIP-002-1 through CIP-009-1 to comply with the near term specific directives included in FERC Order 706. In particular, the SDT addressed the directive in FERC Order 706 that the "... ERO modify the CIP Reliability Standards through its Reliability Standards development process to remove references to reasonable business judgment before compliance audits begin in 2009." In addition, a number of other directives included in FERC Order 706, which apply to specific standards are also addressed in Phase I. More contentious issues to be addressed

by the SDT associated with the modification of this set of standards will be addressed in a later phase(s) of Project 2008-06 Cyber Security Order 706.

This posting of the cyber standards for industry comment only relates to Phase I of the project. Specifically, SDT CSO706 produced a revised version of Standard CIP–003–2 — Cyber Security – Security Management Controls and is posting the proposed modifications for a 45-day comment period.

Future Development Plan:

Anticipated Actions	Anticipated Date
1. Develop and post reply comments to initial posting of standard for industry comment	January 7–February 17, 2009
2. Post for 30-day pre-ballot period.	February 18–March 31, 2009
3. Conduct initial ballot	April 2–11, 2009
4. Post response to comments on first ballot	April 20–May 12, 2009
5. Conduct recirculation ballot	May 13–22, 2009
6. Board adoption date.	To be determined.

A. Introduction

1. Title: Cyber Security — Security Management Controls

2. Number: CIP-003-2

3. Purpose: Standard CIP-003-2 requires that Responsible Entities have minimum security management controls in place to protect Critical Cyber Assets. Standard CIP-003-2 should be read as part of a group of standards numbered Standards CIP-002-2 through CIP-009-2.

4. Applicability:

4.1. Within the text of Standard CIP-003-2, "Responsible Entity" shall mean:

4.1.1 Reliability Coordinator.

4.1.2 Balancing Authority.

4.1.3 Interchange Authority.

4.1.4 Transmission Service Provider.

4.1.5 Transmission Owner.

4.1.6 Transmission Operator.

4.1.7 Generator Owner.

4.1.8 Generator Operator.

4.1.9 Load Serving Entity.

4.1.10 NERC.

4.1.11 Regional Entity.

4.2. The following are exempt from Standard CIP-003-2:

4.2.1 Facilities regulated by the U.S. Nuclear Regulatory Commission or the Canadian Nuclear Safety Commission.

4.2.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.3 Responsible Entities that, in compliance with Standard CIP-002-2, identify that they have no Critical Cyber Assets shall only be required to comply with CIP-003-2 Requirement R2.

5. Effective Date: The first day of the third calendar quarter after applicable regulatory approvals have been received (or the Reliability Standard otherwise becomes effective the first day of the third calendar quarter after BOT adoption in those jurisdictions where regulatory approval is not required).

B. Requirements

R1. Cyber Security Policy — The Responsible Entity shall document and implement a cyber security policy that represents management's commitment and ability to secure its Critical Cyber Assets. The Responsible Entity shall, at minimum, ensure the following:

R1.1. The cyber security policy addresses the requirements in Standards CIP-002-2 through CIP-009-2, including provision for emergency situations.

R1.2. The cyber security policy is readily available to all personnel who have access to, or are responsible for, Critical Cyber Assets.

R1.3. Annual review and approval of the cyber security policy by the senior manager assigned pursuant to R2.

R2. Leadership — The Responsible Entity shall assign a single senior manager with overall responsibility and authority for leading and managing the entity's implementation of, and adherence to, Standards CIP-002-2 through CIP-009-2.

R2.1. The senior manager shall be identified by name, title, and date of designation.

R2.2. Changes to the senior manager must be documented within thirty calendar days of the effective date.

R2.3. Where allowed by Standards CIP-002-2 through CIP-009-2, the senior manager may delegate authority for specific actions to a named delegate or delegates. These delegations shall be documented in the same manner as R2.1 and R2.2, and approved by the senior manager.

R2.4. The senior manager or delegate(s), shall authorize and document any exception from the requirements of the cyber security policy.

R3. Exceptions — Instances where the Responsible Entity cannot conform to its cyber security policy must be documented as exceptions and authorized by the senior manager or delegate(s).

R3.1. Exceptions to the Responsible Entity's cyber security policy must be documented within thirty days of being approved by the senior manager or delegate(s).

R3.2. Documented exceptions to the cyber security policy must include an explanation as to why the exception is necessary and any compensating measures.

R3.3. Authorized exceptions to the cyber security policy must be reviewed and approved annually by the senior manager or delegate(s) to ensure the exceptions are still required and valid. Such review and approval shall be documented.

R4. Information Protection — The Responsible Entity shall implement and document a program to identify, classify, and protect information associated with Critical Cyber Assets.

R4.1. The Critical Cyber Asset information to be protected shall include, at a minimum and regardless of media type, operational procedures, lists as required in Standard CIP-002-2, network topology or similar diagrams, floor plans of computing centers that contain Critical Cyber Assets, equipment layouts of Critical Cyber Assets, disaster recovery plans, incident response plans, and security configuration information.

R4.2. The Responsible Entity shall classify information to be protected under this program based on the sensitivity of the Critical Cyber Asset information.

R4.3. The Responsible Entity shall, at least annually, assess adherence to its Critical Cyber Asset information protection program, document the assessment results, and implement an action plan to remediate deficiencies identified during the assessment.

R5. Access Control — The Responsible Entity shall document and implement a program for managing access to protected Critical Cyber Asset information.

R5.1. The Responsible Entity shall maintain a list of designated personnel who are responsible for authorizing logical or physical access to protected information.

R5.1.1. Personnel shall be identified by name, title, ~~business phone~~ and the information for which they are responsible for authorizing access.

R5.1.2. The list of personnel responsible for authorizing access to protected information shall be verified at least annually.

R5.2. The Responsible Entity shall review at least annually the access privileges to protected information to confirm that access privileges are correct and that they correspond with the Responsible Entity's needs and appropriate personnel roles and responsibilities.

R5.3. The Responsible Entity shall assess and document at least annually the processes for controlling access privileges to protected information.

R6. Change Control and Configuration Management — The Responsible Entity shall establish and document a process of change control and configuration management for adding, modifying, replacing, or removing Critical Cyber Asset hardware or software, and implement supporting configuration management activities to identify, control and document all entity or vendor-related changes to hardware and software components of Critical Cyber Assets pursuant to the change control process.

C. Measures

M1. The Responsible Entity shall make available documentation of its cyber security policy as specified in Requirement R1. Additionally, the Responsible Entity shall demonstrate that the cyber security policy is available as specified in Requirement R1.2.

M2. The Responsible Entity shall make available documentation of the assignment of, and changes to, its leadership as specified in Requirement R2.

M3. The Responsible Entity shall make available documentation of the exceptions, as specified in Requirement R3.

M4. The Responsible Entity shall make available documentation of its information protection program as specified in Requirement R4.

M5. The Responsible Entity shall make available its access control documentation as specified in Requirement R5.

M6. The Responsible Entity shall make available its change control and configuration management documentation as specified in Requirement R6.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

1.1.1 Regional Entity for Responsible Entities that do not perform delegated tasks for their Regional Entity.

1.1.2 ERO for Regional Entity.

1.1.3 Third-party monitor without vested interest in the outcome for NERC.

1.2. Compliance Monitoring Period and Reset Time Frame

Not applicable.

1.3. Compliance Monitoring and Enforcement Processes

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints

1.4. Data Retention

1.4.1 The Responsible Entity shall keep all documentation and records from the previous full calendar year unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

1.4.2 The Compliance Enforcement Authority in conjunction with the Registered Entity shall keep the last audit records and all requested and submitted subsequent audit records.

1.5. Additional Compliance Information

1.5.1 None

2. Violation Severity Levels (Under Development by the CIP VSL Drafting Team)

E. Regional Variances

None identified.

Version History

Version	Date	Action	Change Tracking
2		Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Requirement R2 applies to all Responsible Entities, including Responsible Entities which have no Critical Cyber Assets. Changed compliance monitor to Compliance Enforcement Authority.	
	04 Feb 2009	Modifications to clarify the requirements and to incorporate industry comments. Section 1.5: Additional Compliance Information, added “None” Modified the personnel identification information requirements in R5.1.1 to include name, title, and the information for which they are responsible for authorizing	

		access (removed the business phone information).	

Standard Development Roadmap

This section is maintained by the drafting team during the development of the standard and will be removed when the standard becomes effective.

Development Steps Completed:

1. The Standards Committee (SC) accepted the Standards Authorization Request (SAR) for Project 2008-06 Cyber Security Order 706 on March 10, 2008.
2. The SAR for Project 2008-06 Cyber Security Order 706 was posted for industry comment March 20–April 19, 2008.
3. Nominations for the SAR drafting team members were solicited March 20–April 4, 2008.
4. The Executive Committee of the SC appointed the SAR drafting team for Project 2008-06 Cyber Security Order 706 on April 25, 2008 and the full SC ratified the Executive Committee's action on May 8.
5. The SC accepted the SAR and approved moving forward with Project 2008-06 Cyber Security Order on July 10, 2008.
6. Nominations for the standard drafting team (SDT) for Project 2008-06 Cyber Security Order 706 were solicited July 15–28, 2008.
7. The Executive Committee of the SC appointed the SDT for Project 2008-06 Cyber Security Order 706 on August 7, 2008.

Proposed Action Plan and Description of Current Draft:

The standard drafting team for Project 2008-06 Cyber Security Order 706 (SDT CSO706) has been assigned the responsibility to review each of the following reliability standards to ensure that they conform to the latest version of the ERO Rules of Procedure, including the Reliability Standards Development Procedure, and also address all of the directed modifications identified in the FERC Order 706:

CIP–002–1 — Cyber Security — Critical Cyber Asset Identification
CIP–003–1 — Cyber Security — Security Management Controls
CIP–004–1 — Cyber Security — Personnel and Training
CIP–005–1 — Cyber Security — Electronic Security Perimeter(s)
CIP–006–1 — Cyber Security — Physical Security
CIP–007–1 — Cyber Security — Systems Security Management
CIP–008–1 — Cyber Security — Incident Reporting and Response Planning
CIP–009–1 — Cyber Security — Recovery Plans for Critical Cyber Assets

Because of the extensive scope of Project 2008-06 Cyber Security Order 706 the SDT CSO706 is implementing a multiphase approach for revising this set of standards.

Phase I of the project includes necessary modifications to CIP-002-1 through CIP-009-1 to comply with the near term specific directives included in FERC Order 706. In particular, the SDT addressed the directive in FERC Order 706 that the "... ERO modify the CIP Reliability Standards through its Reliability Standards development process to remove references to reasonable business judgment before compliance audits begin in 2009." In addition, a number of other directives included in FERC Order 706, which apply to specific standards are also addressed in Phase I. More contentious issues to be addressed by the SDT associated with the modification of this set of standards will be addressed in a later phase(s) of Project 2008-06 Cyber Security Order 706.

This posting of the cyber standards for industry comment only relates to Phase I of the project. Specifically, SDT CSO706 produced a revised version of Standard CIP–002–4 — Cyber Security — Personnel and Training and is posting the proposed modifications for a 45-day comment period.

Future Development Plan:

Anticipated Actions	Anticipated Date
1. Develop and post reply comments to initial posting of standard for industry comment	January 7–February 17, 2009
2. Post for 30-day pre-ballot period.	February 18–March 31, 2009
3. Conduct initial ballot	April 2–11, 2009
4. Post response to comments on first ballot	April 20–May 12, 2009
5. Conduct recirculation ballot	May 13–22, 2009
6. Board adoption date.	To be determined.

A. Introduction

1. **Title:** Cyber Security — Personnel & Training

2. **Number:** CIP-004-2

3. **Purpose:** Standard CIP-004-2 requires that personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets, including contractors and service vendors, have an appropriate level of personnel risk assessment, training, and security awareness. Standard CIP-004-2 should be read as part of a group of standards numbered Standards CIP-002-2 through CIP-009-2.

4. **Applicability:**

   4.1. Within the text of Standard CIP-004-2, "Responsible Entity" shall mean:

   4.1.1 Reliability Coordinator.

   4.1.2 Balancing Authority.

   4.1.3 Interchange Authority.

   4.1.4 Transmission Service Provider.

   4.1.5 Transmission Owner.

   4.1.6 Transmission Operator.

   4.1.7 Generator Owner.

   4.1.8 Generator Operator.

   4.1.9 Load Serving Entity.

   4.1.10 NERC.

   4.1.11 Regional Entity.

   4.2. The following are exempt from Standard CIP-004-2:

   4.2.1 Facilities regulated by the U.S. Nuclear Regulatory Commission or the Canadian Nuclear Safety Commission.

   4.2.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

   4.2.3 Responsible Entities that, in compliance with Standard CIP-002-2, identify that they have no Critical Cyber Assets.

5. **Effective Date:** The first day of the third calendar quarter after applicable regulatory approvals have been received (or the Reliability Standard otherwise becomes effective the first day of the third calendar quarter after BOT adoption in those jurisdictions where regulatory approval is not required).

B. Requirements

R1. Awareness — The Responsible Entity shall establish, document, implement, and ~~,~~ maintain, ~~document and implement~~ a security awareness program to ensure personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets receive on-going reinforcement in sound security practices. The program shall include security awareness reinforcement on at least a quarterly basis using mechanisms such as:

- Direct communications (e.g., emails, memos, computer based training, etc.);
- Indirect communications (e.g., posters, intranet, brochures, etc.);

- Management support and reinforcement (e.g., presentations, meetings, etc.).

R2. Training — The Responsible Entity shall establish, document, implement, and maintain, ~~document and implement~~ an annual cyber security training program for personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets. The cyber security training program shall be reviewed annually, at a minimum, ~~reviewed~~ and shall be updated ~~as~~ whenever necessary.

R2.1. This program will ensure that all personnel having such access to Critical Cyber Assets, including contractors and service vendors, are trained prior to their being granted such access except in specified circumstances such as an emergency.

R2.2. Training shall cover the policies, access controls, and procedures as developed for the Critical Cyber Assets covered by CIP-004-2, and include, at a minimum, the following required items appropriate to personnel roles and responsibilities:

R2.2.1. The proper use of Critical Cyber Assets;

R2.2.2. Physical and electronic access controls to Critical Cyber Assets;

R2.2.3. The proper handling of Critical Cyber Asset information; and,

R2.2.4. Action plans and procedures to recover or re-establish Critical Cyber Assets and access thereto following a Cyber Security Incident.

R2.3. The Responsible Entity shall maintain documentation that training is conducted at least annually, including the date the training was completed and attendance records.

R3. Personnel Risk Assessment —The Responsible Entity shall have a documented personnel risk assessment program, in accordance with federal, state, provincial, and local laws, and subject to existing collective bargaining unit agreements, for personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets. A personnel risk assessment shall be conducted pursuant to that program prior to such personnel being granted such access except in specified circumstances such as an emergency.

The personnel risk assessment program shall at a minimum include:

R3.1. The Responsible Entity shall ensure that each assessment conducted include, at least, identity verification (e.g., Social Security Number verification in the U.S.) and seven-year criminal check. The Responsible Entity may conduct more detailed reviews, as permitted by law and subject to existing collective bargaining unit agreements, depending upon the criticality of the position.

R3.2. The Responsible Entity shall update each personnel risk assessment at least every seven years after the initial personnel risk assessment or for cause.

R3.3. The Responsible Entity shall document the results of personnel risk assessments of its personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets, and that personnel risk assessments of contractor and service vendor personnel with such access are conducted pursuant to Standard CIP-004-2.

R4. Access — The Responsible Entity shall maintain list(s) of personnel with authorized cyber or authorized unescorted physical access to Critical Cyber Assets, including their specific electronic and physical access rights to Critical Cyber Assets.

R4.1. The Responsible Entity shall review the list(s) of its personnel who have such access to Critical Cyber Assets quarterly, and update the list(s) within seven calendar days of any change of personnel with such access to Critical Cyber Assets, or any change in the access rights of such personnel. The Responsible Entity shall ensure access list(s) for contractors and service vendors are properly maintained.

R4.2. The Responsible Entity shall revoke such access to Critical Cyber Assets within 24 hours for personnel terminated for cause and within seven calendar days for personnel who no longer require such access to Critical Cyber Assets.

C. Measures

M1. The Responsible Entity shall make available documentation of its security awareness and reinforcement program as specified in Requirement R1.

M2. The Responsible Entity shall make available documentation of its cyber security training program, review, and records as specified in Requirement R2.

M3. The Responsible Entity shall make available documentation of the personnel risk assessment program and that personnel risk assessments have been applied to all personnel who have authorized cyber or authorized unescorted physical access to Critical Cyber Assets, as specified in Requirement R3.

M4. The Responsible Entity shall make available documentation of the list(s), list review and update, and access revocation as needed as specified in Requirement R4.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

1.1.1 Regional Entity for Responsible Entities that do not perform delegated tasks for their Regional Entity.

1.1.2 ERO for Regional Entity.

1.1.3 Third-party monitor without vested interest in the outcome for NERC.

1.2. Compliance Monitoring Period and Reset Time Frame

Not Applicable.

1.3. Compliance Monitoring and Enforcement Processes

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints

1.4. Data Retention

1.4.1 The Responsible Entity shall keep personnel risk assessment documents in accordance with federal, state, provincial, and local laws.

1.4.2 The Responsible Entity shall keep all other documentation required by Standard CIP-004-2 from the previous full calendar year unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

1.4.3 The Compliance Enforcement Authority in conjunction with the Registered Entity shall keep the last audit records and all requested and submitted subsequent audit records.

1.5. Additional Compliance Information

2. Violation Severity Levels (Under Development by the CIP VSL Drafting Team)

E. Regional Variances

None identified.

Version History

Version	Date	Action	Change Tracking
1	01/16/06	D.2.2.4 — Insert the phrase "for cause" as intended. "One instance of personnel termination for cause…"	03/24/06
1	06/01/06	D.2.1.4 — Change "access control rights" to "access rights."	06/05/06
2		Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Reference to emergency situations. Removal of 90 day window to complete training and personnel risk assessments. Changed compliance monitor to Compliance Enforcement Authority.	
	4 Feb 2009	Modifications to clarify the requirements and to incorporate industry comments. Modification to R1 for the awareness and training program to establish, document, implement, and maintain**.** Modification to R2 stating the requirements for the cyber security training program. Modification to R3 Personnel Risk Assessment to clarify that it pertains to personnel having authorized cyber or authorized unescorted physical access to "Critical Cyber Assets".	

Standard Development Roadmap

This section is maintained by the drafting team during the development of the standard and will be removed when the standard becomes effective.

Development Steps Completed:

1. The Standards Committee (SC) accepted the Standards Authorization Request (SAR) for Project 2008-06 Cyber Security Order 706 on March 10, 2008.
2. The SAR for Project 2008-06 Cyber Security Order 706 was posted for industry comment March 20–April 19, 2008.
3. Nominations for the SAR drafting team members were solicited March 20–April 4, 2008.
4. The Executive Committee of the SC appointed the SAR drafting team for Project 2008-06 Cyber Security Order 706 on April 25, 2008 and the full SC ratified the Executive Committee's action on May 8.
5. The SC accepted the SAR and approved moving forward with Project 2008-06 Cyber Security Order on July 10, 2008.
6. Nominations for the standard drafting team (SDT) for Project 2008-06 Cyber Security Order 706 were solicited July 15–28, 2008.
7. The Executive Committee of the SC appointed the SDT for Project 2008-06 Cyber Security Order 706 on August 7, 2008.

Proposed Action Plan and Description of Current Draft:

The standard drafting team for Project 2008-06 Cyber Security Order 706 (SDT CSO706) has been assigned the responsibility to review each of the following reliability standards to ensure that they conform to the latest version of the ERO Rules of Procedure, including the Reliability Standards Development Procedure, and also address all of the directed modifications identified in the FERC Order 706:

CIP–002–1 — Cyber Security — Critical Cyber Asset Identification
CIP–003–1 — Cyber Security — Security Management Controls
CIP–004–1 — Cyber Security — Personnel and Training
CIP–005–1 — Cyber Security — Electronic Security Perimeter(s)
CIP–006–1 — Cyber Security — Physical Security
CIP–007–1 — Cyber Security — Systems Security Management
CIP–008–1 — Cyber Security — Incident Reporting and Response Planning
CIP–009–1 — Cyber Security — Recovery Plans for Critical Cyber Assets

Because of the extensive scope of Project 2008-06 Cyber Security Order 706 the SDT CSO706 is implementing a multiphase approach for revising this set of standards.

Phase I of the project includes necessary modifications to CIP-002-1 through CIP-009-1 to comply with the near term specific directives included in FERC Order 706. In particular, the SDT addressed the directive in FERC Order 706 that the "... ERO modify the CIP Reliability Standards through its Reliability Standards development process to remove references to reasonable business judgment before compliance audits begin in 2009." In addition, a number of other directives included in FERC Order 706, which apply to specific standards are also addressed in Phase I. More contentious issues to be addressed by the SDT associated with the modification of this set of standards will be addressed in a later phase(s) of Project 2008-06 Cyber Security Order 706.

This posting of the cyber standards for industry comment only relates to Phase I of the project. Specifically, SDT CSO706 produced a revised version of Standard CIP–005–2 — Cyber Security — Electronic Security Perimeter(s) and is posting the proposed modifications for a 45-day comment period.

Future Development Plan:

Anticipated Actions	Anticipated Date
1. Develop and post reply comments to initial posting of standard for industry comment	January 7–February 17, 2009
2. Post for 30-day pre-ballot period.	February 18–March 31, 2009
3. Conduct initial ballot	April 2–11, 2009
4. Post response to comments on first ballot	April 20–May 12, 2009
5. Conduct recirculation ballot	May 13–22, 2009
6. Board adoption date.	To be determined.

A. Introduction

1. Title: Cyber Security — Electronic Security Perimeter(s)

2. Number: CIP-005-2

3. Purpose: Standard CIP-005-2 requires the identification and protection of the Electronic Security Perimeter(s) inside which all Critical Cyber Assets reside, as well as all access points on the perimeter. Standard CIP-005-2 should be read as part of a group of standards numbered Standards CIP-002-2 through CIP-009-2.

4. Applicability

4.1. Within the text of Standard CIP-005-2, "Responsible Entity" shall mean:

4.1.1 Reliability Coordinator.

4.1.2 Balancing Authority.

4.1.3 Interchange Authority.

4.1.4 Transmission Service Provider.

4.1.5 Transmission Owner.

4.1.6 Transmission Operator.

4.1.7 Generator Owner.

4.1.8 Generator Operator.

4.1.9 Load Serving Entity.

4.1.10 NERC.

4.1.11 Regional Entity

4.2. The following are exempt from Standard CIP-005-2:

4.2.1 Facilities regulated by the U.S. Nuclear Regulatory Commission or the Canadian Nuclear Safety Commission.

4.2.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.3 Responsible Entities that, in compliance with Standard CIP-002-2, identify that they have no Critical Cyber Assets.

5. Effective Date: The first day of the third calendar quarter after applicable regulatory approvals have been received (or the Reliability Standard otherwise becomes effective in those jurisdictions where regulatory approval is not required).

B. Requirements

R1. Electronic Security Perimeter — The Responsible Entity shall ensure that every Critical Cyber Asset resides within an Electronic Security Perimeter. The Responsible Entity shall identify and document the Electronic Security Perimeter(s) and all access points to the perimeter(s).

R1.1. Access points to the Electronic Security Perimeter(s) shall include any externally connected communication end point (for example, dial-up modems) terminating at any device within the Electronic Security Perimeter(s).

R1.2. For a dial-up accessible Critical Cyber Asset that uses a non-routable protocol, the Responsible Entity shall define an Electronic Security Perimeter for that single access point at the dial-up device.

R1.3. Communication links connecting discrete Electronic Security Perimeters shall not be considered part of the Electronic Security Perimeter. However, end points of these communication links within the Electronic Security Perimeter(s) shall be considered access points to the Electronic Security Perimeter(s).

R1.4. Any non-critical Cyber Asset within a defined Electronic Security Perimeter shall be identified and protected pursuant to the requirements of Standard CIP-005-2.

R1.5. Cyber Assets used in the access control and/or monitoring of the Electronic Security Perimeter(s) shall be afforded the protective measures as a specified in Standard CIP-003-2; Standard CIP-004-2 Requirement R3; Standard CIP-005-2 Requirements R2 and R3; Standard CIP-006-2 Requirement R3; Standard CIP-007-2 Requirements R1 and R3 through R9; Standard CIP-008-2; and Standard CIP-009-2.

R1.6. The Responsible Entity shall maintain documentation of Electronic Security Perimeter(s), all interconnected Critical and non-critical Cyber Assets within the Electronic Security Perimeter(s), all electronic access points to the Electronic Security Perimeter(s) and the Cyber Assets deployed for the access control and monitoring of these access points.

R2. Electronic Access Controls — The Responsible Entity shall implement and document the organizational processes and technical and procedural mechanisms for control of electronic access at all electronic access points to the Electronic Security Perimeter(s).

R2.1. These processes and mechanisms shall use an access control model that denies access by default, such that explicit access permissions must be specified.

R2.2. At all access points to the Electronic Security Perimeter(s), the Responsible Entity shall enable only ports and services required for operations and for monitoring Cyber Assets within the Electronic Security Perimeter, and shall document, individually or by specified grouping, the configuration of those ports and services.

R2.3. The Responsible Entity shall implement and maintain ~~and implement~~ a procedure for securing dial-up access to the Electronic Security Perimeter(s).

R2.4. Where external interactive access into the Electronic Security Perimeter has been enabled, the Responsible Entity shall implement strong procedural or technical controls at the access points to ensure authenticity of the accessing party, where technically feasible.

R2.5. The required documentation shall, at least, identify and describe:

R2.5.1. The processes for access request and authorization.

R2.5.2. The authentication methods.

R2.5.3. The review process for authorization rights, in accordance with Standard CIP-004-2 Requirement R4.

R2.5.4. The controls used to secure dial-up accessible connections.

R2.6. Appropriate Use Banner — Where technically feasible, electronic access control devices shall display an appropriate use banner on the user screen upon all interactive access attempts. The Responsible Entity shall maintain a document identifying the content of the banner.

R3. Monitoring Electronic Access — The Responsible Entity shall implement and document an electronic or manual process(es) for monitoring and logging access at access points to the Electronic Security Perimeter(s) twenty-four hours a day, seven days a week.

R3.1. For dial-up accessible Critical Cyber Assets that use non-routable protocols, the Responsible Entity shall implement and document monitoring process(es) at each access point to the dial-up device, where technically feasible.

R3.2. Where technically feasible, the security monitoring process(es) shall detect and alert for attempts at or actual unauthorized accesses. These alerts shall provide for appropriate notification to designated response personnel. Where alerting is not technically feasible, the Responsible Entity shall review or otherwise assess access logs for attempts at or actual unauthorized accesses at least every ninety calendar days.

R4. Cyber Vulnerability Assessment — The Responsible Entity shall perform a cyber vulnerability assessment of the electronic access points to the Electronic Security Perimeter(s) at least annually. The vulnerability assessment shall include, at a minimum, the following:

R4.1. A document identifying the vulnerability assessment process;

R4.2. A review to verify that only ports and services required for operations at these access points are enabled;

R4.3. The discovery of all access points to the Electronic Security Perimeter;

R4.4. A review of controls for default accounts, passwords, and network management community strings;

R4.5. Documentation of the results of the assessment, the action plan to remediate or mitigate vulnerabilities identified in the assessment, and the execution status of that action plan.

R5. Documentation Review and Maintenance — The Responsible Entity shall review, update, and maintain all documentation to support compliance with the requirements of Standard CIP-005-2.

R5.1. The Responsible Entity shall ensure that all documentation required by Standard CIP-005-2 reflect current configurations and processes and shall review the documents and procedures referenced in Standard CIP-005-2 at least annually.

R5.2. The Responsible Entity shall update the documentation to reflect the modification of the network or controls within ninety calendar days of the change.

R5.3. The Responsible Entity shall retain electronic access logs for at least ninety calendar days. Logs related to reportable incidents shall be kept in accordance with the requirements of Standard CIP-008-2.

C. Measures

M1. The Responsible Entity shall make available ~~dated documents~~ documentation about the Electronic Security Perimeter as specified in Requirement R1.

M2. The Responsible Entity shall make available ~~dated~~ documentation of the electronic access controls to the Electronic Security Perimeter(s), as specified in Requirement R2.

M3. The Responsible Entity shall make available ~~dated~~ documentation of controls implemented to log and monitor access to the Electronic Security Perimeter(s) as specified in Requirement R3.

M4. The Responsible Entity shall make available ~~dated~~ documentation of its annual vulnerability assessment as specified in Requirement R4.

M5. The Responsible Entity shall make available ~~dated~~ access logs and documentation of review, changes, and log retention as specified in Requirement R5.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

1.1.1 Regional Entity for Responsible Entities that do not perform delegated tasks for their Regional Entity.

1.1.2 ERO for Regional Entity.

1.1.3 Third-party monitor without vested interest in the outcome for NERC.

1.2. Compliance Monitoring Period and Reset Time Frame

Not applicable.

1.3. Compliance Monitoring and Enforcement Processes

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints

1.4. Data Retention

1.4.1 The Responsible Entity shall keep logs for a minimum of ninety calendar days, unless: a) longer retention is required pursuant to Standard CIP-008-2, Requirement R2; b) directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

1.4.2 The Responsible Entity shall keep other documents and records required by Standard CIP-005-2 from the previous full calendar year.

1.4.3 The Compliance Enforcement Authority in conjunction with the Registered Entity shall keep the last audit records and all requested and submitted subsequent audit records.

1.5. Additional Compliance Information

2. Violation Severity Levels (Under Development by the CIP VSL Drafting Team)

E. Regional Variances

None identified.

Version History

Version	Date	Action	Change Tracking
1	01/16/06	D.2.3.1 — Change “Critical Assets,” to “Critical Cyber Assets” as intended.	03/24/06
2		Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity.	

		Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
		Modifications to clarify the requirements and to incorporate industry comments. Revised the wording of the Electronic Access Controls requirement stated in R2.3 to clarify that the Responsible Entity shall "implement and maintain" a procedure for securing dial-up access to the Electronic Security Perimeter(s). Deleted the word "dated" from the Measures.	

Standard Development Roadmap

This section is maintained by the drafting team during the development of the standard and will be removed when the standard becomes effective.

Development Steps Completed:

1. The Standards Committee (SC) accepted the Standards Authorization Request (SAR) for Project 2008-06 Cyber Security Order 706 on March 10, 2008.
2. The SAR for Project 2008-06 Cyber Security Order 706 was posted for industry comment March 20–April 19, 2008.
3. Nominations for the SAR drafting team members were solicited March 20–April 4, 2008.
4. The Executive Committee of the SC appointed the SAR drafting team for Project 2008-06 Cyber Security Order 706 on April 25, 2008 and the full SC ratified the Executive Committee's action on May 8.
5. The SC accepted the SAR and approved moving forward with Project 2008-06 Cyber Security Order on July 10, 2008.
6. Nominations for the standard drafting team (SDT) for Project 2008-06 Cyber Security Order 706 were solicited July 15–28, 2008.
7. The Executive Committee of the SC appointed the SDT for Project 2008-06 Cyber Security Order 706 on August 7, 2008.

Proposed Action Plan and Description of Current Draft:

The standard drafting team for Project 2008-06 Cyber Security Order 706 (SDT CSO706) has been assigned the responsibility to review each of the following reliability standards to ensure that they conform to the latest version of the ERO Rules of Procedure, including the Reliability Standards Development Procedure, and also address all of the directed modifications identified in the FERC Order 706:

CIP–002–1 — Cyber Security — Critical Cyber Asset Identification
CIP–003–1 — Cyber Security — Security Management Controls
CIP–004–1 — Cyber Security — Personnel and Training
CIP–005–1 — Cyber Security — Electronic Security Perimeter(s)
CIP–006–1 — Cyber Security — Physical Security
CIP–007–1 — Cyber Security — Systems Security Management
CIP–008–1 — Cyber Security — Incident Reporting and Response Planning
CIP–009–1 — Cyber Security — Recovery Plans for Critical Cyber Assets

Because of the extensive scope of Project 2008-06 Cyber Security Order 706 the SDT CSO706 is implementing a multiphase approach for revising this set of standards.

Phase I of the project includes necessary modifications to CIP-002-1 through CIP-009-1 to comply with the near term specific directives included in FERC Order 706. In particular, the SDT addressed the directive in FERC Order 706 that the "... ERO modify the CIP Reliability Standards through its Reliability Standards development process to remove references to reasonable business judgment before compliance audits begin in 2009." In addition, a number of other directives included in FERC Order 706, which apply to specific standards are also addressed in Phase I. More contentious issues to be addressed by the SDT associated with the modification of this set of standards will be addressed in a later phase(s) of Project 2008-06 Cyber Security Order 706.

This posting of the cyber standards for industry comment only relates to Phase I of the project. Specifically, SDT CSO706 produced a revised version of Standard CIP–006–2 — Cyber Security — Physical Security and is posting the proposed modifications for a 45-day comment period.

Future Development Plan:

Anticipated Actions	Anticipated Date
1. Develop and post reply comments to initial posting of standard for industry comment	January 7–February 17, 2009
2. Post for 30-day pre-ballot period.	February 18–March 31, 2009
3. Conduct initial ballot	April 2–11, 2009
4. Post response to comments on first ballot	April 20–May 12, 2009
5. Conduct recirculation ballot	May 13–22, 2009
6. Board adoption date.	To be determined.

A. Introduction

1. **Title:** Cyber Security — Physical Security of Critical Cyber Assets

2. **Number:** CIP-006-2

3. **Purpose:** Standard CIP-006-2 is intended to ensure the implementation of a physical security program for the protection of Critical Cyber Assets. Standard CIP-006-2 should be read as part of a group of standards numbered Standards CIP-002-2 through CIP-009-2.

4. **Applicability:**

   4.1. Within the text of Standard CIP-006-2, "Responsible Entity" shall mean:

   4.1.1 Reliability Coordinator.

   4.1.2 Balancing Authority.

   4.1.3 Interchange Authority.

   4.1.4 Transmission Service Provider.

   4.1.5 Transmission Owner.

   4.1.6 Transmission Operator.

   4.1.7 Generator Owner.

   4.1.8 Generator Operator.

   4.1.9 Load Serving Entity.

   4.1.10 NERC.

   4.1.11 Regional Entity.

   4.2. The following are exempt from Standard CIP-006-2:

   4.2.1 Facilities regulated by the U.S. Nuclear Regulatory Commission or the Canadian Nuclear Safety Commission.

   4.2.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

   4.2.3 Responsible Entities that, in compliance with Standard CIP-002-2, identify that they have no Critical Cyber Assets.

5. **Effective Date:** The first day of the third calendar quarter after applicable regulatory approvals have been received (or the Reliability Standard otherwise becomes effective the first day of the third calendar quarter after BOT adoption in those jurisdictions where regulatory approval is not required).

B. Requirements

R1. Physical Security Plan — The Responsible Entity shall document, implement, and maintain~~, and implement~~ a physical security plan, approved by the senior manager or delegate(s) that shall address, at a minimum, the following:

R1.1. All Cyber Assets within an Electronic Security Perimeter shall reside within an identified Physical Security Perimeter. Where a completely enclosed ("six-wall") border cannot be established, the Responsible Entity shall deploy and document alternative measures to control physical access to such Cyber Assets.

R1.2. Identification of all access points through each Physical Security Perimeter and measures to control entry at those access points.

R1.3. Processes, tools, and procedures to monitor physical access to the perimeter(s).

R1.4. Appropriate use of physical access controls as described in Requirement ~~R3~~ R4 including visitor pass management, response to loss, and prohibition of inappropriate use of physical access controls.

R1.5. Review of access authorization requests and revocation of access authorization, in accordance with CIP-004-2 Requirement R4.

R1.6. Continuous escorted access within the Physical Security Perimeter of personnel not authorized for unescorted access.

R1.7. Update of the physical security plan within thirty calendar days of the completion of any physical security system redesign or reconfiguration, including, but not limited to, addition or removal of access points through the Physical Security Perimeter, physical access controls, monitoring controls, or logging controls.

R1.8. Annual review of the physical security plan.

R2. Protection of Physical Access Control Systems — Cyber Assets that authorize and/or log access to the Physical Security Perimeter(s), exclusive of hardware at the Physical Security Perimeter access point such as electronic lock control mechanisms and badge readers, shall:

R2.1. Be protected from unauthorized physical access.

R2.2. Be afforded the protective measures specified in Standard CIP-003-2; Standard CIP-004-2 Requirement R3; Standard CIP-005-2 Requirements R2 and R3; Standard CIP-006-2 Requirements R4 and R5; Standard CIP-007-2; Standard CIP-008-2; and Standard CIP-009-2.

R3. Protection of Electronic Access Control Systems — Cyber Assets used in the access control and/or monitoring of the Electronic Security Perimeter(s) shall reside within an identified Physical Security Perimeter.

R4. Physical Access Controls — The Responsible Entity shall document and implement the operational and procedural controls to manage physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week. The Responsible Entity shall implement one or more of the following physical access methods:

- Card Key: A means of electronic access where the access rights of the card holder are predefined in a computer database. Access rights may differ from one perimeter to another.
- Special Locks: These include, but are not limited to, locks with "restricted key" systems, magnetic locks that can be operated remotely, and "man-trap" systems.
- Security Personnel: Personnel responsible for controlling physical access who may reside on-site or at a monitoring station.
- Other Authentication Devices: Biometric, keypad, token, or other equivalent devices that control physical access to the Critical Cyber Assets.

R5. Monitoring Physical Access — The Responsible Entity shall document and implement the technical and procedural controls for monitoring physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week. Unauthorized access attempts shall be reviewed immediately and handled in accordance with the procedures specified in Requirement CIP-008-2. One or more of the following monitoring methods shall be used:

- Alarm Systems: Systems that alarm to indicate a door, gate or window has been opened without authorization. These alarms must provide for immediate notification to personnel responsible for response.
- Human Observation of Access Points: Monitoring of physical access points by authorized personnel as specified in Requirement R4.

R6. Logging Physical Access — Logging shall record sufficient information to uniquely identify individuals and the time of access twenty-four hours a day, seven days a week. The Responsible Entity shall implement and document the technical and procedural mechanisms for logging physical entry at all access points to the Physical Security Perimeter(s) using one or more of the following logging methods or their equivalent:

- Computerized Logging: Electronic logs produced by the Responsible Entity's selected access control and monitoring method.
- Video Recording: Electronic capture of video images of sufficient quality to determine identity.
- Manual Logging: A log book or sign-in sheet, or other record of physical access maintained by security or other personnel authorized to control and monitor physical access as specified in Requirement R4.

R7. Access Log Retention — The responsible entity shall retain physical access logs for at least ninety calendar days. Logs related to reportable incidents shall be kept in accordance with the requirements of Standard CIP-008-2.

R8. Maintenance and Testing — The Responsible Entity shall implement a maintenance and testing program to ensure that all physical security systems under Requirements R4, R5, and R6 function properly. The program must include, at a minimum, the following:

R8.1. Testing and maintenance of all physical security mechanisms on a cycle no longer than three years.

R8.2. Retention of testing and maintenance records for the cycle determined by the Responsible Entity in Requirement R8.1.

R8.3. Retention of outage records regarding access controls, logging, and monitoring for a minimum of one calendar year.

C. Measures

M1. The Responsible Entity shall make available the physical security plan as specified in Requirement R1 and documentation of the implementation, review and updating of the plan.

M2. The Responsible Entity shall make available documentation that the physical access control systems are protected as specified in Requirement R2.

M3. The Responsible Entity shall make available documentation that the electronic access control systems are located within an identified Physical Security Perimeter as specified in Requirement R3.

M4. The Responsible Entity shall make available documentation identifying the methods for controlling physical access to each access point of a Physical Security Perimeter as specified in Requirement R4.

M5. The Responsible Entity shall make available documentation identifying the methods for monitoring physical access as specified in Requirement R5.

M6. The Responsible Entity shall make available documentation identifying the methods for logging physical access as specified in Requirement R6.

M7. The Responsible Entity shall make available documentation to show retention of access logs as specified in Requirement R7.

M8. The Responsible Entity shall make available documentation to show its implementation of a physical security system maintenance and testing program as specified in Requirement R8.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

1.1.1 Regional Entity for Responsible Entities that do not perform delegated tasks for their Regional Entity.

1.1.2 ERO for Regional Entities.

1.1.3 Third-party monitor without vested interest in the outcome for NERC.

1.2. Compliance Monitoring Period and Reset Time Frame

Not applicable.

1.3. Compliance Monitoring and Enforcement Processes

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints

1.4. Data Retention

1.4.1 The Responsible Entity shall keep documents other than those specified in Requirements R7 and R8.2 from the previous full calendar year unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation..

1.4.2 The Compliance Enforcement Authority in conjunction with the Registered Entity shall keep the last audit records and all requested and submitted subsequent audit records.

1.5. Additional Compliance Information

1.5.1 The Responsible Entity may not make exceptions in its cyber security policy to the creation, documentation, or maintenance of a physical security plan.

1.5.2 For dial-up accessible Critical Cyber Assets that use non-routable protocols, the Responsible Entity shall not be required to comply with Standard CIP-006-2 for that single access point at the dial-up device.

2. Violation Severity Levels (Under development by the CIP VSL Drafting Team)

E. Regional Variances

None identified.

Version History

Version	Date	Action	Change Tracking
2		Modifications to remove extraneous information from the requirements, improve readability, and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Replaced the RRO with RE as a responsible entity. Modified CIP-006-1 Requirement R1 to clarify that a physical security plan to protect Critical Cyber Assets must be documented, maintained, implemented and approved by the senior manager. Added Requirement R2 to CIP-006-2 to clarify the requirement to safeguard the Physical Access Control Systems and exclude hardware at the Physical Security Perimeter access point, such as electronic lock control mechanisms and badge readers from the requirement. Requirement R2.1 requires the Responsible Entity to protect the Physical Access Control Systems from unauthorized access. CIP-006-1 Requirement R1.8 was moved to become CIP-006-2 Requirement R2.2. Added Requirement R3 to CIP-006-2, clarifying the requirement for Electronic Access Control Systems to be safeguarded within an identified Physical Security Perimeter. The sub requirements of CIP-006-2 Requirements R4, R5, and R6 were changed from formal requirements to bulleted lists of options consistent with the intent of the requirements. Changed the Compliance Monitor to Compliance Enforcement Authority.	
		Modifications to clarify the requirements and to incorporate industry comments. Modify Physical Security Plan to document, implement, and maintain. Correct Requirement reference in R1.4 to R4	

Standard Development Roadmap

This section is maintained by the drafting team during the development of the standard and will be removed when the standard becomes effective.

Development Steps Completed:

1. The Standards Committee (SC) accepted the Standards Authorization Request (SAR) for Project 2008-06 Cyber Security Order 706 on March 10, 2008.
2. The SAR for Project 2008-06 Cyber Security Order 706 was posted for industry comment March 20–April 19, 2008.
3. Nominations for the SAR drafting team members were solicited March 20–April 4, 2008.
4. The Executive Committee of the SC appointed the SAR drafting team for Project 2008-06 Cyber Security Order 706 on April 25, 2008 and the full SC ratified the Executive Committee's action on May 8.
5. The SC accepted the SAR and approved moving forward with Project 2008-06 Cyber Security Order on July 10, 2008.
6. Nominations for the standard drafting team (SDT) for Project 2008-06 Cyber Security Order 706 were solicited July 15–28, 2008.
7. The Executive Committee of the SC appointed the SDT for Project 2008-06 Cyber Security Order 706 on August 7, 2008.

Proposed Action Plan and Description of Current Draft:

The standard drafting team for Project 2008-06 Cyber Security Order 706 (SDT CSO706) has been assigned the responsibility to review each of the following reliability standards to ensure that they conform to the latest version of the ERO Rules of Procedure, including the Reliability Standards Development Procedure, and also address all of the directed modifications identified in the FERC Order 706:

CIP–002–1 — Cyber Security — Critical Cyber Asset Identification
CIP–003–1 — Cyber Security — Security Management Controls
CIP–004–1 — Cyber Security — Personnel and Training
CIP–005–1 — Cyber Security — Electronic Security Perimeter(s)
CIP–006–1 — Cyber Security — Physical Security
CIP–007–1 — Cyber Security — Systems Security Management
CIP–008–1 — Cyber Security — Incident Reporting and Response Planning
CIP–009–1 — Cyber Security — Recovery Plans for Critical Cyber Assets

Because of the extensive scope of Project 2008-06 Cyber Security Order 706 the SDT CSO706 is implementing a multiphase approach for revising this set of standards.

Phase I of the project includes necessary modifications to CIP-002-1 through CIP-009-1 to comply with the near term specific directives included in FERC Order 706. In particular, the SDT addressed the directive in FERC Order 706 that the "... ERO modify the CIP Reliability Standards through its Reliability Standards development process to remove references to reasonable business judgment before compliance audits begin in 2009." In addition, a number of other directives included in FERC Order 706, which apply to specific standards are also addressed in Phase I. More contentious issues to be addressed by the SDT associated with the modification of this set of standards will be addressed in a later phase(s) of Project 2008-06 Cyber Security Order 706.

This posting of the cyber standards for industry comment only relates to Phase I of the project. Specifically, SDT CSO706 produced a revised version of Standard CIP–007–2 — Cyber Security — Systems Security Management and is posting the proposed modifications for a 45-day comment period.

Future Development Plan:

Anticipated Actions	Anticipated Date
1. Develop and post reply comments to initial posting of standard for industry comment	January 7–February 17, 2009
2. Post for 30-day pre-ballot period.	February 18–March 31, 2009
3. Conduct initial ballot	April 2–11, 2009
4. Post response to comments on first ballot	April 20–May 12, 2009
5. Conduct recirculation ballot	May 13–22, 2009
6. Board adoption date.	To be determined.

A. Introduction

1. Title: Cyber Security — Systems Security Management

2. Number: CIP-007-2

3. Purpose: Standard CIP-007-2 requires Responsible Entities to define methods, processes, and procedures for securing those systems determined to be Critical Cyber Assets, as well as the other (non-critical) Cyber Assets within the Electronic Security Perimeter(s). Standard CIP-007-2 should be read as part of a group of standards numbered Standards CIP-002-2 through CIP-009-2.

4. Applicability:

4.1. Within the text of Standard CIP-007-2, "Responsible Entity" shall mean:

4.1.1 Reliability Coordinator.

4.1.2 Balancing Authority.

4.1.3 Interchange Authority.

4.1.4 Transmission Service Provider.

4.1.5 Transmission Owner.

4.1.6 Transmission Operator.

4.1.7 Generator Owner.

4.1.8 Generator Operator.

4.1.9 Load Serving Entity.

4.1.10 NERC.

4.1.11 Regional Entity.

4.2. The following are exempt from Standard CIP-007-2:

4.2.1 Facilities regulated by the U.S. Nuclear Regulatory Commission or the Canadian Nuclear Safety Commission.

4.2.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.3 Responsible Entities that, in compliance with Standard CIP-002-2, identify that they have no Critical Cyber Assets.

5. Effective Date: The first day of the third calendar quarter after applicable regulatory approvals have been received (or the Reliability Standard otherwise becomes effective the first day of the third calendar quarter after BOT adoption in those jurisdictions where regulatory approval is not required).

B. Requirements

R1. Test Procedures — The Responsible Entity shall ensure that new Cyber Assets and significant changes to existing Cyber Assets within the Electronic Security Perimeter do not adversely affect existing cyber security controls. For purposes of Standard CIP-007-2, a significant change shall, at a minimum, include implementation of security patches, cumulative service packs, vendor releases, and version upgrades of operating systems, applications, database platforms, or other third-party software or firmware.

R1.1. The Responsible Entity shall create, implement, and maintain cyber security test procedures in a manner that minimizes adverse effects on the production system or its operation.

R1.2. The Responsible Entity shall document that testing is performed in a manner that reflects the production environment.

R1.3. The Responsible Entity shall document test results.

R2. Ports and Services — The Responsible Entity shall establish, document and implement a process to ensure that only those ports and services required for normal and emergency operations are enabled.

R2.1. The Responsible Entity shall enable only those ports and services required for normal and emergency operations.

R2.2. The Responsible Entity shall disable other ports and services, including those used for testing purposes, prior to production use of all Cyber Assets inside the Electronic Security Perimeter(s).

R2.3. In the case where unused ports and services cannot be disabled due to technical limitations, the Responsible Entity shall document compensating measure(s) applied to mitigate risk exposure.

R3. Security Patch Management — The Responsible Entity, either separately or as a component of the documented configuration management process specified in CIP-003-2 Requirement R6, shall establish, document and implement a security patch management program for tracking, evaluating, testing, and installing applicable cyber security software patches for all Cyber Assets within the Electronic Security Perimeter(s).

R3.1. The Responsible Entity shall document the assessment of security patches and security upgrades for applicability within thirty calendar days of availability of the patches or upgrades.

R3.2. The Responsible Entity shall document the implementation of security patches. In any case where the patch is not installed, the Responsible Entity shall document compensating measure(s) applied to mitigate risk exposure.

R4. Malicious Software Prevention — The Responsible Entity shall use anti-virus software and other malicious software ("malware") prevention tools, where technically feasible, to detect, prevent, deter, and mitigate the introduction, exposure, and propagation of malware on all Cyber Assets within the Electronic Security Perimeter(s).

R4.1. The Responsible Entity shall document and implement anti-virus and malware prevention tools. In the case where anti-virus software and malware prevention tools are not installed, the Responsible Entity shall document compensating measure(s) applied to mitigate risk exposure.

R4.2. The Responsible Entity shall document and implement a process for the update of anti-virus and malware prevention "signatures." The process must address testing and installing the signatures.

R5. Account Management — The Responsible Entity shall establish, implement, and document technical and procedural controls that enforce access authentication of, and accountability for, all user activity, and that minimize the risk of unauthorized system access.

R5.1. The Responsible Entity shall ensure that individual and shared system accounts and authorized access permissions are consistent with the concept of "need to know" with respect to work functions performed.

R5.1.1. The Responsible Entity shall ensure that user accounts are implemented as approved by designated personnel. Refer to Standard CIP-003-2 Requirement R5.

R5.1.2. The Responsible Entity shall establish methods, processes, and procedures that generate logs of sufficient detail to create historical audit trails of individual user account access activity for a minimum of ninety days.

R5.1.3. The Responsible Entity shall review, at least annually, user accounts to verify access privileges are in accordance with Standard CIP-003-2 Requirement R5 and Standard CIP-004-2 Requirement R4.

R5.2. The Responsible Entity shall implement a policy to minimize and manage the scope and acceptable use of administrator, shared, and other generic account privileges including factory default accounts.

R5.2.1. The policy shall include the removal, disabling, or renaming of such accounts where possible. For such accounts that must remain enabled, passwords shall be changed prior to putting any system into service.

R5.2.2. The Responsible Entity shall identify those individuals with access to shared accounts.

R5.2.3. Where such accounts must be shared, the Responsible Entity shall have a policy for managing the use of such accounts that limits access to only those with authorization, an audit trail of the account use (automated or manual), and steps for securing the account in the event of personnel changes (for example, change in assignment or termination).

R5.3. At a minimum, the Responsible Entity shall require and use passwords, subject to the following, as technically feasible:

R5.3.1. Each password shall be a minimum of six characters.

R5.3.2. Each password shall consist of a combination of alpha, numeric, and "special" characters.

R5.3.3. Each password shall be changed at least annually, or more frequently based on risk.

R6. Security Status Monitoring — The Responsible Entity shall ensure that all Cyber Assets within the Electronic Security Perimeter, as technically feasible, implement automated tools or organizational process controls to monitor system events that are related to cyber security.

R6.1. The Responsible Entity shall implement and document the organizational processes and technical and procedural mechanisms for monitoring for security events on all Cyber Assets within the Electronic Security Perimeter.

R6.2. The security monitoring controls shall issue automated or manual alerts for detected Cyber Security Incidents.

R6.3. The Responsible Entity shall maintain logs of system events related to cyber security, where technically feasible, to support incident response as required in Standard CIP-008-2.

R6.4. The Responsible Entity shall retain all logs specified in Requirement R6 for ninety calendar days.

R6.5. The Responsible Entity shall review logs of system events related to cyber security and maintain records documenting review of logs.

R7. Disposal or Redeployment — The Responsible Entity shall establish and implement formal methods, processes, and procedures for disposal or redeployment of Cyber Assets within the Electronic Security Perimeter(s) as identified and documented in Standard CIP-005-2.

R7.1. Prior to the disposal of such assets, the Responsible Entity shall destroy or erase the data storage media to prevent unauthorized retrieval of sensitive cyber security or reliability data.

R7.2. Prior to redeployment of such assets, the Responsible Entity shall, at a minimum, erase the data storage media to prevent unauthorized retrieval of sensitive cyber security or reliability data.

R7.3. The Responsible Entity shall maintain records that such assets were disposed of or redeployed in accordance with documented procedures.

R8. Cyber Vulnerability Assessment — The Responsible Entity shall perform a cyber vulnerability assessment of all Cyber Assets within the Electronic Security Perimeter at least annually. The vulnerability assessment shall include, at a minimum, the following:

R8.1. A document identifying the vulnerability assessment process;

R8.2. A review to verify that only ports and services required for operation of the Cyber Assets within the Electronic Security Perimeter are enabled;

R8.3. A review of controls for default accounts; and,

R8.4. Documentation of the results of the assessment, the action plan to remediate or mitigate vulnerabilities identified in the assessment, and the execution status of that action plan.

R9. Documentation Review and Maintenance — The Responsible Entity shall review and update the documentation specified in Standard CIP-007-2 at least annually. Changes resulting from modifications to the systems or controls shall be documented within thirty calendar days of the change being completed.

C. Measures

M1. The Responsible Entity shall make available documentation of its security test procedures as specified in Requirement R1.

M2. The Responsible Entity shall make available documentation as specified in Requirement R2.

M3. The Responsible Entity shall make available documentation and records of its security patch management program, as specified in Requirement R3.

M4. The Responsible Entity shall make available documentation and records of its malicious software prevention program as specified in Requirement R4.

M5. The Responsible Entity shall make available documentation and records of its account management program as specified in Requirement R5.

M6. The Responsible Entity shall make available documentation and records of its security status monitoring program as specified in Requirement R6.

M7. The Responsible Entity shall make available documentation and records of its program for the disposal or redeployment of Cyber Assets as specified in Requirement R7.

M8. The Responsible Entity shall make available documentation and records of its annual vulnerability assessment of all Cyber Assets within the Electronic Security Perimeters(s) as specified in Requirement R8.

M9. The Responsible Entity shall make available documentation and records demonstrating the review and update as specified in Requirement R9.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

1.1.1 Regional Entity for Responsible Entities that do not perform delegated tasks for their Regional Entity.

1.1.2 ERO for Regional Entity.

1.1.3 Third-party monitor without vested interest in the outcome for NERC.

1.2. Compliance Monitoring Period and Reset Time Frame

Not applicable.

1.3. Compliance Monitoring and Enforcement Processes

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints

1.4. Data Retention

1.4.1 The Responsible Entity shall keep all documentation and records from the previous full calendar year unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

1.4.2 The Responsible Entity shall retain security–related system event logs for ninety calendar days, unless longer retention is required pursuant to Standard CIP-008-2 Requirement R2.

1.4.3 The Compliance Enforcement Authority in conjunction with the Registered Entity shall keep the last audit records and all requested and submitted subsequent audit records.

1.5. Additional Compliance Information.

2. Violation Severity Levels (Under development by the CIP VSL Drafting Team)

E. Regional Variances

None identified.

Version History

Version	Date	Action	Change Tracking
2		Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment and acceptance of risk. Replaced the RRO with the RE as a responsible	

		entity. Rewording of Effective Date. R9 changed ninety (90) days to thirty (30) days Changed compliance monitor to Compliance Enforcement Authority.	
		Modifications to clarify the requirements and to incorporate industry comments. Revise the Purpose of this standard to clarify that Standard CIP-007-2 requires Responsible Entities to define methods, processes, and procedures for securing Cyber Assets and other (non-Critical) Assets within an Electronic Security Perimeter.	

Standard Development Roadmap

This section is maintained by the drafting team during the development of the standard and will be removed when the standard becomes effective.

Development Steps Completed:

1. The Standards Committee (SC) accepted the Standards Authorization Request (SAR) for Project 2008-06 Cyber Security Order 706 on March 10, 2008.
2. The SAR for Project 2008-06 Cyber Security Order 706 was posted for industry comment March 20–April 19, 2008.
3. Nominations for the SAR drafting team members were solicited March 20–April 4, 2008.
4. The Executive Committee of the SC appointed the SAR drafting team for Project 2008-06 Cyber Security Order 706 on April 25, 2008 and the full SC ratified the Executive Committee's action on May 8.
5. The SC accepted the SAR and approved moving forward with Project 2008-06 Cyber Security Order on July 10, 2008.
6. Nominations for the standard drafting team (SDT) for Project 2008-06 Cyber Security Order 706 were solicited July 15–28, 2008.
7. The Executive Committee of the SC appointed the SDT for Project 2008-06 Cyber Security Order 706 on August 7, 2008.

Proposed Action Plan and Description of Current Draft:

The standard drafting team for Project 2008-06 Cyber Security Order 706 (SDT CSO706) has been assigned the responsibility to review each of the following reliability standards to ensure that they conform to the latest version of the ERO Rules of Procedure, including the Reliability Standards Development Procedure, and also address all of the directed modifications identified in the FERC Order 706:

CIP–002–1 — Cyber Security — Critical Cyber Asset Identification
CIP–003–1 — Cyber Security — Security Management Controls
CIP–004–1 — Cyber Security — Personnel and Training
CIP–005–1 — Cyber Security — Electronic Security Perimeter(s)
CIP–006–1 — Cyber Security — Physical Security
CIP–007–1 — Cyber Security — Systems Security Management
CIP–008–1 — Cyber Security — Incident Reporting and Response Planning
CIP–009–1 — Cyber Security — Recovery Plans for Critical Cyber Assets

Because of the extensive scope of Project 2008-06 Cyber Security Order 706 the SDT CSO706 is implementing a multiphase approach for revising this set of standards.

Phase I of the project includes necessary modifications to CIP-002-1 through CIP-009-1 to comply with the near term specific directives included in FERC Order 706. In particular, the SDT addressed the directive in FERC Order 706 that the "... ERO modify the CIP Reliability Standards through its Reliability Standards development process to remove references to reasonable business judgment before compliance audits begin in 2009." In addition, a number of other directives included in FERC Order 706, which apply to specific standards are also addressed in Phase I. More contentious issues to be addressed

by the SDT associated with the modification of this set of standards will be addressed in a later phase(s) of Project 2008-06 Cyber Security Order 706.

This posting of the cyber standards for industry comment only relates to Phase I of the project. Specifically, SDT CSO706 produced a revised version of Standard CIP–008–2 — Cyber Security — Incident Reporting and Response Planning and is posting the proposed modifications for a 45-day comment period.

Future Development Plan:

Anticipated Actions	Anticipated Date
1. Develop and post reply comments to initial posting of standard for industry comment	January 7–February 17, 2009
2. Post for 30-day pre-ballot period.	February 18–March 31, 2009
3. Conduct initial ballot	April 2–11, 2009
4. Post response to comments on first ballot	April 20–May 12, 2009
5. Conduct recirculation ballot	May 13–22, 2009
6. Board adoption date.	To be determined.

A. Introduction

1. Title: Cyber Security — Incident Reporting and Response Planning

2. Number: CIP-008-2

3. Purpose: Standard CIP-008-2 ensures the identification, classification, response, and reporting of Cyber Security Incidents related to Critical Cyber Assets. Standard CIP-008-2 should be read as part of a group of standards numbered Standards CIP-002-2 through CIP-009-2.

4. Applicability

4.1. Within the text of Standard CIP-008-2, "Responsible Entity" shall mean:

4.1.1 Reliability Coordinator.

4.1.2 Balancing Authority.

4.1.3 Interchange Authority.

4.1.4 Transmission Service Provider.

4.1.5 Transmission Owner.

4.1.6 Transmission Operator.

4.1.7 Generator Owner.

4.1.8 Generator Operator.

4.1.9 Load Serving Entity.

4.1.10 NERC.

4.1.11 Regional Entity.

4.2. The following are exempt from Standard CIP-008-2:

4.2.1 Facilities regulated by the U.S. Nuclear Regulatory Commission or the Canadian Nuclear Safety Commission.

4.2.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.3 Responsible Entities that, in compliance with Standard CIP-002-2, identify that they have no Critical Cyber Assets.

5. Effective Date: The first day of the third calendar quarter after applicable regulatory approvals have been received (or the Reliability Standard otherwise becomes effective the first day of the third calendar quarter after BOT adoption in those jurisdictions where regulatory approval is not required).

B. Requirements

R1. Cyber Security Incident Response Plan — The Responsible Entity shall develop and maintain a Cyber Security Incident response plan and implement the plan in response to Cyber Security Incidents. The Cyber Security Incident response plan shall address, at a minimum, the following:

R1.1. Procedures to characterize and classify events as reportable Cyber Security Incidents.

R1.2. Response actions, including roles and responsibilities of Cyber Security Incident response teams, Cyber Security Incident handling procedures, and communication plans.

R1.3. Process for reporting Cyber Security Incidents to the Electricity Sector Information Sharing and Analysis Center (ES-ISAC). The Responsible Entity must ensure that all reportable Cyber Security Incidents are reported to the ES-ISAC either directly or through an intermediary.

R1.4. Process for updating the Cyber Security Incident response plan within thirty calendar days of any changes.

R1.5. Process for ensuring that the Cyber Security Incident response plan is reviewed at least annually.

R1.6. Process for ensuring the Cyber Security Incident response plan is tested at least annually. A test of the Cyber Security Incident response plan can range from a paper drill, to a full operational exercise, to the response to an actual incident. Testing the Cyber Security Incident response plan does not require removing a component or system from service during the test.

R2. Cyber Security Incident Documentation — The Responsible Entity shall keep relevant documentation related to Cyber Security Incidents reportable per Requirement R1.1 for three calendar years.

C. Measures

M1. The Responsible Entity shall make available its ~~dated~~ Cyber Security Incident response plan as indicated in Requirement R1 and documentation of the review, updating, and testing of the plan

M2. The Responsible Entity shall make available all documentation as specified in Requirement R2.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

1.1.1 Regional Entity for Responsible Entities that do not perform delegated tasks for their Regional Entity.

1.1.2 ERO for Regional Entity.

1.1.3 Third-party monitor without vested interest in the outcome for NERC.

1.2. Compliance Monitoring Period and Reset Time Frame

Not applicable.

1.3. Compliance Monitoring and Enforcement Processes

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints

1.4. Data Retention

1.4.1 The Responsible Entity shall keep documentation other than that required for reportable Cyber Security Incidents as specified in Standard CIP-008-2 for the previous full calendar year unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

1.4.2 The Compliance Enforcement Authority in conjunction with the Registered Entity shall keep the last audit records and all requested and submitted subsequent audit records.

1.5. Additional Compliance Information

1.5.1 The Responsible Entity may not take exception in its cyber security policies to the creation of a Cyber Security Incident response plan.

1.5.2 The Responsible Entity may not take exception in its cyber security policies to reporting Cyber Security Incidents to the ES ISAC.

2. Violation Severity Levels (Under Development by the CIP VSL Drafting Team)

E. Regional Variances

None identified.

Version History

Version	Date	Action	Change Tracking
2		Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
		Modifications to clarify the requirements and to incorporate industry comments. Removed “dated” from Measure M1.	

Standard Development Roadmap

This section is maintained by the drafting team during the development of the standard and will be removed when the standard becomes effective.

Development Steps Completed:

1. The Standards Committee (SC) accepted the Standards Authorization Request (SAR) for Project 2008-06 Cyber Security Order 706 on March 10, 2008.
2. The SAR for Project 2008-06 Cyber Security Order 706 was posted for industry comment March 20–April 19, 2008.
3. Nominations for the SAR drafting team members were solicited March 20–April 4, 2008.
4. The Executive Committee of the SC appointed the SAR drafting team for Project 2008-06 Cyber Security Order 706 on April 25, 2008 and the full SC ratified the Executive Committee's action on May 8.
5. The SC accepted the SAR and approved moving forward with Project 2008-06 Cyber Security Order on July 10, 2008.
6. Nominations for the standard drafting team (SDT) for Project 2008-06 Cyber Security Order 706 were solicited July 15–28, 2008.
7. The Executive Committee of the SC appointed the SDT for Project 2008-06 Cyber Security Order 706 on August 7, 2008.

Proposed Action Plan and Description of Current Draft:

The standard drafting team for Project 2008-06 Cyber Security Order 706 (SDT CSO706) has been assigned the responsibility to review each of the following reliability standards to ensure that they conform to the latest version of the ERO Rules of Procedure, including the Reliability Standards Development Procedure, and also address all of the directed modifications identified in the FERC Order 706:

CIP–002–1 — Cyber Security — Critical Cyber Asset Identification
CIP–003–1 — Cyber Security — Security Management Controls
CIP–004–1 — Cyber Security — Personnel and Training
CIP–005–1 — Cyber Security — Electronic Security Perimeter(s)
CIP–006–1 — Cyber Security — Physical Security
CIP–007–1 — Cyber Security — Systems Security Management
CIP–008–1 — Cyber Security — Incident Reporting and Response Planning
CIP–009–1 — Cyber Security — Recovery Plans for Critical Cyber Assets

Because of the extensive scope of Project 2008-06 Cyber Security Order 706 the SDT CSO706 is implementing a multiphase approach for revising this set of standards.

Phase I of the project includes necessary modifications to CIP-002-1 through CIP-009-1 to comply with the near term specific directives included in FERC Order 706. In particular, the SDT addressed the directive in FERC Order 706 that the "... ERO modify the CIP Reliability Standards through its Reliability Standards development process to remove references to reasonable business judgment before compliance audits begin in 2009." In addition, a number of other directives included in FERC Order 706, which apply to specific standards are also addressed in Phase I. More contentious issues to be addressed by the SDT associated with the modification of this set of standards will be addressed in a later phase(s) of Project 2008-06 Cyber Security Order 706.

This posting of the cyber standards for industry comment only relates to Phase I of the project. Specifically, SDT CSO706 produced a revised version of Standard CIP–009–2 — Cyber Security — Recovery Plans for Critical Cyber Assets and is posting the proposed modifications for a 45-day comment period.

Future Development Plan:

Anticipated Actions	Anticipated Date
1. Develop and post reply comments to initial posting of standard for industry comment	January 7–February 17, 2009
2. Post for 30-day pre-ballot period.	February 18–March 31, 2009
3. Conduct initial ballot	April 2–11, 2009
4. Post response to comments on first ballot	April 20–May 12, 2009
5. Conduct recirculation ballot	May 13–22, 2009
6. Board adoption date.	To be determined.

A. Introduction

1. **Title:** Cyber Security — Recovery Plans for Critical Cyber Assets

2. **Number:** CIP-009-2

3. **Purpose:** Standard CIP-009-2 ensures that recovery plan(s) are put in place for Critical Cyber Assets and that these plans follow established business continuity and disaster recovery techniques and practices. Standard CIP-009-2 should be read as part of a group of standards numbered Standards CIP-002-2 through CIP-009-2.

4. **Applicability:**

   4.1. Within the text of Standard CIP-009-2, "Responsible Entity" shall mean:

   4.1.1 Reliability Coordinator

   4.1.2 Balancing Authority

   4.1.3 Interchange Authority

   4.1.4 Transmission Service Provider

   4.1.5 Transmission Owner

   4.1.6 Transmission Operator

   4.1.7 Generator Owner

   4.1.8 Generator Operator

   4.1.9 Load Serving Entity

   4.1.10 NERC

   4.1.11 Regional Entity

   4.2. The following are exempt from Standard CIP-009-2:

   4.2.1 Facilities regulated by the U.S. Nuclear Regulatory Commission or the Canadian Nuclear Safety Commission.

   4.2.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

   4.2.3 Responsible Entities that, in compliance with Standard CIP-002-2, identify that they have no Critical Cyber Assets.

5. **Effective Date:** The first day of the third calendar quarter after applicable regulatory approvals have been received (or the Reliability Standard otherwise becomes effective the first day of the third calendar quarter after BOT adoption in those jurisdictions where regulatory approval is not required).

B. Requirements

~~The Responsible Entity shall comply with the following requirements of Standard CIP-009-2:~~

R1. Recovery Plans — The Responsible Entity shall create and annually review recovery plan(s) for Critical Cyber Assets. The recovery plan(s) shall address at a minimum the following:

R1.1. Specify the required actions in response to events or conditions of varying duration and severity that would activate the recovery plan(s).

R1.2. Define the roles and responsibilities of responders.

R2. Exercises — The recovery plan(s) shall be exercised at least annually. An exercise of the recovery plan(s) can range from a paper drill, to a full operational exercise, to recovery from an actual incident.

R3. Change Control — Recovery plan(s) shall be updated to reflect any changes or lessons learned as a result of an exercise or the recovery from an actual incident. Updates shall be communicated to personnel responsible for the activation and implementation of the recovery plan(s) within thirty calendar days of the change being completed.

R4. Backup and Restore — The recovery plan(s) shall include processes and procedures for the backup and storage of information required to successfully restore Critical Cyber Assets. For example, backups may include spare electronic components or equipment, written documentation of configuration settings, tape backup, etc.

R5. Testing Backup Media — Information essential to recovery that is stored on backup media shall be tested at least annually to ensure that the information is available. Testing can be completed off site.

C. Measures

M1. The Responsible Entity shall make available its ~~dated~~ recovery plan(s) as specified in Requirement R1.

M2. The Responsible Entity shall make available its ~~dated~~ records documenting required exercises as specified in Requirement R2.

M3. The Responsible Entity shall make available its ~~dated~~ documentation of changes to the recovery plan(s), and documentation of all communications, as specified in Requirement R3.

M4. The Responsible Entity shall make available its ~~dated~~ documentation regarding backup and storage of information as specified in Requirement R4.

M5. The Responsible Entity shall make available its ~~dated~~ documentation of testing of backup media as specified in Requirement R5.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

1.1.1 Regional Entity for Responsible Entities that do not perform delegated tasks for their Regional Entity.

1.1.2 ERO for Regional Entities.

1.1.3 Third-party monitor without vested interest in the outcome for NERC.

1.2. Compliance Monitoring Period and Reset Time Frame

Not applicable.

1.3. Compliance Monitoring and Enforcement Processes

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints

1.4. Data Retention

1.4.1 The Responsible Entity shall keep documentation required by Standard CIP-009-2 from the previous full calendar year unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

1.4.2 The Compliance Enforcement Authority in conjunction with the Registered Entity shall keep the last audit records and all requested and submitted subsequent audit records.

1.5. Additional Compliance Information

2. Violation Severity Levels (Under development by the CIP VSL Drafting Team)

E. Regional Variances

None identified.

Version History

Version	Date	Action	Change Tracking
2		Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Communication of revisions to the recovery plan changed from 90 days to 30 days. Changed compliance monitor to Compliance Enforcement Authority.	
		Modifications to clarify the requirements and to incorporate industry comments. Revised the wording in Section B, Requirements, to be consistent with the other standards. Remove “dated” from the measures.	

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Consideration of Comments on 1st Draft of CIP-002-2 through CIP-009-2 — Project 2008-06 — Cyber Security Order 706

The Cyber Security for Order 706 Standard Drafting Team thanks all commenters who submitted comments on the first draft of following CIP standards:

CIP–002–2 — Cyber Security — Critical Cyber Asset Identification
CIP–003–2 — Cyber Security — Security Management Controls
CIP–004–2 — Cyber Security — Personnel and Training
CIP–005–2 — Cyber Security — Electronic Security Perimeter(s)
CIP–006–2 — Cyber Security — Physical Security
CIP–007–2 — Cyber Security — Systems Security Management
CIP–008–2 — Cyber Security — Incident Reporting and Response Planning
CIP–009–2 — Cyber Security — Recovery Plans for Critical Cyber Assets

These standards were posted for a 45-day public comment period from November 21, 2008 through January 5, 2009. The stakeholders were asked to provide feedback on the standards through a special Electronic Comment Form. There were 52 sets of comments, including comments from more than 100 different people from over 55 companies representing 9 of the 10 Industry Segments as shown in the table on the following pages.

http://www.nerc.com/filez/standards/Project_2008-06_Cyber_Security.html

If you feel that your comment has been overlooked, please let us know immediately. Our goal is to give every comment serious consideration in this process! If you feel there has been an error or omission, you can contact the Vice President and Director of Standards, Gerry Adamski, at 609-452-8060 or at gerry.adamski@nerc.net. In addition, there is a NERC Reliability Standards Appeals Process.[1]

[1] The appeals process is in the Reliability Standards Development Procedures: http://www.nerc.com/standards/newstandardsprocess.html.

Index to Questions, Comments, and Responses

The Industry Segments are:

1 — Transmission Owners
2 — RTOs, ISOs
3 — Load-serving Entities
4 — Transmission-dependent Utilities
5 — Electric Generators
6 — Electricity Brokers, Aggregators, and Marketers
7 — Large Electricity End Users
8 — Small Electricity End Users
9 — Federal, State, Provincial Regulatory or other Government Entities
10 — Regional Reliability Organizations, Regional Entities

		Commenter	Organization	Industry Segment									
				1	2	3	4	5	6	7	8	9	10
1.	Individual	Kent Kujala	Detroit Edison Company			✓		✓					
2.	Individual	Paul Golden	PacifiCorp	✓		✓		✓					
3.	Group	Doug Hohlbaugh	FirstEnergy Corp	✓		✓	✓	✓	✓				
4.	Individual	Ray Andrews	MidAmerican Energy Company	✓		✓		✓					
5.	Group	Guy Zito	Northeast Power Coordinating Council										✓

	Additional Member	Additional Organization	Region	Segment Selection
1.	Sam Ciccone	FE	RFC	1, 3, 4, 5, 6
2.	Terry Malone	FE	RFC	1, 3, 4, 5, 6
3.	Karen Yoder	FE	RFC	1, 3, 4, 5, 6
4.	Dave Folk	FE	RFC	1, 3, 4, 5, 6
5.	Henry Stevens	FE	RFC	1, 3, 4, 5, 6

	Commenter	Organization	Industry Segment									
			1	2	3	4	5	6	7	8	9	10

	Additional Member	Additional Organization	Region	Segment Selection
1.	Edward Dahill	National Grid	NPCC	3
2.	Gerald Mannarino	NYPA	NPCC	5
3.	Frederick White	Northeast Utilities	NPCC	1
4.	Michael Garton	Dominion Resources Services, Inc.	NPCC	5
5.	Kathleen Goodman	ISO - New England	NPCC	2
6.	Michael Gildea	Constellation Energy	NPCC	6
7.	Donald Nelson	Massachusetts Dept. of Public Utilities	NPCC	9
8.	Roger Champagne	Hydro-Quebec TransEnergie	NPCC	1
9.	David Kiguel	Hydro One Networks Inc.	NPCC	1
10.	Brian Hogue	NPCC	NPCC	10
11.	Gerry Dunbar	NPCC	NPCC	10
12.	Lee Pedowicz	NPCC	NPCC	10
13.	Brian Evans-Mongeon	Utility Services	NPCC	6

6.	Individual	Linda Perez	WECC Reliability Coordination										✓
7.	Group	Marc M. Butts	Southern Company	✓		✓		✓	✓				

	Additional Member	Additional Organization	Region	Segment Selection
1.	Rodney O'Bryant	Southern Company Services	SERC	1
2.	Larry Spoonemore	Southern Company Services	SERC	5
3.	Jim Busbin	Southern Company Services	SERC	1
4.	Bonnie Parker	Southern Company Services	SERC	5
5.	Boyd Nation	Southern Company Services	SERC	1
6.	Wes Stewart	Southern Company Services	SERC	1
7.	Bob Canada	Southern Company Services	SERC	1
8.	Wade Mundy	Southern Company Services	SERC	1
9.	John Greaves	Georgia Power Company	SERC	1, 3

	Commenter	Organization	Industry Segment									
			1	2	3	4	5	6	7	8	9	10
	10. Jay Cribb	Southern Company Services	SERC	1								
	11. Chris Wilson	Southern Company Services	SERC	1								
	12. Terry Coggins	Southern Company Services	SERC	1								
	13. Russ Ward	Southern Company Services	SERC	1								
	14. Steve Bennett	Georgia Power Company	SERC	1, 3								
	15. Larry Smith	Alabama Power Company	SERC	1, 3								
8.	Individual	Rick Terrill	Luminant Power					✓					
9.	Group	Matthew E. Luallen	Encari								✓		
	Additional Member	**Additional Organization**	**Region**	**Segment Selection**									
	1. Steve Hamburg	Encari	NA - Not Applicable	8									
	2. Mark Simon	Encari	NA - Not Applicable	8									
	3. Lenny Mansell	Encari	NA - Not Applicable	8									
	4. Peter Brown	Encari	NA - Not Applicable	8									
10.	Individual	Mark Phillips	TransAlta Centralia Generation, LLC					✓					
11.	Group	Denise Koehn	Bonneville Power Administration	✓		✓		✓	✓				
	Additional Member	**Additional Organization**	**Region**	**Segment Selection**									
	1. Curt Wilkins	Transmission System Operations	WECC	1									
	2. Bradley Folden	Transmission Technical Training	WECC	1									
	3. Kelly Hazelton	Transmission Control Cntr HW Design & Maint	WECC	1									
12.	Individual	John Lim	Consolidated Edison Company of New York, Inc.	✓		✓		✓	✓				
13.	Individual	Rebecca Furman	Southern California Edison Company	✓		✓		✓	✓				

		Commenter	Organization	Industry Segment									
				1	2	3	4	5	6	7	8	9	10
14.	Individual	T.J. Szelistowski	Tampa Electric Company	✓		✓		✓					
15.	Group	Jalal Babik	Electric Market Policy	✓		✓		✓	✓				

	Additional Member	Additional Organization	Region	Segment Selection
1.	Louis Slade	Electric Market Policy	RFC	6
2.	Mike Garton	Electric Market Policy	NPCC	5
3.	Mark Engels	IT Risk Management	SERC	
4.	Ruth Blevins	IT Risk Management	SERC	
5.	Dennis Sollars	IT Risk Management	SERC	
6.	John Albert	Security Compliance	SERC	

16.	Group	Annette M. Bannon	PPL Corporation	✓				✓	✓				

Please complete the following information.

	Additional Member	Additional Organization	Region	Segment Selection
1.	Mark Heimbach	PPL EnergyPlus	MRO	6
2.			NPCC	6
3.			RFC	6
4.			SERC	6
5.			SPP	6
6.	Jim Batug	PPL Generation	NPCC	5
7.			RFC	5
8.			WECC	5
9.	Barry Skoras	PPL Electric Utilities	RFC	1

17.	Group	Michael Brytowski	MRO NERC Standards Review Subcommittee										✓

	Additional Member	Additional Organization	Region	Segment Selection
1.	Neal Balu	WPS	MRO	3, 4, 5, 6

	Commenter	Organization	Industry Segment									
			1	2	3	4	5	6	7	8	9	10
	2. Terry Bilke	MISO	MRO	2								
	3. Carol Gerou	MP	MRO	1, 3, 5, 6								
	4. Jim Haigh	WAPA	MRO	1, 6								
	5. Charles Lawrence	ATC	MRO	1								
	6. Ken Goldsmith	ALTW	MRO	4								
	7. Terry Harbour	MEC	MRO	1, 3, 5, 6								
	8. Pam Sordet	XCEL	MRO	1, 3, 5, 6								
	9. Dave Rudolph	BEPC	MRO	1, 3, 5, 6								
	10. Eric Ruskamp	LES	MRO	1, 3, 5, 6								
	11. Joseph Knight	GRE	MRO	1, 3, 5, 6								
	12. Larry Brusseau	MRO	MRO	10								
	13. Scott Nickels	RPU	MRO	3, 4, 5, 6								
18.	Group	Richard Kafka	Pepco Holdings, Inc - Affiliates		✓		✓		✓	✓				
	Additional Member	**Additional Organization**	**Region**	**Segment Selection**								
	1. Mark Godfrey	Pepco Holdings, Inc.	RFC	1								
19.	Individual	Michael Puscas	United Illuminating Company		✓		✓							
20.	Individual	Steven Dougherty	Deloitte& Touché, LLP											
21.	Individual	Chris Scanlon	Exelon		✓		✓		✓	✓				
22.	Individual	Mark Ringhausen	Old Dominion Electric Cooperative					✓						
23.	Individual	Alan Gale	City of Tallahassee (TAL)		✓		✓		✓					
24.	Individual	Brian Martin	BC Transmission Corporation		✓	✓								
25.	Individual	Joe Weiss	Applied Control Solutions, LLC											

		Commenter	Organization	Industry Segment									
				1	2	3	4	5	6	7	8	9	10
26.	Individual	Martin Bauer	US Bureau of Reclamation	✓				✓					
27.	Individual	Edward Bedder	Orange and Rockland Utilities Inc.	✓									
28.	Individual	Martin Narendorf	CenterPoint Energy	✓									
29.	Individual	Kris Manchur	Manitoba Hydro	✓	✓		✓	✓					
30.	Individual	Anita Lee	Alberta Electric System Operator		✓								
31.	Individual	Greg Mason	Dynegy					✓					
32.	Individual	Tim Conway	Northern Indiana Public Service Company	✓		✓		✓					
33.	Individual	Robert Huffman	CoreTrace								✓		
34.	Individual	Darryl Curtis / Greg Ward	Oncor Electric Delivery LLC	✓									
35.	Individual	Bob Thomas	Illinois Municipal Electric Agency				✓						
36.	Individual	Cathie Mellerup	Ontario Power Generation					✓					
37.	Individual	Jim Sorrels	American Electric Power	✓		✓		✓	✓				
38.	Individual	Dan Rochester	Ontario IESO		✓								
39.	Individual	Kirit Shah	Ameren	✓		✓		✓	✓				
40.	Individual	Jianmei Chai	Consumers Energy Company			✓	✓	✓					
41.	Individual	Alice Druffel	Xcel Energy	✓		✓		✓	✓				

		Commenter	Organization	Industry Segment									
				1	2	3	4	5	6	7	8	9	10
42.	Individual	Kathleen Goodman	ISO New England Inc		✓								
43.	Individual	Jason Shaver	American Transmission Company	✓									
44.	Individual	James W. Sample	TVA	✓		✓		✓	✓				
45.	Individual	Greg Rowland	Duke Energy	✓		✓		✓	✓				
46.	Individual	Tony Kroskey	Brazos Electric Power Cooperative, Inc.	✓									
47.	Group	Ed Goff	Progress Energy	✓		✓		✓	✓				
48.	Group	Ben Li	Standards Review Committee of ISO/RTO Council										

	Additional Member	Additional Organization	Region	Segment Selection
1.	Patrick Brown	PJM	NPCC	2
2.	Jim Castle	NYISO	NPCC	2
3.	Matt Goldberg	ISONE	NPCC	2
4.	Lourdes Estrada-Salinero	CAISO	WECC	2
5.	Anita Lee	AESO	WECC	2
6.	Steve Myers	ERCOT	ERCOT	2
7.	Bill Phillips	MISO	RFC	2
8.	Charles Yeung	SPP	SPP	2

49.	Individual	Aldo Nevarez	KEMA										
50.	Individual	Dave DeGroot	Austin Energy	✓				✓					

		Commenter	Organization	Industry Segment									
				1	2	3	4	5	6	7	8	9	10
51.	Individual	Glen Hattrup	Kansas City Power & Light	✓		✓		✓					
52.	Individual	Randy Schimka	San Diego Gas and Electric Co.	✓		✓	✓	✓					

1. The CSO706 SDT added management approval of the risk-based assessment methodology (per FERC Order 706, paragraph 236) to **CIP-002-1 Requirement R4**. Do you agree with the proposed modification? If not, please explain and provide an alternative to the proposed modification that would eliminate or minimize your disagreement.

Summary Consideration:

Organization	Yes or No	Question 1 Comment
Detroit Edison Company	Yes	
PacifiCorp	Yes	
FirstEnergy Corp	Yes	
MidAmerican Energy Company	Yes	
Northeast Power Coordinating Council	No	We recommend that CIP-002 be updated by moving CIP-003 R2 into CIP-002. By moving CIP-003 R2 into CIP-002 all the Requirements that all Entities must complete are in one Standard. The senior manager has not been identified in CIP-002. Moving CIP-003 R2 into the CIP-002 Standard clarifies who the senior manager is, and allows for only one Standard (CIP-002) that must be completed by everyone.
Response: **The SDT has received numerous comments related to either referencing CIP-003 R2 within CIP-002 R4 or moving CIP-003 R2 into CIP-002 in order to clarify the reference to the senior manager. Phase 1 of this project includes necessary modifications to CIP-002-1 through CIP-009-1 to comply with the near term specific directives included in FERC Order 706. The issue identified in your comment is an issue better suited for a later phase of this project. The SDT suggests that you review the changes proposed in the later phases of the project and resubmit your comments as appropriate if they have not been addressed.**		
WECC Relibaility Coordination	Yes	
Southern Company	Yes	CIP-002 Section D - Compliance: 1.1.1 does not specify who is responsible for the enforcement authority.

Organization	Yes or No	Question 1 Comment
		CIP-002 Section D - Compliance: 1.4.1 - Indefinite retention is not feasible, overall cost of storage depending on scope could potentially be very large. Item should define an upper bound of the request (e.g. a maximum of 3 years) CIP-002 Section D - Compliance: 1.4.2- Should have a time limit to reduce the overall liability of confidential information.
Response: **1.1.1 - The Regional Entity will serve as the Compliance Enforcement Authority for most entities. As the Regional Entity may not audit itself, the ERO will serve as the Compliance Enforcement Authority in auditing the Regional Entity. A third-party monitor without a vested interest in the outcome will serve as the Compliance Enforcement Authority for NERC. (Refer to NERC's Rules of Procedure, Paragraphs 404 and 405).** **1.4.1 – With the exception of retaining evidence in support of an investigation, the standard defines a finite retention period. The language that indicates the Compliance Enforcement Authority may direct the responsible entity to retain evidence for a longer period of time as part of an investigation is a restatement of what is included in the ERO Rules of Procedure. Reference the ERO Rules of Procedure Appendix 4C – Uniform Compliance Monitoring and Enforcement Procedures – Section 3.4.1 Compliance Violation Investigation Process Steps. While the duration of an investigation cannot be predicted, further clarification of the retention timeframe is outside the scope of the SDT.** **1.4.2 – This language supports the regularly scheduled audit intervals for all entities and supports the need to retain the confidentiality of some data. The audit data retention period is determined by the audit period for each Registered Entity.**		
Luminant Power	Yes	
Encari	No	1. R4 should also include a direct reference to CIP-003-2 R2 to ensure that the Responsible Entities are aware are all applicable requirements. A Responsible Entity that identifies a null CA list must still perform CIP-003-1 R2. This would allow the exemption in CIP-003-2 (4.2.3) to be removed. General Comment Provided in All Submissions--Other modifications were also made to this standard that are not included as part of the question. 2. The wording of 1.1.1 is awkward and should be modified. 3. We also request further clarification regarding the Data Retention Requirement 1.4.2 as to which entity will be maintaining the last audit records and submitted subsequent audit records. As the statement is currently worded "in conjunction" leaves this open to interpretation.

Organization	Yes or No	Question 1 Comment
Response: **1. The SDT has received numerous comments related to either referencing CIP-003 R2 within CIP-002 R4 or moving CIP-003 R2 into CIP-002 in order to clarify the reference to the senior manager. Phase 1 of this project includes necessary modifications to CIP-002-1 through CIP-009-1 to comply with the near term specific directives included in FERC Order 706. The issue identified in your comment is an issue better suited for a later phase of this project. The SDT suggests that you review the changes proposed in the later phases of the project and resubmit your comments as appropriate if they have not been addressed.** **2. The intent of the wording in 1.1.1 is to clarify which entity will serve as the Compliance Enforcement Authority. For most standards, the Regional Entity serves as the Compliance Enforcement Authority and audits the performance of the Reliability Coordinator, Transmission Operator, Balancing Authority, Generator Operator, Generator Owner, etc. In this standard, the Regional Entity is responsible for some of the requirements – but an entity cannot audit its own performance. Where the Regional Entity is also the responsible entity, the ERO will audit the Regional Entity's performance. Where the ERO is the responsible entity, a third-party monitor without vested interest in the outcome will conduct the audit.** **3. The data retention periods for the standard requirements are specified in the standards. The language of 1.4.2 indicates that the Compliance Enforcement Authority and the Registered Entity will retain all the audit records from the previous audit and all audit records submitted since the previous audit, until completion of the next audit. This supports the audit intervals for all entities. The audit data retention period is determined by the audit period for each Registered Entity.** **The phrase, "in conjunction with" was deliberately used to recognize that there may be some confidential records that fall into the category of "critical energy infrastructure information" as defined in the ERO Rules of Procedure – and the responsible entity has the right to retain control over these records. Most other records will be retained by the Compliance Enforcement Authority.**		
TransAlta Centralia Generation, LLC	Yes	
Bonneville Power Administration	Yes	
Consolidated Edison Company of New York, Inc.	No	We agree with the proposed modification, but have suggestions which affect CIP-002 in one area of the Leadership requirement which would be more logical.CIP-002 requires the approval of the Senior Manager for many requirements, and is the standard that determines whether other CIP standards are applicable to the Entity. In order to streamline compliance filing in these cases, and also as a more logical place for the identification of a Senior Manager, we recommend that CIP-002 be updated by 1) moving CIP-003 R2 into CIP-002 or 2) CIP-002 R4 should reference CIP-003 R2. We prefer moving CIP-003 R2 into CIP-002 so that all the Requirements that all Entities must complete are in one Standard.1 - The senior manager has not been identified in CIP-002. Many requirements make

Organization	Yes or No	Question 1 Comment
		reference to the Senior Manager or delegate. Moving CIP-003 R2 into CIP-002 Standard clarifies who the senior manager is, and allows for only one Standard (CIP-002) that must be completed by everyone. This is the preferred option.Or2 - The senior manager or delegate(s) assigned per CIP-003 R2 and its sub-Requirements shall?
Response: **The SDT has received numerous comments related to either referencing CIP-003 R2 within CIP-002 R4 or moving CIP-003 R2 into CIP-002 in order to clarify the reference to the senior manager. Phase 1 of this project includes necessary modifications to CIP-002-1 through CIP-009-1 to comply with the near term specific directives included in FERC Order 706. The issue identified in your comment is an issue better suited for a later phase of this project. The SDT suggests that you review the changes proposed in the later phases of the project and resubmit your comments as appropriate if they have not been addressed.**		
Southern California Edison Company	Yes	
Tampa Electric Company	Yes	
Electric Market Policy	Yes	1) NERC (Step 4.1.10) and Regional Entity (Step 4.1.11) are not defined in the NERC Glossary of Terms or Functional Model. 2) Propose that section 4.2 for each standard (CIP-002-2 through CIP-009-2) be updated to state that law enforcement agencies and emergency services in the performance of their duties are exempt from the standards.
Response: **1) NERC and Regional Entity are defined in NERC's corporate documents including, but not limited to, the Certificate of Incorporation and ByLaws.** **2) Law enforcement agencies and emergency services are not users, owners, or operators of the Bulk Power System; therefore, it is not necessary to exempt them. Their access should be included in the emergency provisions of the cyber security policy as required by the Emergency Situations Provision in CIP-003-R1.1.**		
PPL Corporation	Yes	
MRO NERC Standards	No	The MRO NSRS believes that R4 is prescriptive in nature. The requirement tells how to accomplish, not

Organization	Yes or No	Question 1 Comment
Review Subcommittee		what to accomplish.
Response: **The SDT respectfully disagrees with the comment. CIP-002-2 R4 is a requirement for governance over the critical cyber asset identification standard. The SDT's intent was to define annual approval by the senior manager.**		
Pepco Holdings, Inc - Affiliates	No	We appreciate and support the CSO706 SDT efforts. We agree and support the following proposed changes in CIP-002-2 through CIP-009-2: 1. Nomenclature and clarification changes (e.g. changing RRO to Regional Entity, version references) 2. Clearly state that requirements not only need a program but need to be implemented (e.g. electronic access controls, awareness program, Security Patch Management program) 3. Removed the term "reasonable business judgment" 4. Where applicable, removed the phrase "acceptance of risk" 5. Added annual review and approval of risk-based assessment methodology 6. Background checks and training would be required prior to allowing unescorted physical access or cyber access to critical cyber assets (i.e. eliminates 90 days or 30 days after the fact but allows for emergencies) 7. Added protection of physical access control systems However we have the following questions about changes in CIP-002-2. (These questions also apply to CIP-003-2 through CIP-009-2 but will not be repeated below.): 1). The proposed change for D. Compliance, Section 1.1 appears to add a new term, "Compliance Enforcement Authority", (which we do not believe is in the Glossary of Terms or in any other standards as of 12/1/08). Does the CSO706 SDT plan to define this new term? If yes, how will it be different from the term "Compliance Monitor" (defined in the Glossary of Terms)? 2). In D. Compliance, Section 1.1.2 The proposed change is to replace NERC with ERO. We believe that this should be left as NERC as we do not believe ERO appears in the Glossary of Terms or in any other standards. If ERO remains, does ERO need to be added to the applicability list in A. Introduction, Section 4.1 and the Glossary of Terms?
Response: **1) The term, "Compliance Enforcement Authority" is used extensively in the ERO Rules of Procedure and replaced the term,**		

Organization	Yes or No	Question 1 Comment
"Compliance Monitor." This term has been used in standards under development since November of 2007 to more closely match the language used in the ERO Rules of Procedure – Appendix 4C – Uniform Compliance Monitoring and Enforcement Procedures. **2) Under the ERO Rules of Procedure, the ERO can be penalized but not NERC – therefore the use of the term, "Electric Reliability Organization" or "ERO" is technically correct. As a guideline, drafting teams are asked not to add terms to the glossary unless there is a chance that the term will be misunderstood. In this case, the entities who follow these standards should know what is meant by these terms, and we don't believe the terms need to be added to the glossary.**		
United Illuminating Company	Yes	
Deloitte& Touche, LLP	Yes	
Exelon	Yes	
Old Dominion Electric Cooperative	Yes	
City of Tallahassee (TAL)	Yes	While I agree with the R4 revision, I disagree with the removal of the "reasonable business judgement" in all the standards. While this was in response to FERC directive, it creates a one-size-fits-all approach. Every system is different, as is their Risk Assessment Procedure. This will be one of the more contentious issues. While it may be outside the perview of the SDT, the industry has not been given the information that is needed to specifically address the Auroura fiasco. All we know is someone set up a generator and "hacked" in to change the set frequency and damage ensued. We are not aware of what software was in place to protect this "asset" or what controlling software was. Can the specifics of who set up the test and the hardware/software/control systems being utilized be shared with the industry through a NERC Alert Industry Advisory? While I do not think I have my head buried in the sand about the potential for Cyber attack, I do have a problem with taking all-encompassing action with so little information on what caused the initial knee-jerk reaction. The cost of safeguarding a system against such unknown attacks, to a level that will be acceptable during an audit (a second unknown) will surely be a significant burden to many utilities. While entities have some latitude in our "methodology" in identifying Critical Assets, the fact will remain that you have to spend money on new tools and hardware to comply with the existing requirements outside of routine budget cycles at a significant impact to operations. According to the letter from Rick

Organization	Yes or No	Question 1 Comment
		Sergel to the BOT of July 7, 2008 even after we spend a ton of money, we are still susceptible to attack. Without the flexibility of determining cost vs. benefit, we will overachieve the goal of ".. .reasonably ensure the reliability of the BPS. . ."
Response: **The comments concerning Aurora are outside of the aegis of the SDT.** **The removal of "reasonable business judgment" was done in accordance with FERC Order 706. The revisions made to the standards in Phase 1 are intended to be responsive to specific FERC directives relevant to the onset of compliance audits in July 2009. The expansion of the Technical Feasibility Exception Process should address the concerns regarding the removal of reasonable business judgment and acceptance of risk.**		
BC Transmission Corporation	Yes	
Applied Control Solutions, LLC	No	Need to include the NIST Framework in addition to senior management approval
Response: **The SDT plans to consider the NIST Framework during future phases of standards review, as directed by FERC Order 706.**		
US Bureau of Reclamation	No	The modification of the standard to require that a specific individual approve the risk-assessment methodology appears to be overstepping the bounds of the authority of the regulatory agencies as it pertains to improved reliability. It is difficult to imagine or prove that having one individual within an agency approve a methodology (as opposed to making the entity responsible for having and using a methodology) improves system reliability. Such a requirement is also not consistent with most of the other BES reliability standards. For consistency, the standard should refer to "Responsible Entity" rather than specific individuals within the organization. That determination is the sole discretion of the Responsible Entity and was not required by FERC. FERC required, in paragraph 236, that "internal, management, approval of the riskbased assessment" is required. FERC further clarified: "A responsible entity, however, remains responsible to identify the critical assets on its system". To that end the standard should require that the 'Responsible Entity" ensure that management has approved the risk based assessment. The "Responsible Entity" is then responsible to demonstrate that the requirement has been met and who approved it.

Organization	Yes or No	Question 1 Comment
Response: **The intent of the standard is not to define an entity's organizational structure. The intent is to ensure that the appropriate governance structure is taken into consideration and that, as directed by FERC, there exists a single individual with overarching authority.**		
Orange and Rockland Utilities Inc.	No	We recommend that CIP-002 be updated by 1) moving CIP-003 R2 into CIP-002 or 2) CIP-002 R4 should reference CIP-003 R2. We prefer moving CIP-003 R2 into CIP-002 so that all the Requirements that all Entities must complete are in one Standard.1 – The senior manager has not been identified in CIP-002. Moving CIP-003 R2 into CIP-002 Standard clarifies who the senior manager is, and allows for only one Standard (CIP-002) that must be completed by everyone.2 - The senior manager or delegate(s) assigned per CIP-003 R2 and its sub-Requirements shall?
Response: **The SDT has received numerous comments related to either referencing CIP-003 R2 within CIP-002 R4 or moving CIP-003 R2 into CIP-002 in order to clarify the reference to the senior manager. Phase 1 of this project includes necessary modifications to CIP-002-1 through CIP-009-1 to comply with the near term specific directives included in FERC Order 706. The issue identified in your comment is an issue better suited for a later phase of this project. The SDT suggests that you review the changes proposed in the later phases of the project and resubmit your comments as appropriate if they have not been addressed.**		
CenterPoint Energy		
Manitoba Hydro	Yes	
Alberta Electric System Operator	No	The functional entity (e.g. the Balancing Authority, etc) should be designated as the responsible entity for this requirement, not an individual. This would be consistent with other ERO standards. Also, R1 implies that the purpose of this standard is not only to identify the "Critical Cyber Assets" but also the "Critical Assets" (which must be done before you can identify the Critical Cyber Assets), and hence we suggest that either the identification of "critical Assets" be specified in its own and separate standard or the Title and Purpose of CIP-002 be clarified to state that there are 2 purposes to this standard. We suggest that R1 should be re-written to improve clarity. R1, as currently written, contains not only a single requirement, but with at least two, and possibly three or more requirements embedded in it. The accountabilities for these different requirements could be different within an organization, so assigning them to one person would be inappropriate.

Organization	Yes or No	Question 1 Comment
Response: **The change made in CIP-002 includes adding the management approval of the risk-based assessment methodology per directives in FERC Order 706. Given the limited scope and timeline for Phase 1, please readdress the additional concerns during the Phase 2 comment period.**		
Dynegy	No	Agree with requiring management approval of the risk-based assessment methodology. Also, suggest moving CIP-003, R2 into CIP-002 so that all the Requirements that all Entities must comply with are in one Standard.
Response: **The SDT has received numerous comments related to either referencing CIP-003 R2 within CIP-002 R4 or moving CIP-003 R2 into CIP-002 in order to clarify the reference to the senior manager. Phase 1 of this project includes necessary modifications to CIP-002-1 through CIP-009-1 to comply with the near term specific directives included in FERC Order 706. The issue identified in your comment is an issue better suited for a later phase of this project. The SDT suggests that you review the changes proposed in the later phases of the project and resubmit your comments as appropriate if they have not been addressed.**		
Northern Indiana Public Service Company	No	I do support the recommended change to require management approval of the risk-based assessment methodology per FERC Order 706, paragraph 236. I would like to recommend the addition of some language to CIP-002-2 Req 4. Currently the language in R4 directs the responsible entity to comply with CIP-002-2 R1-R3 and retain a record of the resulting CA and CCA asset list (even if that list is null). My concern is that if the list is null the entity may feel they have completed all necessary actions for compliance. There is however compliance actions for an entity with a null list contained within CIP-003-2. As it stands there is an oddly placed exemption in the applicability section of CIP-003 4.2.3. I would recommend the inclusion of language in CIP-002-2 Req. 4 to identify the need for compliance with CIP-003-2 R2 as well as the currently referenced CIP-002-2 R1-3; in order to contain all applicability for CIP-002-2 R4 in one location and in turn removing the exemption in CIP-003-2. As there is no other means through the use of this comment form I would also like to comment on changes made in CIP-002-2 that repeat throughout CIP-002-2 - CIP-009-2 In the purpose section of CIP-002-2, I would like to see as a component of this draft, an attempt to develop alternative language to replace reasonable business judgment as mentioned in Order 706 in paragraph 135. In the Data Retention section of CIP-002-2, I would like to request clarification on the language added to 1.4.2. As the language was there was a limit on data retention that matched the audit enforcement

Organization	Yes or No	Question 1 Comment
		period of three years. The language provided currently removes this limit and extends the retention into perpetuity as well as leaving it unclear which entity is responsible for retaining the data into perpetuity.

Response:

The SDT has received numerous comments related to either referencing CIP-003 R2 within CIP-002 R4 or moving CIP-003 R2 into CIP-002 in order to clarify the reference to the senior manager. Phase 1 of this project includes necessary modifications to CIP-002-1 through CIP-009-1 to comply with the near term specific directives included in FERC Order 706. The issue identified in your comment is an issue better suited for a later phase of this project. The SDT suggests that you review the changes proposed in the later phases of the project and resubmit your comments as appropriate if they have not been addressed.

The removal of "reasonable business judgment" was done in accordance with FERC Order 706. The revisions made to the standards in Phase 1 are intended to be responsive to specific FERC directives relevant to the onset of compliance audits in July 2009. The expansion of the Technical Feasibility Exception Process should address the concerns regarding the removal of reasonable business judgment and acceptance of risk.

The data retention periods for the standard requirements are specified in the standards. The language of 1.4.2 indicates that the Compliance Enforcement Authority and the Registered Entity will retain all the audit records from the previous audit and all audit records submitted since the previous audit, until completion of the next audit. This supports the audit intervals for all entities. The audit data retention period is determined by the audit period for each Registered Entity.

CoreTrace	Yes	
Oncor Electric Delivery LLC	Yes	
Illinois Municipal Electric Agency	Yes	
Ontario Power Generation	No	Measures M2 and M3 add a requirement by specifying the lists of Critical Assets and Critical Cyber Assets must be dated. M2 references Requirement R2 and M3 references Requirement R3. Neither R2 or R3 require a list to be dated.

Response: **Phase 1 of this project includes necessary modifications to CIP-002-1 through CIP-009-1 to comply with the near term specific directives included in FERC Order 706. The issue identified in your comment is an issue better suited for a later phase of this project. The SDT suggests that you review the changes proposed in the later phases of the project and resubmit your comments as appropriate if they have not been addressed.** **The word "dated" will be removed at this time. The measures will be reviewed and considered in an upcoming drafting phase of these standards.**		
American Electric Power	Yes	Section R4 of the Requirements category does not clearly define what type of unit the senior manager represents. We would suggest a clarifying comment like "for each responsible entity" be added following the word "delegate(s)." This does not appear again in any of the following standards. However, throughout all of these standards, the drafting team has introduced a new term in its use of "Responsible Entity." If this term is to be used, it should probably be considered by the NERC organization with corresponding updates to lists of compliance term glossaries and/or definitions.
Response: **The SDT believes that this change could be too prescriptive and limits the flexibility allowed in delegation.** **"Responsible Entity" is defined within the Applicability section of each CIP standard.**		
Ontario IESO	No	Standards should hold a functional entity(ies) responsible for meeting the requirements, not a person or a position. Furthermore, delegation is an internal process which does not need to be explicitly mentioned/allowed in a standard. We propose R4 be revised to: "Annual Approval? The Responsible Entity shall appoint a senior manager with the authority to approve annually the risk-based assessment methodology, the list of Critical Assets and the list of Critical Cyber Assets. Based on Requirements R1, R2, and R3, the Responsible Entity may determine that it has no Critical Assets or Critical Cyber Assets. The Responsible Entity shall keep a signed and dated record of its approval of the risk-based assessment methodology, the list of Critical Assets and the list of Critical Cyber Assets (even if such lists are null.) "If appointing a senior manager is required to ensure standards are complied with and implemented, we recommend that CIP-002 be updated by 1) moving CIP-003 R2 into CIP-002 or 2) CIP-002 R4 should explicitly reference CIP-003 R2. We prefer moving CIP-003 R2 into CIP-002 so that all the Requirements that all Entities must complete are in one Standard.

Response: **The SDT has received numerous comments related to either referencing CIP-003 R2 within CIP-002 R4 or moving CIP-003 R2 into CIP-002 in order to clarify the reference to the senior manager. Phase 1 of this project includes necessary modifications to CIP-002-1 through CIP-009-1 to comply with the near term specific directives included in FERC Order 706. The issue identified in your comment is an issue better suited for a later phase of this project. The SDT suggests that you review the changes proposed in the later phases of the project and resubmit your comments as appropriate if they have not been addressed.** **The senior manager is held responsible to ensure that there is a clear line of authority and that cyber security functions are given the prominence they deserve. The SDT believes that delegation needs to be addressed in the CIP standards to ensure that the appropriate governance structure is considered by the Responsible Entity.**		
Ameren	Yes	None.
Response: **Thank you for your comment.**		
Consumers Energy Company	Yes	
Xcel Energy	Yes	
ISO New England Inc	No	1) - We recommend that CIP-002 be updated by: moving CIP-003 R2 into CIP-002 or CIP-002 R4 should explicitly reference CIP-003 R2. We prefer moving CIP-003 R2 into CIP-002 so that all the Requirements that all Entities must complete are in one Standard. Rational: 2) - The senior manager has not been identified in CIP-002. Moving CIP-003 R2 into CIP-002 Standard clarifies who the senior manager is, and allows for only one Standard (CIP-002) that must be completed by everyone. Allows for, "The senior manager or delegate(s) assigned per CIP-003 R2 and its sub-Requirements" shall" 3. In this Standard and throughout several other CIP Standards, "Dated" is used only in the Measures. Adding a requirement in the measures is inappropriate and cannot be applied.
Response: **1) The SDT has received numerous comments related to either referencing CIP-003 R2 within CIP-002 R4 or moving CIP-003 R2 into CIP-002 in order to clarify the reference to the senior manager. Phase 1 of this project includes necessary modifications to CIP-002-1 through CIP-009-1 to comply with the near term specific directives included in FERC Order 706. The issue identified in your comment is an issue better suited for a later phase of this project. The SDT suggests that you review the changes proposed in**		

the later phases of the project and resubmit your comments as appropriate if they have not been addressed. **2) The senior manager is held responsible in order to ensure that there is a clear line of authority and that cyber security functions are given the prominence they deserve. The SDT believes that delegation should be addressed in the CIP standards to ensure that the appropriate governance structure is considered by the Responsible Entity.** **3) Phase 1 of this project includes necessary modifications to CIP-002-1 through CIP-009-1 to comply with the near term specific directives included in FERC Order 706. The issue identified in your comment is an issue better suited for a later phase of this project. The SDT suggests that you review the changes proposed in the later phases of the project and resubmit your comments as appropriate if they have not been addressed.** **The word "dated" will be removed at this time. The measures will be reviewed and considered in an upcoming drafting phase of these standards.**		
American Transmission Company	Yes	
TVA	No	There are three areas we feel need clarification: 1. Standards should hold a functional entity(ies), not a person or a position, responsible for meeting the requirements; 2. Delegation is an internal process which does not need to be explicitly mentioned/allowed in a standard; and 3. An appointment of a senior manager is a part of CIP-003 and for Responsible Entities without Critical Assets only CIP-002 is applicable. We propose the following: i) R4 be revised to: Annual Approval - The Responsible Entity shall appoint a senior manager with the authority to approve annually the risk-based assessment methodology, the list of Critical Assets and the list of Critical Cyber Assets. Based on Requirements R1, R2, and R3, the Responsible Entity may determine that it has no Critical Assets or Critical Cyber Assets. ii) The Responsible Entity shall keep a signed and dated record of its approval of the risk-based assessment methodology, the list of Critical Assets and the list of Critical Cyber Assets (even if such lists are null.) iii. Move the senior manager appointment from CIP-003 R2 to CIP-002. Incorporate, by reference to CIP-003, for a senior manager appointment into CIP-002.
Response:		

i) The SDT has received numerous comments related to either referencing CIP-003 R2 within CIP-002 R4 or moving CIP-003 R2 into CIP-002 in order to clarify the reference to the senior manager. Phase 1 of this project includes necessary modifications to CIP-002-1 through CIP-009-1 to comply with the near term specific directives included in FERC Order 706. The issue identified in your comment is an issue better suited for a later phase of this project. The SDT suggests that you review the changes proposed in the later phases of the project and resubmit your comments as appropriate if they have not been addressed. (Reference FERC Order 706 Paragraph 381) **ii) The senior manager is held responsible in order to ensure that there is a clear line of authority and that cyber security functions are given the prominence they deserve. The SDT believes that delegation should be addressed in the CIP standards to ensure that the appropriate governance structure is considered by the Responsible Entity. (reference FERC Order 706, Paragraph 381)** **iii) As stated in CIP-003-2, all Responsible Entities regardless of a null Critical Cyber Asset list are required to perform CIP003-2 R2.**		
Duke Energy	Yes	
Brazos Electric Power Cooperative, Inc.	No	Suggest that the first sentence of R4 be re-written as follows: R4 The Responsible Entity shall assign a single senior manager with overall responsibility and authority for approving annually the risk-based assessment methodology, the list of Critical Assets and the list of Critical Cyber Assets.
Response: **The SDT has received numerous comments related to either referencing CIP-003 R2 within CIP-002 R4 or moving CIP-003 R2 into CIP-002 in order to clarify the reference to the senior manager. Phase 1 of this project includes necessary modifications to CIP-002-1 through CIP-009-1 to comply with the near term specific directives included in FERC Order 706. The issue identified in your comment is an issue better suited for a later phase of this project. The SDT suggests that you review the changes proposed in the later phases of the project and resubmit your comments as appropriate if they have not been addressed.**		
Progress Energy	Yes	
Standards Review Committee of ISO/RTO Council	No	(1) Standards should hold a functional entity(ies), not a person or a position, responsible for meeting the requirements. Further, delegation is an internal process which does not need to be explicitly mentioned/allowed in a standard. We propose R4 be revised to: "Annual Approval — The Responsible Entity shall appoint a senior manager with the authority to approve annually the risk-based assessment methodology, the list of Critical Assets and the list of Critical Cyber Assets. Based on Requirements R1, R2, and R3, the Responsible Entity may determine that it has no Critical Assets or Critical Cyber Assets. The Responsible Entity shall keep a signed and dated record of its approval of the risk-based assessment methodology, the list of Critical Assets and the list of Critical Cyber Assets (even if such lists are null.)" If appointing a senior mangager is required to ensure standards are complied with and implemented, we recommend that CIP-002 be updated by 1) moving CIP-003 R2 into CIP-002 or 2) CIP-002 R4 should

		explicitly reference CIP-003 R2. We prefer moving CIP-003 R2 into CIP-002 so that all the Requirements that all Entities must complete are in one Standard. (2) In this Standard and throughout several other CIP Standards, "Dated" is used only in the Measures. Adding a requirement in the measures is inappropriate and cannot be applied.
Response: **(1) The senior manager is held responsible in order to ensure that there is a clear line of authority and that cyber security functions are given the prominence they deserve. The SDT believes that delegation should be addressed in the CIP standards to ensure that the appropriate governance structure is considered by the Responsible Entity.** **The SDT has received numerous comments related to either referencing CIP-003 R2 within CIP-002 R4 or moving CIP-003 R2 into CIP-002 in order to clarify the reference to the senior manager. Phase 1 of this project includes necessary modifications to CIP-002-1 through CIP-009-1 to comply with the near term specific directives included in FERC Order 706. The issue identified in your comment is an issue better suited for a later phase of this project. The SDT suggests that you review the changes proposed in the later phases of the project and resubmit your comments as appropriate if they have not been addressed.** **(2) The word "dated" will be removed at this time. The measures will be reviewed and considered in an upcoming drafting phase of these standards.**		
KEMA	Yes	
Austin Energy	Yes	
Kansas City Power & Light	Yes	
San Diego Gas and Electric Co.	Yes	

2. The CSO706 SDT is proposing the following modifications to **CIP-003-1**:

   - Revise Applicability 4.2.3 to specify that compliance with Requirement R2 applies to Responsible Entities that have determined they have no Critical Cyber Assets (per FERC Order 706, paragraph 376)
   - Clarify the intent of the Requirement R2 on Leadership that a senior manager be assigned with the overall responsibility and authority for cyber security matters (per FERC Order 706, paragraph 381).
   - Add Requirement R2.3 to address senior manager delegation of authority for specific actions to a named delegate.
   - Renumber the original R2.3 to R2.4.
   - Delete the phrase "or a statement accepting risk" from Requirement R3.2.(per FERC Order 706, paragraph 376)

   Do you agree with the proposed modifications? If not, please explain and provide an alternative to the proposed modification that would eliminate or minimize your disagreement.

Summary Consideration:

Organization	Yes or No	Question 2 Comment
Detroit Edison Company	Yes	
PacifiCorp	No	Suggested modification to R2.3"Where allowed by Standards CIP-002-2 through CIP-009-2, the senior manager may delegate authority for specific actions assigned to the senior manager to a named delegate or delegates."
Response: **The SDT received a number of comments that suggested clarifications to the delegation in CIP-003-2 R2.3. The SDT discussed this specific language and did not agree that it provided clarity over the posted language in the delegation requirement.**		
FirstEnergy Corp	Yes	
MidAmerican Energy Company	No	Suggest an addition: The senior may delegate authority for actions assigned to the senior manager in Standards CIP-002-2 through CIP-009-2 to a named delegate or delegates. These delegations shall be documented in the same manner as R2.1 and R2.2, and approved by the senior manager.

Organization	Yes or No	Question 2 Comment
Response: **The SDT believes that the senior manager should annually approve, without delegation, the Cyber Security Policy. As indicated in R2.3, delegation is only allowed where specifically stated in the requirement. Consequently, there is no delegation allowed in the approval of the Cyber Security Policy.**		
Northeast Power Coordinating Council	No	1 - We recommend moving CIP-003 R2 into the CIP-002 Standard. 2 - We request clarification of CIP-003 R2. 3 "the senior manager may delegate authority for specific actions to a named delegate or delegates." Please clarify a) the named delegate(s) and b) the delegation.
Response: **1.-2. The SDT has received numerous comments related to either referencing CIP-003 R2 within CIP-002 R4 or moving CIP-003 R2 into CIP-002 in order to clarify the reference to the senior manager. Phase 1 of this project includes necessary modifications to CIP-002-1 through CIP-009-1 to comply with the near term specific directives included in FERC Order 706. The issue identified in your comment is an issue better suited for a later phase of this project. The SDT suggests that you review the changes proposed in the later phases of the project and resubmit your comments as appropriate if they have not been addressed.** **3, The SDT believes that the clarifications requested regarding who a delegate is and how a delegation is performed should be determined by the entity, and the SDT does not intend to prescribe a delegation process.**		
WECC Reliability Coordination	Yes	
Southern Company	Yes	CIP-003 Section D - Compliance: 1.1.1 does not specify who is responsible for the enforcement authority. CIP-003 Section D - Compliance: 1.4.1 - Indefinite retention is not feasible, overall cost of storage depending on scope could potentially be very large. Item should define an upper bound of the request (e.g. a maximum of 3 years) CIP-003 Section D - Compliance: 1.4.2 - Should have a time limit to reduce the overall liability of confidential information.

Organization	Yes or No	Question 2 Comment
Response: **1.1.1 - The Regional Entity will serve as the Compliance Enforcement Authority for most entities. As the Regional Entity may not audit itself, the ERO will serve as the Compliance Enforcement Authority in auditing the Regional Entity. A third-party monitor without a vested interest in the outcome will serve as the Compliance Enforcement Authority for NERC. (Refer to NERC's Rules of Procedure, Paragraphs 404 and 405).** **1.4.1 – With the exception of retaining evidence in support of an investigation, the standard defines a finite retention period. The language that indicates the Compliance Enforcement Authority may direct the responsible entity to retain evidence for a longer period of time as part of an investigation is a restatement of what is included in the ERO Rules of Procedure. Reference the ERO Rules of Procedure Appendix 4C – Uniform Compliance Monitoring and Enforcement Procedures – Section 3.4.1 Compliance Violation Investigation Process Steps. While the duration of an investigation cannot be predicted, further clarification of the retention timeframe is outside the scope of the SDT.** **1.4.2 – This language supports the regularly scheduled audit intervals for all entities and supports the need to retain the confidentiality of some data. The audit data retention period is determined by the audit period for each Registered Entity.**		
Luminant Power	Yes	
Encari	No	Also see comments on Question 1 pertaining to exemption 4.2.3--General Comments Provided in All Submissions--Other modifications were also made to this standard that are not included as part of the question. 1. The wording of 1.1.1 is awkward and should be modified. 2. We also request further clarification regarding the Data Retention Requirement 1.4.2 as to which entity will be maintaining the last audit records and submitted subsequent audit records. 3. As the statement is currently worded "in conjunction" leaves this open to interpretation.
Response: **1. The intent of the wording in 1.1.1 is to clarify which entity will serve as the Compliance Enforcement Authority. For most standards, the Regional Entity serves as the Compliance Enforcement Authority and audits the performance of the Reliability Coordinator, Transmission Operator, Balancing Authority, Generator Operator, Generator Owner, etc. In this standard, the Regional Entity is responsible for some of the requirements – but an entity cannot audit its own performance. Where the Regional Entity is also the responsible entity, the ERO will audit the Regional Entity's performance. Where the ERO is the responsible entity, a third-party monitor without vested interest in the outcome will conduct the audit.** **2. The data retention periods for the standard requirements are specified in the standards. The language of 1.4.2 indicates that the**		

Organization	Yes or No	Question 2 Comment
Compliance Enforcement Authority and the Registered Entity will retain all the audit records from the previous audit and all audit records submitted since the previous audit, until completion of the next audit. This supports the audit intervals for all entities. The audit data retention period is determined by the audit period for each Registered Entity. **3. The phrase, "in conjunction with" was deliberately used to recognize that there may be some confidential records that fall into the category of "critical energy infrastructure information" as defined in the ERO Rules of Procedure – and the responsible entity has the right to retain control over these records. Most other records will be retained by the Compliance Enforcement Authority.**		
TransAlta Centralia Generation, LLC	Yes	
Bonneville Power Administration	Yes	
Consolidated Edison Company of New York, Inc.	No	1) - We recommend moving CIP-003 R2 into the CIP-002 Standard. (See comments to Question 1). 2) - We request clarification of CIP-003 R2. 3) -"the senior manager may delegate authority for specific actions to a named delegate or delegates." 4)- Please clarify a) the named delegate(s) (e.g. does he/she have to be a senior manager?) and b) the requirements for what the delegation must contain (i.e. does it have to explicitly reference the standard and requirement?)
Response: **1)-3) The SDT has received numerous comments related to either referencing CIP-003 R2 within CIP-002 R4 or moving CIP-003 R2 into CIP-002 in order to clarify the reference to the senior manager. Phase 1 of this project includes necessary modifications to CIP-002-1 through CIP-009-1 to comply with the near term specific directives included in FERC Order 706. The issue identified in your comment is an issue better suited for a later phase of this project. The SDT suggests that you review the changes proposed in the later phases of the project and resubmit your comments as appropriate if they have not been addressed.** **4) The SDT believes that the clarifications requested regarding who a delegate is and how a delegation is performed should be determined by the entity, and the SDT does not intend to prescribe a delegation process.**		
Southern California Edison Company	No	R1.3 - Add language to indicate whether Senior Manager may or may not delegate annual review and approval of the policy.R3.2 - SCE believes that the removal of "acceptance of risk" limits SCE's ability to analyze risk and determine a proper response. For example, SCE could determine that the residual risk

Organization	Yes or No	Question 2 Comment
		posed by the state of maturity of a technology used to address CIP requirements is both low risk and low probability. Removing the acceptance of risk language would require SCE to continue to allocate time and resources to address the residual risk rather than deeming it acceptable within the CIP Standards. SCE recommends adding language to indicate that where unavoidable residual risk remains after remediation, it must be documented and authorized by the Senior Manager or delegate.
Response: **The SDT believes that the senior manager should annually approve, without delegation, the Cyber Security Policy. As indicated in R2.3, delegation is only allowed where specifically stated in the requirement. Consequently, there is no delegation allowed in the approval of the Cyber Security Policy.** **FERC has directed the ERO to have the technical feasibility exception process supersede all instances of acceptance of risk. Where requirements cannot be met due to technical, safety, or operational limitations, those limitations are to be treated and documented according to a technical feasibility exception process. [Please refer to FERC 706, Paragraph 151]**		
Tampa Electric Company	No	Regarding the removal of the language in Section 1.5 : Additional Compliance Information: It is not clear if removal of this language is implying that authorized exceptions result in non-compliance. There are situations where requirements of this standard cannot be met, particularly for legacy equipment and associated vendor supplied systems. The following language should be reinstated in the standard: "Duly authorized exceptions will not result in non-compliance."
Response: **Situations where the standards requirements cannot be met will be handled through the Technical Feasibility Exception process under the NERC Rules of Procedure. The technical feasibility exception process will address the requirements for documenting, approving, and remediating the exception. Any sanction decisions will arise from the TFE process. It is not appropriate to assert that "duly authorized exceptions will not result in non-compliance" within Section D-1.5 of the standard.**		
Electric Market Policy	Yes	1) NERC (Step 4.1.10) and Regional Entity (Step 4.1.11) are not defined in the NERC Glossary of Terms or Functional Model. 2) Suggest R3.1 read thirty calendar days.
Response: **1) NERC and Regional Entity are defined in NERC's corporate documents including, but not limited to, the Certificate of Incorporation and ByLaws.**		

Organization	Yes or No	Question 2 Comment
2) Phase 1 of this project includes necessary modifications to CIP-002-1 through CIP-009-1 to comply with the near term specific directives included in FERC Order 706. The issue identified in your comment is an issue better suited for a later phase of this project. The SDT suggests that you review the changes proposed in the later phases of the project and resubmit your comments as appropriate if they have not been addressed.		
PPL Corporation	Yes	
MRO NERC Standards Review Subcommittee	No	The MRO NSRS believes the R2 should be moved to CIP-002. This would package all of the requirements in one standard the apply to every entitiy. The senior may delegate authority for actions assigned to the senior manager in Standards CIP-002-2 through CIP-009-2 to a named delegate or delegates. These delegations shall be documented in the same manner as R2.1 and R2.2, and approved by the senior manager.
Response: **The SDT has received numerous comments related to either referencing CIP-003 R2 within CIP-002 R4 or moving CIP-003 R2 into CIP-002 in order to clarify the reference to the senior manager. Phase 1 of this project includes necessary modifications to CIP-002-1 through CIP-009-1 to comply with the near term specific directives included in FERC Order 706. The issue identified in your comment is an issue better suited for a later phase of this project. The SDT suggests that you review the changes proposed in the later phases of the project and resubmit your comments as appropriate if they have not been addressed.** **The SDT believes that the senior manager should annually approve, without delegation, the Cyber Security Policy. As indicated in R2.3, delegation is only allowed where specifically stated in the requirement. Consequently, there is no delegation allowed in the approval of the Cyber Security Policy.** **The SDT received a number of comments that suggested clarifications to the delegation in CIP-003-2 R2.3. The SDT discussed this specific language and did not agree that it provided clarity over the posted language in the delegation requirement.**		
Pepco Holdings, Inc - Affiliates	Yes	We support the proposed modifications including the removal of business phone and business address from B. Requirements, R2.1. Similary, should the business phone requirement be removed from B. Requirements, R5.1.1 - Similar to CIP-002-2, D. Compliance, Section 1.5, should CIP-003-2, D. Compliance, Section 1.5 say "None"?
Response: **Thank you for identifying the inconsistency. Section 1.5 should state, “None”, and “Business phone” in R5.1.1 will be removed.**		
United Illuminating	Yes	

Organization	Yes or No	Question 2 Comment
Company		
Deloitte& Touche, LLP	Yes	
Exelon	Yes	
Old Dominion Electric Cooperative	Yes	
City of Tallahassee (TAL)	Yes	Although the "acceptance of risk" ties in with the discusson above on business judgement.
Response: **The removal of "reasonable business judgment" was done in accordance with FERC Order 706. The revisions made to the standards in Phase 1 are intended to be responsive to specific FERC directives relevant to the onset of compliance audits in July 2009. The expansion of the Technical Feasibility Exception Process should address the concerns regarding the removal of reasonable business judgment and acceptance of risk.**		
BC Transmission Corporation	Yes	
Applied Control Solutions, LLC	Yes	
US Bureau of Reclamation	No	The reference to a senior manager in paragraph 381 was not intended be a requirement. FERC did allow registered entities some flexibility, to wit: "The Commission adopts its CIP NOPR interpretation that Requirement R2 of CIP-003-1 requires the designation of a single manager who has direct and comprehensive responsibility and accountability for implementation and ongoing compliance with the CIP Reliability Standards. The Commission's intent is to ensure that there is a clear line of authority and that cyber security functions are given the prominence they deserve". The modification by the SDT, which specifies delegation by the "senior manager", is intrusive upon the Responsible Entity's organizational structure. It is sufficient to require that the Responsible Entity must be able to produce documentation of who has responsibility for the CIP implementation. For geographically diverse organizations, that responsibility will change depending on the location of the affected systems. Each Responsible Entity generally has identified an individual who is authorized to submit documentation in response to a Regional Entity's requests or through the certification process. The specific requirement

Organization	Yes or No	Question 2 Comment
		that the senior manager have the authority of leading and managing CIP is not the same as requiring certification and may not fit with the organizational lines of the Responsible Entity. Organizational structures must not be legislated in industry standards, especially when the organizations have a vast array of responsibilities and authorities that govern their function. Reclamation has functional responsibilities delegated to Regional Directors in order to manage the vast array of legislated mandates. To require Reclamation to alter its organizational structure in no way improves the reliability of the BES and the requirement appears arbitratry. Each entity certifies that it complies with the integrity of its security through one individual who is authorized to speak for the agency. The requirements should focus on the desired performance outcome which is needed to maintain reliability of the power system, not how the performance is accomplished.
Response: **The SDT believes that R2.3 provides Responsible Entities the flexibility to meet the leadership requirements without prescribing organizational changes.**		
Orange and Rockland Utilities Inc.	No	1) We recommend moving CIP-003 R2 into the CIP-002 Standard. 2) We request clarification of CIP-003 R2. 3) “the senior manager may delegate authority for specific actions to a named delegate or delegates." Please clarify a) the named delegate(s) (e.g. does he/she have to be a senior manager?) and b) the delegation (i.e. does it have to explicitly reference the standard and requirement?)
Response: **The SDT has received numerous comments related to either referencing CIP-003 R2 within CIP-002 R4 or moving CIP-003 R2 into CIP-002 in order to clarify the reference to the senior manager. Phase 1 of this project includes necessary modifications to CIP-002-1 through CIP-009-1 to comply with the near term specific directives included in FERC Order 706. The issue identified in your comment is an issue better suited for a later phase of this project. The SDT suggests that you review the changes proposed in the later phases of the project and resubmit your comments as appropriate if they have not been addressed.** **The SDT believes that the clarifications requested regarding who a delegate is and how a delegation is performed should be determined by the entity, and the SDT does not intend to prescribe a delegation process.**		
CenterPoint Energy		
Manitoba Hydro	No	In CIP-003 R2.3 the assignment to delegate authority could be done specifically or by assignment through the entitities policies. It should not be necessary to perform specific delegation for all

Organization	Yes or No	Question 2 Comment
		circumstances which necessitates additional overhead for maintaining such documentation of delegation from the senior manager. The webinar on the revisions to the CIP Standards and other recent discussions mentioned the possible creation of a new process for instances when the phrase "where technically feasible" is applied. These instances might also be exceptions to a responsible entity's cyber security policies. Any new process dealing with "where technically feasible" must be supported by additional requirements(s) in the CIP Standards. Responsible Entities should be given direction in the CIPC Standards for identifying, documenting, managing and approving internally these instances. An additional requirement based on CIP-003-1 R3 Exceptions would provide the required direction for industry. Additional requirement(s) must included prior to further industry commenting or balloting on revised CIP Standards or before any new industry process is implemented for "where technically feasible".
Response: **The SDT believes that the clarifications requested regarding how a delegation is performed should be determined by the entity and does not intend to prescribe a delegation process. There is no requirement to delegate.** **The Technical Feasibility Exception process is under development by NERC staff. Please readdress this issue during the Phase 2 comment period.**		
Alberta Electric System Operator	Yes	However, we would like to comment that the responsibility for meeting requirements in standards must lie with the functional entity, not an individual within the entity. Also, we don't believe details on how delegation is done within an entity should be included in a standard. We propose R4 be revised to: "Annual Approval". The Responsible Entity shall appoint a senior manager with the authority to approve annually the risk-based assessment methodology, the list of Critical Assets and the list of Critical Cyber Assets. Based on Requirements R1, R2, and R3, the Responsible Entity may determine that it has no Critical Assets or Critical Cyber Assets. The Responsible Entity shall keep a signed and dated record of its approval of the risk-based assessment methodology, the list of Critical Assets and the list of Critical Cyber Assets (even if such lists are null).
Response: **The senior manager is held responsible in order to ensure that there is a clear line of authority and that cyber security functions are given the prominence they deserve. The intent of the SDT is to uphold the directive from Paragraph 381 of FERC Order 706 which clarifies that the senior manager is not a user, owner, or operator of the Bulk Power System who is personally subject to civil penalties pursuant to Section 215 of FPA. The SDT believes that delegation should be addressed in the CIP standards in order to ensure that the appropriate governance structure is considered by the Responsible Entity.** **We have received numerous comments related to either referencing CIP-003 R2 within CIP-002 R4 or moving CIP-003 R2 into CIP-002**		

Organization	Yes or No	Question 2 Comment
in order to clarify the reference to the senior manager. Phase 1 of this project includes necessary modifications to CIP-002-1 through CIP-009-1 to comply with the near term specific directives included in FERC Order 706. The issue identified in your comment is an issue better suited for a later phase of this project. The SDT suggests that you review the changes proposed in the later phases of the project and resubmit your comments as appropriate if they have not been addressed.		
Dynegy	No	Agree with proposed modifications except recommend moving CIP-003, R2 into the CIP-002 Standard (see comment on Item #1).
Response: **The SDT has received numerous comments related to either referencing CIP-003 R2 within CIP-002 R4 or moving CIP-003 R2 into CIP-002 in order to clarify the reference to the senior manager. Phase 1 of this project includes necessary modifications to CIP-002-1 through CIP-009-1 to comply with the near term specific directives included in FERC Order 706. The issue identified in your comment is an issue better suited for a later phase of this project. The SDT suggests that you review the changes proposed in the later phases of the project and resubmit your comments as appropriate if they have not been addressed.**		
Northern Indiana Public Service Company	No	As stated in question 1 I believe the revised applicability in CIP-003-2 section 4.2.3 is oddly placed as an entity could read CIP-002-2 in entirety and feel that the resulting null asset list excludes the entity from any other CIP standards. If a single requirement also applies to an entity that has a resulting null list, I believe it is better to call out the additional requirement within CIP-002-2 R4 rather than adding revised applicability language to CIP-003-2.
Response: **The SDT has received numerous comments related to either referencing CIP-003 R2 within CIP-002 R4 or moving CIP-003 R2 into CIP-002 in order to clarify the reference to the senior manager. Phase 1 of this project includes necessary modifications to CIP-002-1 through CIP-009-1 to comply with the near term specific directives included in FERC Order 706. The issue identified in your comment is an issue better suited for a later phase of this project. The SDT suggests that you review the changes proposed in the later phases of the project and resubmit your comments as appropriate if they have not been addressed.**		
CoreTrace	Yes	
Oncor Electric Delivery LLC	Yes	
Illinois Municipal Electric Agency	No	IMEA agrees with the intent of the proposed modifications, but recommends they be incorporated into CIP-002-1 (instead of CIP-003-1) modifications for clarification of applicability regardless of Critical

Organization	Yes or No	Question 2 Comment
		Cyber Asset identification.
Response: **The SDT has received numerous comments related to either referencing CIP-003 R2 within CIP-002 R4 or moving CIP-003 R2 into CIP-002 in order to clarify the reference to the senior manager. Phase 1 of this project includes necessary modifications to CIP-002-1 through CIP-009-1 to comply with the near term specific directives included in FERC Order 706. The issue identified in your comment is an issue better suited for a later phase of this project. The SDT suggests that you review the changes proposed in the later phases of the project and resubmit your comments as appropriate if they have not been addressed.**		
Ontario Power Generation		
American Electric Power	Yes	Refer to comments provided in questions 1 and 13.
Response: **"Responsible Entity" is defined within the Applicability section of each CIP standard.** **The ERO Rules of Procedure include sections on dealing with confidential data associated with the Cyber Security standards, and recognize that there may be some evidence retained by the Responsible Entity. The data retention section of these standards was written to support this concept.** **Phase 1 of this project includes necessary modifications to CIP-002-1 through CIP-009-1 to comply with the near term specific directives included in FERC Order 706. The issue identified in your comment is an issue better suited for a later phase of this project. The SDT suggests that you review the changes proposed in the later phases of the project and resubmit your comments as appropriate if they have not been addressed.**		
Ontario IESO	No	With respect to individual bullet points: (1) We find this question confusing. We interpret Applicability as written to mean that those Responsible Entities that have determined that they have no Critical Cyber Assets need only to meet R2 of CIP-003. The question as posted here seems to suggest that R2 of CIP-003 only applies to these Responsible Entities, but NOT to those other Responsible Entities that have identified that they have Critical Cyber Assets. Please clarify. Currently, only CIP-002 is applicable to entities without Critical Assets. Thus, the recommended modification to CIP-003 would be insufficient for accomplishing the intent of the change. One solution might be to move the Senior Manager appointment requirement from CIP-003 R2 to CIP-002 (as suggested under Q1), or incorporate the requirement for a Senior Manager appointment by

Organization	Yes or No	Question 2 Comment
		reference within CIP-002. (2) Agreed, and this is consistent with our comments on CIP-002, above. (3) Agreed (4) Agreed (5) Agreed
Response: **To clarify, the question refers to the addition of a requirement for entities with no Critical Cyber Assets, not the exclusive application of CIP-003-2 R2 to entities with no Critical Cyber Assets. All Responsible Entities, regardless of their ownership of critical assets, are required to meet CIP-003-2 R2.** **The SDT has received numerous comments related to either referencing CIP-003 R2 within CIP-002 R4 or moving CIP-003 R2 into CIP-002 in order to clarify the reference to the senior manager. Phase 1 of this project includes necessary modifications to CIP-002-1 through CIP-009-1 to comply with the near term specific directives included in FERC Order 706. The issue identified in your comment is an issue better suited for a later phase of this project. The SDT suggests that you review the changes proposed in the later phases of the project and resubmit your comments as appropriate if they have not been addressed.**		
Ameren	Yes	None.
Response: **Thank you for your comment.**		
Consumers Energy Company	Yes	
Xcel Energy	No	It appears as though R3.2 could be interpreted to require compensating measures, once the phrase "or a statement accepting risk" is eliminated. We would like clarification if this was the intent.
Response: **The phrase “any compensating measures” is not intended to require compensating measures. As an Entity is free to develop a Cyber Security Policy which exceeds the minimum requirements of CIP-002-2 through CIP-009-2, there exists the case where an Entity may take exception to its Cyber Security Policy, but still meet all of the CIP requirements. Consequently, the SDT concluded that it was overreaching to require compensating measures for all exceptions to the Cyber Security Policy at this time.**		

Organization	Yes or No	Question 2 Comment
ISO New England Inc	No	1) In R1, and throughout other Requirements in this and other CIP Standards, the inclusion of the word "Implement" is redundent and unnecessary. A Policy, Program, or Plan does not exist if it is not in fact put into practice. 2) We recommend moving CIP-003 R2 into the CIP-002 Standard. Therefore the change to APPLICABILITY 4.2.3 would not be necessary. 3) We take exceptiopn to the inclusion of the words "single" and "authority." These inclusions present a specific example where the CIP Standards are too prescriptive in that they seek to regulate company's internal management, as opposed to regulating performance. This modification is inappropriate and potentially outside NERC's legislative mandate. The drafting team must explain what it intends by adding the word "authority" to the word "responsibility." Second, if "authority" is given a meaning of having the power to ensure that capital resources are expended to achieve the objectives laid out in the Standard, we have questions about how NERC can propose regulating how companies manage their budgets. Some companies budgets must be approved by their Boards, and some companies' budgets must be approved by FERC. 4) We support the change to R2.1 5) We request clarification of CIP-003 R2.3. Would very short term delegations (less than 30 days) for vacation and out-of-office travel need same level of recording and Senior Manager approval. 6) In this Standard and throughout several other CIP Standards, the lead focus statement in the Measures is re-stated redundantly throughout each of the bulleted Measure statements. Please clean-up such text.

Response:

1) The addition of the "implement" language was in response to a determination in the FERC Order. [Please refer to FERC Order 706 Paragraph 75.]

2) The SDT has received numerous comments related to either referencing CIP-003 R2 within CIP-002 R4 or moving CIP-003 R2 into CIP-002 in order to clarify the reference to the senior manager. Phase 1 of this project includes necessary modifications to CIP-002-1 through CIP-009-1 to comply with the near term specific directives included in FERC Order 706. The issue identified in your comment is an issue better suited for a later phase of this project. The SDT suggests that you review the changes proposed in the later phases of the project and resubmit your comments as appropriate if they have not been addressed.

3) The SDT believes that R2.3 provides Responsible Entities the flexibility to meet the leadership requirements without prescribing organizational changes.

Organization	Yes or No	Question 2 Comment
4) Thank you for your comment. **5) There is no adjustment of the requirement based upon longevity of absence.** **6) This modification was done in order to be in line with the structure of other ERO standards.**		
American Transmission Company	Yes	
TVA	Yes	
Duke Energy	No	We believe that R3.2 should be revised to require an analysis of risk, in order to provide understanding of what the compensating measures are achieving. Suggested language is as follows: "Documented exceptions to the cyber security policy must include an explanation as to why the exception is necessary, any compensating measures, and analysis of residual risk."
Response: **The SDT does not intend to prescribe an analysis of risk for all exceptions. Please readdress this issue during the phase 2 comment period.**		
Brazos Electric Power Cooperative, Inc.	No	Under the Applicability section it makes no sense for a Responsible Entity to have to comply with CIP003 R2 when there are no CCAs. This should be deleted.
Response: **The intent of the application of CIP-003-2 R2 to Responsible Entities with no Critical Cyber Assets is to ensure that the appropriate individual approves the null list of Critical Cyber Assets.**		
Progress Energy	Yes	
Standards Review Committee of ISO/RTO Council	Yes No	(1) We are confused by the question asked here. We interpret Applicability as written to mean that those Responsible Entities that have determined that they have no Critical Cyber Assets need only to meet R2 of CIP-003. The question as posted here seems to suggest that R2 of CIP-003 only applies to these Responsible Entities, but NOT to those other Responsible Entities that have identified that they have Critical Cyber Assets. Please clarify. Currently, only CIP-002 is applicable to entities without Critical Assets. Thus, the recommended modification to CIP-003 would be insufficient for accomplishing the intent of the change. One solution

Organization	Yes or No	Question 2 Comment
		might be to move the Senior Manager appointment requirement from CIP-003 R2 to CIP-002 (as suggested under Q1), or incorporate the requirement for a Senior Manager appointment by reference within CIP-002. Specific to R2, notwithstanding the above recommendation to move it to CIP-002, we have concerns with the inclusion of the words "single" and "authority." These inclusions present a specific example where the CIP Standards are overly prescriptive in that they seek to regulate company's internal management, as opposed to regulating performance. This modification is inappropriate, unnecessary and outside NERC's legislative mandate. The drafting team must explain what it intends by adding the word "authority" to the word "responsibility." Second, if "authority" is given a meaning of having the power to ensure that capital resources are expended to achieve the objectives laid out in the Standard, we have questions about how NERC can propose regulating how companies manage their budgets. Some companies budgets must be approved by their Boards, and some companies' budgets must be approved by FERC. (2) Agreed, and this is consistent with our comments on CIP-002, above. (3) Agreed (4) Agreed (5) Agreed
Response: **To clarify, the question refers to the addition of a requirement for entities with no Critical Cyber Assets, not the exclusive application of CIP-003-2 R2 to entities with no Critical Cyber Assets. All Responsible Entities, regardless of their ownership of critical assets, are required to meet CIP-003-2 R2.** **The SDT has received numerous comments related to either referencing CIP-003 R2 within CIP-002 R4 or moving CIP-003 R2 into CIP-002 in order to clarify the reference to the senior manager. Phase 1 of this project includes necessary modifications to CIP-002-1 through CIP-009-1 to comply with the near term specific directives included in FERC Order 706. The issue identified in your comment is an issue better suited for a later phase of this project. The SDT suggests that you review the changes proposed in the later phases of the project and resubmit your comments as appropriate if they have not been addressed.**		
KEMA	No	Agree with all modifications, but strongly suggest rather than deleting the phrase "or a statement accepting risk" rewording it instead. Any time compensating measures are used instead of complying with established policy or standards, some residual risk is always involved, which must be acknowledged and accepted by executive management. Use wording similar to: "...any compensating measures with executive management accepting any residual security risks." This will also force

Organization	Yes or No	Question 2 Comment
		individuals to develop compensating measures with adequate coverage.
Response: **The SDT will consider a Risk Management Framework as defined by NIST during future phases of modifications as directed by FERC Order 706. In addition, FERC has directed the ERO to have the technical feasibility exception process supersede all instances of acceptance of risk. Where requirements cannot be met due to technical, safety, or operational limitations, those limitations are to be treated and documented according to a technical feasibility exception process. [Please refer to FERC 706, Paragraph 151]**		
Austin Energy	Yes	
Kansas City Power & Light	No	In CIP-003 R2, internal political difficulties are created by requiring the designated senior manager to have the authority to implement the security program. Many medium to large utilities have IT departments separate from their operations or compliance departments. In order to find a manager of sufficient direct line authority, you have moved to a level within the organization where the manager will either not have the appropriate level of knowledge to review compliance actions or will not have sufficient time to dedicate to the task. Either way, all that will occur will be a perfunctory signature on the compliance documentation which defeats multiple goals of the program. I believe most utilities will want to comply with the spirit of this provision, but the proposed phrasing will make doing so more difficult.
Response: **The senior manager is held responsible to ensure that there is a clear line of authority and that cyber security functions are given the prominence they deserve. The SDT believes that delegation needs to be addressed in the CIP standards to ensure that the appropriate governance structure is considered by the Responsible Entity.** **The responsibilities of the senior manager may be delegated with the exception of approving (1) the Cyber Security Policy required by CIP-003, Requirement R1; (2) the Risk-based Assessment Methodology required by CIP-002, Requirement R1, and (3) the technical feasibility exceptions. For those instances where delegation is not permitted or not granted, the senior manager would reasonably be expected to seek the advice of technically qualified staff before giving approval.**		
San Diego Gas and Electric Co.	Yes	

3. The The CSO706 SDT is proposing the following modifications to **CIP-004-1**:
   - In R1 and R2, clarify the requirement to implement security awareness and annual cyber security training programs.
   - Revise R2.1 to train personnel prior to granting access (per FERC Order, paragraph 431).
   - Revise R3 to complete a personnel risk assessment prior to granting access (per FERC Order, paragraph 443).
   - In Requirements R2.1 and R3, the SDT adopted the FERC Order 706 language, "except in specified circumstances such as an emergency," to address unusual events that demand urgent action before the personnel risk assessment can be completed.

   Do you agree with the proposed modifications? If not, please explain and provide an alternative to the proposed modifications that would eliminate or minimize your disagreement.

Summary Consideration:

Organization	Yes or No	Question 3 Comment
Detroit Edison Company	No	The language "except in specified circumstances such as emergency." introduces ambiguity into this requirement. What would other circumstances be? Is each Responsible Entity allowed to define this on their own? Paragraph 443 of FERC order 706 directs the SDT to provide guidance on defining emergencies. "The Commission adopts with modifications the proposal to direct the ERO to modify Requirement R3 of CIP-004-1 to provide that newly-hired personnel and vendors should not have access to critical cyber assets prior to the satisfactory completion of a personnel risk assessment, except in specified circumstances such as an emergency. We also direct the ERO to identify the parameters of such exceptional circumstances through the Reliability Standards development process."
Response: **This language was included as specified in Paragraph 443 of FERC Order 706 which permits an entity to grant such access under specified circumstances. The responsible entity shall define and document its own specified circumstances**		
PacifiCorp	Yes	
FirstEnergy Corp	No	Regarding R2.1 and R3, we believe that the phrase "specified circumstances such as an emergency" is ambiguous. It is not clear what would constitute acceptable "specified circumstances" other than an emergency situation. This phrase should be replaced with simply "emergency situations", which would also be consistant with language in other CIP requirements such as in CIP-003 R1.1.

Organization	Yes or No	Question 3 Comment
Response: **This language was included as specified in Paragraph 443 of FERC Order 706 which permits an entity to grant such access under specified circumstances. The responsible entity shall define and document its own specified circumstances.**		
MidAmerican Energy Company	Yes	
Northeast Power Coordinating Council	Yes	
WECC Relibaility Coordination	No	do not agree with R1.2 that personnel need to be trained before they are granted access. Training in this area is extensive and we feel the 90 day window allows appropriate training to take place along with our employee orientation.
Response: **It has been identified in FERC Order 706 and the SDT agrees that the requisite training shall be completed prior to granting unescorted access. Providing escorted access is permitted prior to the requisite training being completed. Granting unescorted access is permitted for specified circumstances such as an emergency prior to the requisite training being completed. The responsible entity shall define their own specified circumstances and document them within their cyber security training program or cyber security policy.**		
Southern Company	Yes	CIP-004 Section D - Compliance: 1.1.1 does not specify who is responsible for the enforcement authority. CIP-004 Section D - Compliance: 1.4.2 - Indefinite retention is not feasible, overall cost of storage depending on scope could potentially be very large. Item should define an upper bound of the request (e.g. a maximum of 3 years) CIP-004 Section D - Compliance: 1.4.3 - Should have a time limit to reduce the overall liability of confidential information.
Response: **1.1.1 - The Regional Entity will serve as the Compliance Enforcement Authority for most entities. As the Regional Entity may not audit itself, the ERO will serve as the Compliance Enforcement Authority in auditing the Regional Entity. A third-party monitor without a vested interest in the outcome will serve as the Compliance Enforcement Authority for NERC. (Refer to NERC's Rules of Procedure.**		

Organization	Yes or No	Question 3 Comment
Paragraphs 404 and 405). **1.4.2 – With the exception of retaining evidence in support of an investigation, the standard defines a finite retention period. The language that indicates the Compliance Enforcement Authority may direct the responsible entity to retain evidence for a longer period of time as part of an investigation is a restatement of what is included in the ERO Rules of Procedure. Reference the ERO Rules of Procedure Appendix 4C – Uniform Compliance Monitoring and Enforcement Procedures – Section 3.4.1 Compliance Violation Investigation Process Steps. While the duration of an investigation cannot be predicted, further clarification of the retention timeframe is outside the scope of the SDT.** **1.4.3 – This language supports the regularly scheduled audit intervals for all entities and supports the need to retain the confidentiality of some data. The audit data retention period is determined by the audit period for each Registered Entity.**		
Luminant Power	Yes	
Encari	No	1. The new language within R2.1 allows for an exception in specific circumstances. What are specified circumstances? And, if these specific circumstances occur do the individuals ever have to take the training? - The prior requirement was within ninety calendar days. 2. An additional crossover requirement exists leading to confusion. CIP-006-2 R3 now states cyber assets residing in a PSP; however the language now in CIP-004-2 does not require access to Cyber Assets to undergo training, awareness and PRAs. We recommend providing further clarification around this requirement.— General Comments Pertaining to All Standards--Other modifications were also made to this standard that are not included as part of the question. 3. The wording of 1.1.1 is awkward and should be modified. We also request further clarification regarding the Data Retention Requirement 1.4.2 as to which entity will be maintaining the last audit records and submitted subsequent audit records. As the statement is currently worded "in conjunction" leaves this open to interpretation.
Response: **1. This language was included as specified in Paragraph 443 of FERC Order 706 which permits an entity to grant such access under specified circumstances. The responsible entity shall define and document its own specified circumstances.** **2. If personnel roles and responsibilities require access after the specified circumstance, then training must be completed**		

Organization	Yes or No	Question 3 Comment
according to CIP-004. Personnel can be granted such access as long as a personnel risk assessment has been conducted according to the requirements in R3, and the minimum training has been conducted according to personnel roles and responsibilities according to the requirements in R2. **3. The data retention periods for the standard requirements are specified in the standards. If a standard does not specify any data retention period, then there are default periods in the Compliance Monitoring and Enforcement Procedures –and in general, the default data retention periods are longer than the periods specified in the standards. The compliance staff worked to develop guidelines that drafting teams could use to determine reasonable data retention periods – trying to balance the needs of the compliance program to have sufficient evidence to review to determine compliance, with the burden to responsible entities of collecting and retaining that evidence.** **The language of 1.4.2 indicates that the Compliance Enforcement Authority "in conjunction with" the Registered Entity will retain all audit records from the previous audit and all audit records submitted since the previous audit, until completion of the next audit. This supports the audit intervals for all entities and supports the need to retain the confidentiality of some data.** **The audit data retention period is determined by the audit period for each Registered Entity. The Reliability Coordinator, Transmission Operator and Balancing Authority are audited for each requirement once every three years – and all others are audited once every six years. The intent is to assure that, if there was an event and the performance of an entity was in question, there would be, at a minimum, at least one record showing the past performance of that entity.**		
TransAlta Centralia Generation, LLC	Yes	
Bonneville Power Administration	Yes	
Consolidated Edison Company of New York, Inc.	No	CIP-003 requires "including provision for emergency situations" in the Entity's cyber security policy. This "emergency" is referenced in CIP-004 R2.1 and R3. Nowhere in the standards is any requirement or more specific guidance provided in what should be addressed in these provisions: e.g. description of what it is and who declares it, start and end conditions, documentation requirements: is it left to the entity to set its own parameters on how and what to declare as an emergency?
Response: **This language was included as specified in Paragraph 443 of FERC Order 706 which permits an entity to grant such access under specified circumstances. The responsible entity shall define and document its own specified circumstances.**		

Organization	Yes or No	Question 3 Comment
Southern California Edison Company	Yes	
Tampa Electric Company	No	Requirement R3 The proposed changes would result in the language: "....A personnel risk assessment shall be conducted pursuant to that program prior to such personnel being granted such access except in specified circumstances such as an emergency."(removing within 30 days of being granted access). This would leave the standard open to the interpretation that as long as an assessment is no older than 7 years old, then this risk assessment is "prior" to the personnel begin granted access. Tampa Electric is unsure if this is the intention of the language change. If this is not the intenct, then the wording should be clarified. Section 1.5 Regarding the removal of the language in Section 1.5: Additional Compliance Information: It is not clear if removal of this language is implying that authorized exceptions result in non-compliance. There are situations where requirements of this standard cannot be met, particularly for legacy equipment and associated vendor supplied systems. The following language should be reinstated in the standard: "Duly authorized exceptions will not result in non-compliance."
Response: **As stated in R3, personnel can be granted such access as long as the personnel risk assessment has been conducted within the last seven years. CIP-003-2 Requirement R3 includes the identification and approval of exceptions to the corporate Cyber Security Policy.Situations where the standards requirements cannot be met will be handled through the Technical Feasibility Exception process under the NERC Rules of Procedure. The technical feasibility exception process will address the requirements for documenting, approving, and remediating the exception. Any sanction decisions will arise from the TFE process. It is not appropriate to assert that "duly authorized exceptions will not result in non-compliance" within Section D-1.5 of the standard.**		
Electric Market Policy	Yes	1) NERC (Step 4.1.10) and Regional Entity (Step 4.1.11) are not defined in the NERC Glossary of Terms or Functional Model. 2) Suggest rewording Requirement R2.1 as follows: "This program will ensure that all personnel requiring access to Critical Cyber Assets," for clarity.
Response: **1) NERC and Regional Entity are defined in NERC's corporate documents including, but not limited to, the Certificate of Incorporation and ByLaws.** **2) Phase 1 of this project includes necessary modifications to CIP-002-1 through CIP-009-1 to comply with the near term specific**		

Organization	Yes or No	Question 3 Comment
directives included in FERC Order 706. The issue identified in your comment is an issue better suited for a later phase of this project. The SDT suggests that you review the changes proposed in the later phases of the project and resubmit your comments as appropriate if they have not been addressed.		
PPL Corporation	Yes	
MRO NERC Standards Review Subcommittee	Yes	
Pepco Holdings, Inc - Affiliates	Yes	We agree with the proposed modifications especially with the phrase "except in specified circumstances such as an emergency". Similar to CIP-002-2, D. Compliance, Section 1.5, should CIP-004-2, D. Compliance, Section 1.5 say "None"?
Response: **Phase 1 of this project includes necessary modifications to CIP-002-1 through CIP-009-1 to comply with the near term specific directives included in FERC Order 706. The issue identified in your comment is an issue better suited for a later phase of this project. The SDT suggests that you review the changes proposed in the later phases of the project and resubmit your comments as appropriate if they have not been addressed.**		
United Illuminating Company	Yes	
Deloitte & Touche, LLP	Yes	With the adoption of "implement", will the drafting team release a FAQ on what entities and auditors should consider for evidence of compliance of implementation (i.e. a documentation of a formal training and awareness program that has ownership, stakeholders, documented narratives & workflows, risk assessment and internal control testing).
Response: **Reliability standards are limited to specifying what to do, not how to do it.** **Please refer to NERC Rules of Procedure Appendix 4C Compliance Process.**		
Exelon	Yes	

Organization	Yes or No	Question 3 Comment
Old Dominion Electric Cooperative	Yes	
City of Tallahassee (TAL)	Yes	
BC Transmission Corporation		
Applied Control Solutions, LLC	No	Training needs to be specifically control system cyber security training
Response: **R2.2 defines minimum required items which are Critical Cyber Asset specific.**		
US Bureau of Reclamation	No	Requirement R2 needs to more specifically distinguish between access types and required training. Individuals with physical access may only need general security awareness training, whereas those with physical and logical access may require specific role-based training. The requirement, as written, addresses proper use of cyber assets, physical and logical access controls, proper handling of information, etc., in what appears to be an all-inclusive manner. Some of these training requirements would appear to be unnecessary for an individual who may only need limited physical access and the requirement should support this. The requirement does not recognize that Entities may have a more rigorous background check process which takes longer than the abbreviated process described in the standard. While describing the minimum helps to clarify what is needed, the standard should allow Entities that have more rigorous requirements longer time frames to implement the background checks. In most cases the background checks timeframes are not within the control of the Entity. In addition the standard would hamper the ability of existing experienced staff who have passed a more exhaustive check from operating thereby defeating the value to reliability. Can the requirement, R3, be structured in such a manner as to support access following initial screening in situations where full investigations may take a significant period of time? As an example, a national security check resulting in a clearance may take an extended period of time, limiting an organization's ability to utilize an employee - even in a decreased sensitivity role - while awaiting results. If the employee is allowed access - even limited - following a preliminary check (through local/national law enforcement agencies), would this meet the intent of the requirements while awaiting the results of a full and more comprehensive investigation? Further, is there a means, within the present requirements, to address the temporary "grandfathering" of

Organization	Yes or No	Question 3 Comment
		individuals who have access today while they are undergoing investigations? Without such an allowance, staff availability, during investigation activities, could be severely limited.
Response: **Personnel can be granted such access as long as a personnel risk assessment has been conducted according to the requirements in R3, and the minimum training has been conducted according to personnel roles and responsibilities according to the requirements in R2. A national security investigation contains elements beyond the scope of R3, which are not necessary to meet R3.As stated in R3, personnel can be granted access as long as the personnel risk assessment has been conducted within the last seven years. If a personnel risk assessment has not been conducted within the last seven years, it must be completed before the individual can be granted access.**		
Orange and Rockland Utilities Inc.	No	CIP-003 requires "including provision for emergency situations" in the Entity's cyber security policy. This "emergency" is referenced in CIP-004 R2.1 and R3. Nowhere in the standards is any requirement or more specific guidance provided in what should be addressed in these provisions: e.g. description of what it is and who declares it, start and end conditions, documentation requirements: is it left to the entity to set its own parameters on how and what to declare as an emergency?
Response: **This language was included as specified in Paragraph 443 of FERC Order 706 which permits an entity to grant such access under specified circumstances. The responsible entity shall define and document its own specified circumstances.**		
CenterPoint Energy		
Manitoba Hydro	Yes	
Alberta Electric System Operator	No	The term "specified circumstances" implies that a set of circumstances is specified somewhere. Where is this list and who will decide what comprises it? Suggest that this list be clarified.
Response: **This language was included as specified in Paragraph 443 of FERC Order 706 which permits an entity to grant such access under specified circumstances. The responsible entity shall define and document its own specified circumstances.**		
Dynegy	Yes	

Organization	Yes or No	Question 3 Comment
Northern Indiana Public Service Company	No	Clarification regarding the definition of specified circumstances and emergency conditions is needed. Additionally, language needs to be added to clarify what steps need to be taken if an emergency occurs and access is granted. As the draft reads, an entity could declare an emergency, grant access, and document the emergency condition. There is no language directing follow up action that would ever require the responsible entity to perform training or a PRA of the individual that was granted access under the emergency condition. Depending on the direction provided from the drafting team in regards to what would consist of an emergency, the removal of the 30-90 day after the fact language may create significant concern in regards to bargaining unit operations and service personnel. Secondly, I have a comment regarding the additional clarifying language that was added to CIP004-2 R1 to indicate applicability to critical cyber assets. I understand that this language was added to provide uniformity in scope between CIP-004-2 R1, R2, and all of the respective sub-requirements. I have a concern regarding the absence of the CCA language in CIP-004-2 R3. I feel R3 should be modified to include similar CCA language to provide uniformity with R1, R2 and the R3 sub-requirements.
Response: **This language was included as specified in Paragraph 443 of FERC Order 706 which permits an entity to grant such access under specified circumstances. The responsible entity shall define and document its own specified circumstances.** **If personnel roles and responsibilities require access after the specified circumstance, then training and a personnel risk assessment must be conducted according to CIP-004.** **Phase 1 of this project includes necessary modifications to CIP-002-1 through CIP-009-1 to comply with the near term specific directives included in FERC Order 706. The issue identified in your comment is an issue better suited for a later phase of this project. The SDT suggests that you review the changes proposed in the later phases of the project and resubmit your comments as appropriate if they have not been addressed.**		
CoreTrace	Yes	
Oncor Electric Delivery LLC	Yes	
Illinois Municipal Electric Agency		
Ontario Power Generation		

Organization	Yes or No	Question 3 Comment
American Electric Power	Yes	Refer to comments provided in questions 1 and 13.
Response: **"Responsible Entity" is defined within the Applicability section of each CIP standard.** **The ERO Rules of Procedure include sections on dealing with confidential data associated with the Cyber Security standards, and recognize that there may be some evidence retained by the Responsible Entity. The data retention section of these standards was written to support this concept.** **Phase 1 of this project includes necessary modifications to CIP-002-1 through CIP-009-1 to comply with the near term specific directives included in FERC Order 706. The issue identified in your comment is an issue better suited for a later phase of this project. The SDT suggests that you review the changes proposed in the later phases of the project and resubmit your comments as appropriate if they have not been addressed.**		
Ontario IESO	Yes	
Ameren	No	The elimination of the 30 day temporary access time will have a significant "operational" impact to fill personnel positions in a timely manner within protected areas. Without the 30 day temporary access criteria, personnel will not be allowed "unescorted" access into a facility until the candidate has completed training and a background check is completed, reviewed and returned with a positive and acceptable response. Additionally, mandating that another employee watch or "escort" the new candidate all the time during their shift is both a nuisance and a possible safety hazard. It is important to note that this proposed change is a "180 degree conceptual change" from what was a noticeable and unwavering stance that most companies took when the original CIP standards were implemented. Not being able to shift personnel around from one area of the company to the protected-area assignments (when personnel are re-assigned) immediately, places an unnecessary burden on both areas of the company. When comparing the proposed change to the current process, the benefits gained by the elimination of the 30-day temporary access window clearly don't outweigh what is already a solid and workable solution.
Response: **It has been identified in FERC Order 706 and the SDT agrees that the personnel risk assessment and requisite training shall be completed prior to granting unescorted access. Providing escorted access is permitted prior to the personnel risk assessment and requisite training being completed. Granting unescorted access is permitted for specified circumstances such as an emergency prior to the personnel risk assessment and requisite training being completed. The responsible entity shall define their own specified circumstances and document them within their cyber security training program, personnel risk assessment program, or**		

Organization	Yes or No	Question 3 Comment
cyber security policy.		
Consumers Energy Company	Yes	
Xcel Energy	Yes	
ISO New England Inc	No	1 - In R1, and throughout other Requirements in this and other CIP Standards, the inclusion of the word "Implement" is redundent and unnecessary. A Policy, Program, or Plan does not exist if it is not in fact put into practice.
Response: **The word 'implement' was included per FERC Order 706 Paragraph 75 to remove any doubt that a particular process/procedure/program could be only designed, developed, documented but not implemented. This was a result of previous questions around implementation from Industry. It is added for clarity and completeness**		
American Transmission Company	Yes	
TVA	Yes	
Duke Energy	Yes	
Brazos Electric Power Cooperative, Inc.	Yes	
Progress Energy	Yes	CIP004R2 – The cyber security training program shall be annually reviewed and updated as necessary – Please provide clarification, does updated as necessary mean updates only need to occur annually during the annual review period?
Response: **The cyber security training program shall be reviewed annually, at a minimum, and shall be updated whenever necessary.**		

Organization	Yes or No	Question 3 Comment
Standards Review Committee of ISO/RTO Council	No	In R1, and throughout other Requirements in this and other CIP Standards, the inclusion of the word "Implement" is redundant and unnecessary. A Policy, Program, or Plan does not exist if it is not in fact put into practice.
Response: **The word 'implement' was included per FERC Order 706 Paragraph 75 to remove any doubt that a particular process/procedure/program could be only designed, developed, documented but not implemented. This was a result of previous questions around implementation from Industry. It is added for clarity and completeness.**		
KEMA	Yes	
Austin Energy	Yes	
Kansas City Power & Light	Yes	
San Diego Gas and Electric Co.	No	To help clarify training requirements for different users and access levels, SDG&E would like to see language added to CIP-004-1 R2.2 stating that training should be appropriate to user duties, functions, experience, and access level. Information concerning vulnerabilities should be revealed on a need to know basis and not universally.
Response: **Given the limited scope and timeline for Phase 1, please readdress this issue during the Phase 2 comment period.**		

4. The CSO706 SDT is proposing the following modifications to **CIP-005-1**:

   - In R1.5, clarify the requirement to safeguard Cyber Assets used in the control or monitoring of Electronic Security Perimeter.
   - The term "implement" was added to CIP-005-1 Requirement R2.3 to clarify that the procedure for securing dial-up access to the Electronic Security Perimeter must be both maintained and implemented.

   Do you agree with the proposed modifications? If not, please explain and provide an alternative to the proposed modifications that would eliminate or minimize your disagreement.

Summary Consideration:

Organization	Yes or No	Question 4 Comment
Detroit Edison Company	Yes	
PacifiCorp	No	Yes to the second bullet. No to the first bullet and other points.R1.1 - It is unclear what is meant by "externally connected". Does "connectivity" refer to logical or physical connectivity? Is "external" a reference to the ESP in question, or to the entity? Is it a reference to layer 3 (and above)? PacifiCorp recommends some clarifying language similar to the following: • Any device accessible via routable protocol (layer 3) from outside the ESP is an access point unless such traffic is already passing through and controlled (layer 3) by another CIP005 compliant access point. • Additionally, any device serving as an endpoint of an encrypted and/or encapsulated layer 3 (and above) tunnel (IPSEC, GRE, SSL-VPN, SSH, CIPE, etc..) which provides remote network connectivity to the ESP network and not merely application access to the host itself, and where the other endpoint is outside the ESP, is also an access point.? • Externally connected also includes devices accessible via modem or any form of wireless access point providing network connectivity to other devices within the ESP." • Externally connected does not include encrypted communication links where the end points are within the ESP.R1.3 - This should be eliminated. By definition,

Organization	Yes or No	Question 4 Comment
		communication links between discrete ESPs are “out of scope” (CIP-005-2 4.2.2) Additionally, where such links are using routable protocols, the termination point would be a “communication end point” and thus covered by R1.1. This section provides no additional value.R1.5 references to CIP005.R2 and CIP005.R3 should be removed as these are not applicable to the access control and monitoring equipment which are not "Access points". Additionally, the proper security practices for these devices are covered under CIP007 R2-R9.R1.5 (continued) - The access control and/or monitoring devices for the electronic security perimeter are not clearly identified in the standard, such as mobile devices. The proposed language may jeopardize the integrity of the bulk electric system by limiting the ability to quickly assess and respond to events and alarms from these access control and/or monitoring devices. PacifiCorp believes strengthening CIP-006 R3 with the language below achieves the intent of the standard by protecting mobile devices used for access control and/or monitoring. The proposed language parallels the requirements of language in CIP-005-2, R2.4.PAC proposes the following language: R3. Protection of Electronic Access Control Systems - Cyber Assets used in the access control and/or monitoring of the Electronic Security Perimeter(s) shall reside within an identified Physical Security Perimeter, except for mobile devices, for which the Responsible Entity shall implement strong procedural or technical controls to ensure authenticity of the accessing party.
Response: **These types of issues will be addressed in Phase 2. Please use the Phase 2 comment period if you feel that your concerns have not been addressed.**		
FirstEnergy Corp	Yes	
MidAmerican Energy Company	No	Comment: On CIP-005, R1.5, the access control and/or monitoring devices for the electronic security perimeter are not clearly identified in the standard, such as client-server applications. The proposed language may jeopardize the integrity of the bulk electric system by limiting the ability to quickly assess and respond to events and alarms from these access control and/or monitoring devices. For example, we cannot place laptops used by technicians inside a physical security perimeter. MidAmerican believes strengthening CIP-006 R3 with the language below achieves the intent of the standard by protecting client-server applications used for access control and/or monitoring. The proposed language parallels the requirements of language in CIP-005-2, R2.4.MEC proposes the following language: CIP-006 R3. Protection of Electronic Access Control Systems - Cyber Assets used in the access control and/or monitoring of the Electronic Security Perimeter(s) shall reside within an identified Physical Security Perimeter, except for the client of a client-server application. In a client-server application, the server will be located in a Physical Security Perimeter, and the Responsible Entity shall implement strong

Organization	Yes or No	Question 4 Comment
		procedural or technical controls to ensure authenticity of the accessing party.
Response: **The scope of the modification is only to include devices that perform access control and/or monitoring as identified in CIP-005 R2 and R3 and not those devices that are receiving alerts.** **Phase 1 of this project includes necessary modifications to CIP-002-1 through CIP-009-1 to comply with the near term specific directives included in FERC Order 706. The issue identified in your comment is an issue better suited for a later phase of this project. The SDT suggests that you review the changes proposed in the later phases of the project and resubmit your comments as appropriate if they have not been addressed.**		
Northeast Power Coordinating Council	No	"Dated" is used only in the Measures (M1, M2, M3, M4, M5). Adding a requirement in the measures is inappropriate. R1 refers to documentation while M1 uses documents. Recommend using documentation consistently.
Response: **The word "dated" will be removed at this time. The measures will be reviewed and considered in an upcoming drafting phase of these standards.**		
WECC Reliability Coordination	Yes	
Southern Company	Yes	CIP-005 Section D - Compliance: 1.1.1 does not specify who is responsible for the enforcement authority. CIP-005 Section D - Compliance: 1.4.2- Indefinite retention is not feasible, overall cost of storage depending on scope could potentially be very large. Item should define an upper bound of the request (e.g. a maximum of 3 years) CIP-005 Section D - Compliance: 1.4.3 - Should have a time limit to reduce the overall liability of confidential information.
Response: **1.1.1 - The Regional Entity will serve as the Compliance Enforcement Authority for most entities. As the Regional Entity may not audit itself, the ERO will serve as the Compliance Enforcement Authority in auditing the Regional Entity. A third-party monitor without a**		

Organization	Yes or No	Question 4 Comment
vested interest in the outcome will serve as the Compliance Enforcement Authority for NERC. (Refer to NERC's Rules of Procedure, Paragraphs 404 and 405). **1.4.2 – With the exception of retaining evidence in support of an investigation, the standard defines a finite retention period. The language that indicates the Compliance Enforcement Authority may direct the responsible entity to retain evidence for a longer period of time as part of an investigation is a restatement of what is included in the ERO Rules of Procedure. Reference the ERO Rules of Procedure Appendix 4C – Uniform Compliance Monitoring and Enforcement Procedures – Section 3.4.1 Compliance Violation Investigation Process Steps. While the duration of an investigation cannot be predicted, further clarification of the retention timeframe is outside the scope of the SDT.** **1.4.3 – This language supports the regularly scheduled audit intervals for all entities and supports the need to retain the confidentiality of some data. The audit data retention period is determined by the audit period for each Registered Entity.**		
Luminant Power	Yes	
Encari	No	1. It is very important to define monitoring in the new context. Originally the cyber assets had to be used for the dual purpose of access control and monitoring. Now, simply a monitoring device is considered a cyber asset under this new language. We ask for an additional clarification around to what extent monitoring is covered, for example: a. The original monitoring cyber asset (device a) b. 2. The cyber asset receiving alerts from the original device (device b) c. 3. The cyber asset forwarding the alerts (device c) d. 4. The cyber asset receiving the alerts (device d)The current language could be interpreted in a way that a blackberry receiving alerts is "monitoring" the ESP. General Comments Pertaining to All Standards--Other modifications were also made to this standard that are not included as part of the question. 2. The wording of 1.1.1 is awkward and should be modified. 3. We also request further clarification regarding the Data Retention Requirement 1.4.2 as to which entity will be maintaining the last audit records and submitted subsequent audit records. As the statement is currently worded "in conjunction" leaves this open to interpretation.

Organization	Yes or No	Question 4 Comment
Response: **1) The scope of the modification is to only include devices that perform access control and/or monitoring as identified in CIP-005 R2 and R3 and not those devices that are receiving alerts. Phase 1 of this project includes necessary modifications to CIP-002-1 through CIP-009-1 to comply with the near term specific directives included in FERC Order 706. The issue identified in your comment is an issue better suited for a later phase of this project. The SDT suggests that you review the changes proposed in the later phases of the project and resubmit your comments as appropriate if they have not been addressed.** **2) The intent of the wording in 1.1.1 is to clarify which entity will serve as the Compliance Enforcement Authority. For most standards, the Regional Entity serves as the Compliance Enforcement Authority and audits the performance of the Reliability Coordinator, Transmission Operator, Balancing Authority, Generator Operator, Generator Owner, etc. In this standard, the Regional Entity is responsible for some of the requirements – but an entity cannot audit its own performance. Where the Regional Entity is also the responsible entity, the ERO will audit the Regional Entity's performance. Where the ERO is the responsible entity, a third-party monitor without vested interest in the outcome will conduct the audit.** **3) The data retention periods for the standard requirements are specified in the standards. If a standard does not specify any data retention period, then there are default periods in the Compliance Monitoring and Enforcement Procedures –and in general, the default data retention periods are longer than the periods specified in the standards. The compliance staff worked to develop guidelines that drafting teams could use to determine reasonable data retention periods – trying to balance the needs of the compliance program to have sufficient evidence to review to determine compliance, with the burden to responsible entities of collecting and retaining that evidence.** **The language of 1.4.2 indicates that the Compliance Enforcement Authority "in conjunction with" the Registered Entity will retain all audit records from the previous audit and all audit records submitted since the previous audit, until completion of the next audit. This supports the audit intervals for all entities and supports the need to retain the confidentiality of some data.** **The audit data retention period is determined by the audit period for each Registered Entity. The Reliability Coordinator, Transmission Operator and Balancing Authority are audited for each requirement once every three years – and all others are audited once every six years. The intent is to assure that, if there was an event and the performance of an entity was in question, there would be, at a minimum, at least one record showing the past performance of that entity.**		
TransAlta Centralia Generation, LLC	Yes	
Bonneville Power Administration	No	The revision to CIP-005-2 R1.5 referenced only CIP-006-2 R3. CIP-003 R3 requires that the organization identify the Physical Security Perimeter. In the original CIP-005-1 R1.5, the physical protections had to meet CIP-006-1 R2 and R3 which are now renumbered R4 and R5 in CIP-006-2. This represents a major revision and a much less robust security in the physical protection requirements

Organization	Yes or No	Question 4 Comment
		for cyber assets used for access control or monitoring of the Electronic Security Perimeter. To retain the original intent of CIP-005-1 R1.5, the requirement must include a reference to CIP-006-2 R3, R4, and R5.
Response: **CIP-006-R3 requires placing the devices of CIP-005-2 R1.5 within a Physical Security Perimeter. Once a device is within a Physical Security Perimeter, physical control is automatically established, making these inclusions redundant.**		
Consolidated Edison Company of New York, Inc.	No	"Dated" is used only in the Measures (M1, M2, M3, M4, M5). The corresponding requirements do not state a requirement for a date: adding a requirement in the measures is inappropriate. R1 refers to documentation while M1 uses documents. Recommend using documentation consistently
Response: **The word "dated" will be removed at this time. The measures will be reviewed and considered in an upcoming drafting phase of these standards.**		
Southern California Edison Company	Yes	Request clarification on the difference between "process" and "procedure."
Response: **Phase 1 of this project includes necessary modifications to CIP-002-1 through CIP-009-1 to comply with the near term specific directives included in FERC Order 706. The issue identified in your comment is an issue better suited for a later phase of this project. The SDT suggests that you review the changes proposed in the later phases of the project and resubmit your comments as appropriate if they have not been addressed.**		
Tampa Electric Company	No	In R1.5, the change from "and" to "and/or" could bring unintended devices into scope of this standard. The change should be clarified to say "access control of and/or monitoring access to of the Electronic Security Perimeter(s)." Section 1.5 Regarding the removal of the language in Section 1.5: Additional Compliance Information: It is not clear if removal of this language is implying that authorized exceptions result in non-compliance. There are situations where requirements of this standard cannot be met, particularly for legacy equipment and associated vendor supplied systems. The following language should be reinstated in the standard: "Duly authorized exceptions will not result in non-compliance."

Organization	Yes or No	Question 4 Comment
Response: **The scope of the modification is to only include devices that perform access control and/or monitoring as identified in CIP-005 R2 and R3 and not those devices that are receiving alerts.** **Situations where standards requirements cannot be met will be handled through the Technical Feasibility Exception process under the NERC Rules of Procedure. The TFE process will address the requirements for documenting, approving, and remediating the exception.** **Phase 1 of this project includes necessary modifications to CIP-002-1 through CIP-009-1 to comply with the near term specific directives included in FERC Order 706. The issue identified in your comment is an issue better suited for a later phase of this project. The SDT suggests that you review the changes proposed in the later phases of the project and resubmit your comments as appropriate if they have not been addressed.**		
Electric Market Policy	Yes	NERC (Step 4.1.10) and Regional Entity (Step 4.1.11) are not defined in the NERC Glossary of Terms or Functional Model.
Response: **NERC and Regional Entity are defined in NERC's corporate documents including, but not limited to, the Certificate of Incorporation and ByLaws.**		
PPL Corporation	Yes	
MRO NERC Standards Review Subcommittee	No	On CIP-005, R1.5, the access control and/or monitoring devices for the electronic security perimeter are not clearly identified in the standard, such as client-server applications. The proposed language may jeopardize the integrity of the bulk electric system by limiting the ability to quickly assess and respond to events and alarms from these access control and/or monitoring devices. For example, we cannot place laptops used by technicians inside a physical security perimeter. The MRO NSRS believes strengthening CIP-006 R3 with the language below achieves the intent of the standard by protecting client-server applications used for access control and/or monitoring. The proposed language parallels the requirements of language in CIP-005-2, R2.4.The MRO NSRS proposes the following language: CIP-006 R3. Protection of Electronic Access Control Systems? Cyber Assets used in the access control and/or monitoring of the Electronic Security Perimeter(s) shall reside within an identified Physical Security Perimeter, except for the client of a client-server application. In a client-server application, the server will be located in a Physical Security Perimeter, and the Responsible Entity shall implement strong procedural or technical controls to ensure authenticity of the accessing party.

Organization	Yes or No	Question 4 Comment
Response: **The scope of the modification is to only include devices that perform access control and/or monitoring as identified in CIP-005 R2 and R3 and not those devices that are receiving alerts.** **Phase 1 of this project includes necessary modifications to CIP-002-1 through CIP-009-1 to comply with the near term specific directives included in FERC Order 706. The issue identified in your comment is an issue better suited for a later phase of this project. The SDT suggests that you review the changes proposed in the later phases of the project and resubmit your comments as appropriate if they have not been addressed.**		
Pepco Holdings, Inc - Affiliates	Yes	
United Illuminating Company	Yes	
Deloitte& Touche, LLP	Yes	With the adoption of "implement", will the drafting team release a FAQ on what entities and auditors should consider for evidence of compliance of implementation (i.e., a documentation of a formal dial-up security program and procedure that has ownership, stakeholders, documented narratives & workflows, risk assessment and internal control testing).
Response: **Reliability standards are limited to specifying what to do, not how to do it.** **Please refer to NERC Rules of Procedure Appendix 4C Compliance Process.**		
Exelon	Yes	We support all comments noted for CIP005 in this section with the recommendation to move the word implement before maintain in R2.3 so the sentence reads ?implement and maintain.? Reason for the recommendation is a control must be implemented before it can be maintained
Response: **The SDT will make the appropriate change in R2.3 from “maintain and implement” to “implement and maintain”.**		
Old Dominion Electric Cooperative		

Organization	Yes or No	Question 4 Comment
City of Tallahassee (TAL)	Yes	
BC Transmission Corporation	Yes	
Applied Control Solutions, LLC	Yes	
US Bureau of Reclamation	No	The standard should be worded to be applicable for existing dial-up access or if dial-up access is added.
Response: **The requirement applies to all dial-up access, both existing and future.**		
Orange and Rockland Utilities Inc.	No	"Dated" is used only in the Measures (M1, M2, M3, M4, M5). Adding a requirement in the measures is inappropriate. R1 refers to documentation while M1 uses documents. Recommend using documentation consistently
Response: **The word "dated" will be removed at this time. The measures will be reviewed and considered in an upcoming drafting phase of these standards.**		
CenterPoint Energy		
Manitoba Hydro	Yes	
Alberta Electric System Operator	Yes	
Dynegy	Yes	
Northern Indiana Public	No	I would request a clarification on scope and depth of the devices to be included in the access control

Organization	Yes or No	Question 4 Comment
Service Company		and/or monitoring. The previous language would have limited the devices to those that performed access control and monitoring of the ESP (traditional Firewalls, routers with ACL's, any IPS devices, VPN endpoints, etc.). The new language provided in the draft under CIP-005-2 R1.5 modifies the scope to include cyber assets used in the access control and/or monitoring of the ESP. I am concerned with the depth of devices involved in the monitoring chain that have no relevance on access control, but are an active component in the monitoring of the ESP. Specifically: log correlation servers, SNMP trap servers, SMTP relay servers for notification, pagers, blackberry's, enterprise email servers, backup and recovery servers for these extended devices, etc.. In the current draft it is unclear whether the device performing the monitoring is the only device that is subject to the requirements specified in CIP-005-2 R1.5 or if all devices involved in monitoring are subject to those requirements specified in CIP-005-2 R1.5. I feel that additional language needs to be provided to clarify the scope and depth of the devices to be included under the classification of cyber assets used in the monitoring of the ESP.
Response: **The scope of the modification is to only include devices that perform access control and/or monitoring as identified in CIP-005 R2 and R3 and not those devices that are receiving alerts.** **Phase 1 of this project includes necessary modifications to CIP-002-1 through CIP-009-1 to comply with the near term specific directives included in FERC Order 706. The issue identified in your comment is an issue better suited for a later phase of this project. The SDT suggests that you review the changes proposed in the later phases of the project and resubmit your comments as appropriate if they have not been addressed.**		
CoreTrace	Yes	
Oncor Electric Delivery LLC	Yes	
Illinois Municipal Electric Agency		
Ontario Power Generation	No	R1.5 creates issues where an entity may be using a third party to remotely monitor and administer Cyber Assets used in the control or monitoring of the ESP. The new requirement will require the entity to police the physical security measures of any such third party to a degree not required for third parties who may support CCAs within the ESP. OPG suggests that the requirements for Cyber Assets used in the access control and / or monitoring of the ESP require protections to the same standards as those

Organization	Yes or No	Question 4 Comment
		which are used to access CCAs
Response: **Requirements apply regardless of who performs the functions.**		
American Electric Power	Yes	Refer to comments provided in questions 1 and 13.
Response: **"Responsible Entity" is defined within the Applicability section of each CIP standard.** **The ERO Rules of Procedure include sections on dealing with confidential data associated with the Cyber Security standards, and recognize that there may be some evidence retained by the Responsible Entity. The data retention section of these standards was written to support this concept.** **Phase 1 of this project includes necessary modifications to CIP-002-1 through CIP-009-1 to comply with the near term specific directives included in FERC Order 706. The issue identified in your comment is an issue better suited for a later phase of this project. The SDT suggests that you review the changes proposed in the later phases of the project and resubmit your comments as appropriate if they have not been addressed.**		
Ontario IESO	Yes	
Ameren	Yes	
Consumers Energy Company	Yes	
Xcel Energy	Yes	
ISO New England Inc	No	1) "Dated" is used only in the Measures (M1, M2, M3, M4, M5). Adding a requirement in the measures is inappropriate. 2) R1 refers to documentation while M1 uses documents. Recommend using documentation consistently.

Organization	Yes or No	Question 4 Comment
Response: **1) The word "dated" will be removed at this time. The measures will be reviewed and considered in an upcoming drafting phase of these standards.** **2) The text will be changed to read "documentation".** **The SDT has received numerous comments related to wording preferences. Phase 1 of this project includes necessary modifications to CIP-002-1 through CIP-009-1 to comply with the near term specific directives included in FERC Order 706. The issue identified in your comment is an issue better suited for a later phase of this project. The SDT suggests that you review the changes proposed in the later phases of the project and resubmit your comments as appropriate if they have not been addressed.**		
American Transmission Company	Yes	
TVA	Yes	
Duke Energy	Yes	
Brazos Electric Power Cooperative, Inc.	Yes	
Progress Energy	Yes	
Standards Review Committee of ISO/RTO Council	Yes	
KEMA	Yes	
Austin Energy	Yes	
Kansas City Power & Light	Yes	

Organization	Yes or No	Question 4 Comment
San Diego Gas and Electric Co.	Yes	

5. The CSO706 SDT is proposing the following modifications to **CIP-006-1**:

- Clarify Requirement R1 that a physical security plan to protect Critical Cyber Assets must be documented, maintained, implemented and approved by the senior manager. CIP-006-1 Requirements R1.1 through R1.7 and R1.9 were revised to clarify the elements that, at a minimum, must be addressed in the physical security plan.
- The SDT added Requirement R2 to CIP-006-2 to clarify the requirement to safeguard the Physical Access Control Systems and exclude hardware at the Physical Security Perimeter access point, such as electronic lock control mechanisms and badge readers from the requirement. Requirement R2.1 requires the Responsible Entity to protect the Physical Access Control Systems from unauthorized access. CIP-006-1 Requirement R1.8 was moved to become CIP-006-2 Requirement R2.2.
- The SDT added Requirement R3 to CIP-006-2, clarifying the requirement for Electronic Access Control Systems to be safeguarded within an identified Physical Security Perimeter.
- Subsequent Requirements were renumbered and references were appropriately revised. The sub requirements of CIP-006-2 Requirements R4, R5, and R6 were changed from formal requirements to lists of options consistent with the intent of the requirements.
- The SDT revised the Measures to add “implementation” to Measure M1 documentation elements for Requirement R1, added Measure M2 to document the protection of physical access control systems, added Measure M3 to document the protection of electronic access control systems, and renumbered subsequent Measures and references to Requirements. The SDT also added failure to implement the security plan as Level 4 non-compliance.

Do you agree with the proposed modifications? If not, please explain and provide an alternative to the proposed modifications that would eliminate or minimize your disagreement.

Summary Consideration:

Organization	Yes or No	Question 5 Comment
Detroit Edison Company	No	CIP-006-2 R1.4 references "physical access controls as described in Requirement R3". R1.4 should reference Requirement R4 since the requirements were renumbered and Physical Access Controls is now R4.CIP-006-2 Introduction, 3. Purpose, it should read something like, ?. . . . . to ensure the implementation and continued maintenance of a physical . . . . . ? This program is not only being implemented, but will also be maintained going forward. (i.e. ? does not make sense to implement a program and do nothing else)CIP-006-2 Introduction, 4.2 The following are exempt from Standard CIP-006-2, in addition to listing the exemptions to NERC Standard CIP-006, they may also want to comment

Organization	Yes or No	Question 5 Comment
		on potentially overlapping security requirements for facilities which are also regulated under the Maritime Transportation Security Act (33 CFR 101/105) and the Chemical Facility Anti-Terrorism Standards. (6 CFR 27)CIP-006-2 R2 Protection of Physical Access Control Systems, sub-requirements R2.1 & R2.2. R2.1 is ambiguous in that it states, "Be protected from unauthorized physical access," yet it does not explain how this is to be accomplished. R2.2 defines the protective measures to be utilized? R4 and R5, Physical Access Controls and Monitoring Physical Access. It appears they want to grant the responsible entity flexibility in R2.1, but then it is limited by R2.2. These two sub-requirements should be combined into one to avoid confusion.
Response: **The Drafting team agrees that R1.4 should reference R4 and not R3. This change will be implemented. With regard to inclusion of maintenance within the Purpose of the requirement, the drafting team agrees that this could add clarity however for consistency we would need to review how this would impact the purpose statements of the remaining CIP standards hence this will be addressed in Phase 2. The issue of conflicting regulatory authorities will be brought before NERC for discussion. Relating to protection of Physical Access Control Systems, reliability standards only prescribe "What" and not "How". These types of issues will be addressed in Phase 2. Please resubmit your comments during the Phase 2 comment period if you feel that your concerns have not been addressed.**		
PacifiCorp	No	No for the third bullet (R3) (See comment on CIP-005-2). Yes for remaining bullets.
Response: **Phase 1 of this project includes necessary modifications to CIP-002-1 through CIP-009-1 to comply with the near term specific directives included in FERC Order 706. The issue identified in your comment is an issue better suited for a later phase of this project. The SDT suggests that you review the changes proposed in the later phases of the project and resubmit your comments as appropriate if they have not been addressed.**		
FirstEnergy Corp	Yes	
MidAmerican Energy Company	No	See comment for question 5
Response: **The scope of the modification is only to include devices that perform access control and/or monitoring as identified in CIP-005 R2**		

Organization	Yes or No	Question 5 Comment
and R3 and not those devices that are receiving alerts. **Phase 1 of this project includes necessary modifications to CIP-002-1 through CIP-009-1 to comply with the near term specific directives included in FERC Order 706. The issue identified in your comment is an issue better suited for a later phase of this project. The SDT suggests that you review the changes proposed in the later phases of the project and resubmit your comments as appropriate if they have not been addressed.**		
Northeast Power Coordinating Council	No	1) We recommend changing R1.2 from "Identification of all access points" to "Identification of all physical access points". 2) We request a correction to R1.4 which references R3. We believe this is now R4. 3) Regarding R1.6, we are concerned with the new word "continuous", and that it will be difficult to demonstrate compliance. Requirements need to be auditable, measurable and enforceable. We request removing "continuous." 4) We recommend changing R1.7 from "within thirty calendar days of the completion of any" to "within thirty calendar days of completion of the entity's change process for any".
Response: **1) Adding "physical" to access point in R1.2 - the drafting team feels that it is clear that the access points are "physical" since the requirement is directed at Physical Security Perimeters.** **2) The drafting team agrees and will implement this change.** **3) The drafting team feels that 'continuous' is a clarification of an active process of escorting as opposed to just being in the same room as an individual (i.e. escorted).** **4) Phase 1 of this project includes necessary modifications to CIP-002-1 through CIP-009-1 to comply with the near term specific directives included in FERC Order 706. The issue identified in your comment is an issue better suited for a later phase of this project. The SDT suggests that you review the changes proposed in the later phases of the project and resubmit your comments as appropriate if they have not been addressed.**		
WECC Reliability Coordination	Yes	
Southern Company	Yes	CIP-006 R1.1 - Change to the last sentence should be clarifed that it applies to Critical Cyber Assets and not Critical Assets.

Organization	Yes or No	Question 5 Comment
		R1.4 makes reference to "Requirement 3", but the correct reference in the new standard should now be "Requirement 5". CIP-006 Section D - Compliance: 1.1.1 does not specify who is responsible for the enforcement authority. CIP-006 Section D - Compliance: 1.4.1 - Indefinite retention is not feasible, overall cost of storage depending on scope could potentially be very large. Item should define an upper bound of the request (e.g. a maximum of 3 years) CIP-006 Section D - Compliance: 1.4.3 - Should have a time limit to reduce the overall liability of confidential information.
Response: **Within CIP-006 R1.1, the requirement now reads "to such Cyber Assets". The Drafting team agrees that the R1.4 reference is incorrect. The SDT points out that the correct reference is R4 and not R5.** **1.1.1 - The Regional Entity will serve as the Compliance Enforcement Authority for most entities. As the Regional Entity may not audit itself, the ERO will serve as the Compliance Enforcement Authority in auditing the Regional Entity. A third-party monitor without a vested interest in the outcome will serve as the Compliance Enforcement Authority for NERC. (Refer to NERC's Rules of Procedure, Paragraphs 404 and 405).** **1.4.1 – With the exception of retaining evidence in support of an investigation, the standard defines a finite retention period. The language that indicates the Compliance Enforcement Authority may direct the responsible entity to retain evidence for a longer period of time as part of an investigation is a restatement of what is included in the ERO Rules of Procedure. Reference the ERO Rules of Procedure Appendix 4C – Uniform Compliance Monitoring and Enforcement Procedures – Section 3.4.1 Compliance Violation Investigation Process Steps. While the duration of an investigation cannot be predicted, further clarification of the retention timeframe is outside the scope of the SDT.** **1.4.3 – This language supports the regularly scheduled audit intervals for all entities and supports the need to retain the confidentiality of some data. The audit data retention period is determined by the audit period for each Registered Entity.**		
Luminant Power	Yes	
Encari	No	1. The redlining appears to be inaccurate. For example R2 in CIP-006-1 is now R4 in CIP-006-2. This modification is very important to note as compliance monitoring systems may have been defined to key on the requirement field.2. CIP-006-2 R4/R5/R6 now use bullets instead of numbered identifiers for the individual physical access methods. A unique identifier should be selected to identify these bulleted

Organization	Yes or No	Question 5 Comment
		items.3. R3 requires cyber assets used in the access control and/or monitoring of the ESP to be in a PSP. Please see our comments in Question 4 (CIP-005-2) pertaining to the extent of what assets need to be in a PSP (device a / b / c / d). --General Comments Pertaining to All Standards--Other modifications were also made to this standard that are not included as part of the question. The wording of 1.1.1 is awkward and should be modified. We also request further clarification regarding the Data Retention Requirement 1.4.2 as to which entity will be maintaining the last audit records and submitted subsequent audit records. As the statement is currently worded "in conjunction" leaves this open to interpretation.

Response:

1) **The drafting team agrees that not all of the changes are clearly identified. The posted version (the one that was commented on) is the official version, and while the drafting team did renumber some of the requirements, these are consistent across the reliability standards.**

2) **The changes that made individual sub-requirements into bullets were made to correct an original error, since requirements cannot be levied upon an item that may not be implemented.**

3) **CIP-006-R3 requires placing the devices of CIP-005-2 R1.5 within a Physical Security Perimeter. Once a device is within a Physical Security Perimeter, physical control is automatically established, making these inclusions redundant. Relating to not including all of the changes within the questions, the questions were meant to only address substantive changes to the standards.**

General: The data retention periods for the standard requirements are specified in the standards. If a standard does not specify any data retention period, then there are default periods in the Compliance Monitoring and Enforcement Procedures –and in general, the default data retention periods are longer than the periods specified in the standards. The compliance staff worked to develop guidelines that drafting teams could use to determine reasonable data retention periods – trying to balance the needs of the compliance program to have sufficient evidence to review to determine compliance, with the burden to responsible entities of collecting and retaining that evidence.

The language of 1.4.2 indicates that the Compliance Enforcement Authority "in conjunction with" the Registered Entity will retain all audit records from the previous audit and all audit records submitted since the previous audit, until completion of the next audit. This supports the audit intervals for all entities and supports the need to retain the confidentiality of some data.

The audit data retention period is determined by the audit period for each Registered Entity. The Reliability Coordinator, Transmission Operator and Balancing Authority are audited for each requirement once every three years – and all others are audited once every six years. The intent is to assure that, if there was an event and the performance of an entity was in question, there would be, at a minimum, at least one record showing the past performance of that entity.

Organization	Yes or No	Question 5 Comment
TransAlta Centralia Generation, LLC	Yes	
Bonneville Power Administration	No	While the majority of the revisions to R1 do provide clarity, the revision to Requirement R1.1 is less clear than the previous version and represents a change to the requirement. In the previous version, R1.1 requires that the Physical Security Plan address "Processes to ensure and document that" all Cyber Assets within an Electronic Security Perimeter reside within an identified Physical Security Perimeter consisting of a six-wall border. With this new revision, the Physical Security Plan shall address all Cyber Assets within an Electronic Security Perimeter. Address cyber assets how? There is no longer any requirement to describe the process the organization uses to ensure that cyber assets reside within an identified Physical Security Perimeter. Is the intent of this revision to clarify that a Physical Security Plan must simply exist and address identified Physical Security Perimeters protecting Cyber Assets within an Electronic Security Perimeter? There is no requirement for Physical Security Plans for cyber assets used for access control and/or monitoring of Physical Security Perimeters or Electronic Security Perimeters. If the intent of Phase 1 changes to R1 are simply to provide clarity, then recommend retaining the original R1.1 text from the previous version and make changes to R1.1 in a later phase of Project 2008-06 - Cyber Security Order 706.
Response: **Requirement 1 identifies what must be within the Physical Security Plan, and Requirement 1.1 identifies that all cyber assets within an ESP must be within a Physical Security Perimeter, (i.e, the plan must address ensuring that all cyber assets within an ESP are within a PSP). Relating to exclusion of cyber assets used for access control and/or monitoring from the Physical Security Plan, the SDT refers you to Requirements 1.2 and 1.3.**		
Consolidated Edison Company of New York, Inc.	No	1) We recommend changing R1.2 from "Identification of all access points" to "Identification of all physical access points" 2) We request a correction to R1.4 which references R3. We believe this is now R4. 3) Regarding R1.6, we are concerned with the new word "continuous," it will be difficult to demonstrate compliance. Requirements need to be auditable, measurable and enforceable. We request removing "continuous." 4) We recommend changing R1.7 from "within thirty calendar days of the completion of any" to "within thirty calendar days of completion of the Entity's Change Process for any": a change generally includes more processes than just the change, e.g. acceptance period, required internal approvals,

Organization	Yes or No	Question 5 Comment
		"as built" regulatory approvals.
Response: **1) Adding "physical" to access point in R1.2 - the drafting team feels that it is clear that the access points are "physical" since the requirement is directed at Physical Security Perimeters.** **2) The drafting team agrees and will implement this change.** **3) The drafting team feels that 'continuous' is a clarification of an active process of escorting as opposed to just being in the same room as an individual (i.e. escorted).** **4) Phase 1 of this project includes necessary modifications to CIP-002-1 through CIP-009-1 to comply with the near term specific directives included in FERC Order 706. The issue identified in your comment is an issue better suited for a later phase of this project. The SDT suggests that you review the changes proposed in the later phases of the project and resubmit your comments as appropriate if they have not been addressed.**		
Southern California Edison Company	No	For R1.8 Annual review and approval - we interpret it as the Senior Manager or delegate reviews and approves the physical security plan annually. For consistency with R2, suggest re-wording R3 to: "Protection of Electronic Access Control Systems - Cyber Assets that authorize and/or log access to the Electronic Security Perimeter (s) shall reside within an identified Physical Security Perimeter." Delete R2.1.
Response: **The drafting team feels that since Requirement 1.8 is a subrequirement of Requirement 1, it is appropriate to interpret that the annual review would be signed off by the senior manager or delegate as identified in Requirement 1.** **For your additional comments, these types of issues will be addressed in Phase 2. Please resubmit your comments during the Phase 2 comment period if you feel that your concerns have not been addressed.**		
Tampa Electric Company	No	Requirement 1.3: Remove "processes" from the wording to be consistent with the other changes in CIP006 Requirement 1 and eliminate the redundancy of having "processes" and "procedures" in same statement. Processes are included in the procedures. Section 1.5 Regarding the removal of the language in Section 1.5: Additional Compliance Information: It is not clear if removal of this language is implying that authorized exceptions result in non-compliance. There are situations where requirements of this standard cannot be met, particularly for legacy equipment and associated vendor supplied systems. The following language should be reinstated in the

Organization	Yes or No	Question 5 Comment
		standard: “Duly authorized exceptions will not result in non-compliance.”
Response: **Phase 1 of this project includes necessary modifications to CIP-002-1 through CIP-009-1 to comply with the near term specific directives included in FERC Order 706. The issue identified in your comment is an issue better suited for a later phase of this project. The SDT suggests that you review the changes proposed in the later phases of the project and resubmit your comments as appropriate if they have not been addressed.** **Situations where the standards requirements cannot be met will be handled through the Technical Feasibility Exception process under the NERC Rules of Procedure. The technical feasibility exception process will address the requirements for documenting, approving, and remediating the exception. Any sanction decisions will arise from the TFE process. It is not appropriate to assert that “duly authorized exceptions will not result in non-compliance” within Section D-1.5 of the standard.**		
Electric Market Policy	Yes	1) NERC (Step 4.1.10) and Regional Entity (Step 4.1.11) are not defined in the NERC Glossary of Terms or Functional Model. 2) Requirement R1.4, it is not clear what is intended by the phrase "response to loss." . 3) Requirement R1.4 should reference R4 rather than R3. 4) Suggest standardizing the language used in R4, R5 and R6. (R4 refers to security personnel; R5, second bullet, to authorized personnel; R6, third bullet, to security or other authorized personnel.)
Response: **1) NERC and Regional Entity are defined in NERC’s corporate documents including, but not limited to, the Certificate of Incorporation and ByLaws.** **2) Due to the limited scope and timeline for Phase 1, issues such as “response to loss” will be addressed in Phase 2. Please use the Phase 2 comment period if you feel that your concerns have not been addressed.** **3) The drafting team agrees with the correction of Requirement 1.4, and will implement this.** **4) Standardizing language will additionally be addressed in Phase 2.**		
PPL Corporation	No	Recommend a correction to R1.4 which references R3. We believe this is now R4.

Organization	Yes or No	Question 5 Comment
Response: **The drafting team agrees with the correction of Requirement 1.4, and will implement this.**		
MRO NERC Standards Review Subcommittee	No	The MRO NSRS believes strengthening CIP-006 R3 with the language below achieves the intent of the standard by protecting client-server applications used for access control and/or monitoring. The proposed language parallels the requirements of language in CIP-005-2, R2.4.The MRO NSRS proposes the following language:CIP-006 R3. Protection of Electronic Access Control Systems ? Cyber Assets used in the access control and/or monitoring of the Electronic Security Perimeter(s) shall reside within an identified Physical Security Perimeter, except for the client of a client-server application. In a client-server application, the server will be located in a Physical Security Perimeter, and the Responsible Entity shall implement strong procedural or technical controls to ensure authenticity of the accessing party. The MRO NSRS agrees with the remaining changes in CIP-006-2.
Response: **You bring up a good point of clarification. The intent of the modification was to clarify that a device that performs either function must be included. However an unintended consequence of this change was to add ambiguity as to what constitutes a monitoring device. The intent is to only include devices that perform access control and/or monitoring as identified in CIP-005 R2 and R3 and not those devices that are receiving alerts.** **Phase 1 of this project includes necessary modifications to CIP-002-1 through CIP-009-1 to comply with the near term specific directives included in FERC Order 706. The issue identified in your comment is an issue better suited for a later phase of this project. The SDT suggests that you review the changes proposed in the later phases of the project and resubmit your comments as appropriate if they have not been addressed.**		
Pepco Holdings, Inc - Affiliates		
United Illuminating Company	Yes	
Deloitte& Touche, LLP	Yes	With the adoption of "implement", will the drafting team release a FAQ on what entities and auditors should consider for evidence of compliance of implementation (i.e. a documentation of a formal physical security program that has ownership, stakeholders, documented narratives & workflows, risk assessment and internal control testing).

Organization	Yes or No	Question 5 Comment
Response: **Reliability standards are limited to specifying what to do, not how to do it.** **Please refer to NERC Rules of Procedure Appendix 4C Compliance Process.**		
Exelon	Yes	Recommendation to increase the timeframe in R1.7 to update the physical security plan to 60 days from 30 days. Reason for the recommendation is 30 days is not a sufficient time period to accomplish this level of change management on documentation. We support all the other comments noted for CIP006 in this section with the recommendation to move the word implement before maintain in R1 so the sentence reads “create, implement and maintain.” Reason for the recommendation is a control must be implemented before it can be maintained. .
Response: **Thank you for your comments. They will be considered in future phases of these standards.** **Revising the order of “create, implement, and maintain” is accepted.**		
Old Dominion Electric Cooperative		
City of Tallahassee (TAL)	Yes	
BC Transmission Corporation	Yes	
Applied Control Solutions, LLC	Yes	
US Bureau of Reclamation	No	The requirement that the Physical Security plan be approved by a single senior manager is not appropriate. It should be sufficient to require that the entity have a management approved plan. As stated before, submissions from the regional entities in geographically diverse entities pass through and are certified by the entity's compliance POC and represent an official entity position and commitment to action. To require more adds an unnecessary organizational and administrative burden.

Organization	Yes or No	Question 5 Comment
Response: **The requirement specifically provides for the Senior Manager or delegate(s) to approve the plan, thereby providing enough flexibility while maintaining a specific chain of authority.**		
Orange and Rockland Utilities Inc.	No	1) We recommend changing R1.2 from "Identification of all access points" to "Identification of all physical access points" 2) We request a correction to R1.4 which references R3. We believe this is now R4. 3) Regarding R1.6, we are concerned with the new word "continuous," it will be difficult to demonstrate compliance. Requirements need to be auditable, measurable and enforceable. We request removing "continuous." 4) We recommend changing R1.7 from "within thirty calendar days of the completion of any" to "within thirty calendar days of completion of the Entity's Change Process for any"
Response: **1) Adding "physical" to access point in R1.2 - the drafting team feels that it is clear that the access points are "physical" since the requirement is directed at Physical Security Perimeters.** **2) The drafting team agrees and will implement this change.** **3) The drafting team feels that 'continuous' is a clarification of an active process of escorting as opposed to just being in the same room as an individual (i.e. escorted).** **4) Phase 1 of this project includes necessary modifications to CIP-002-1 through CIP-009-1 to comply with the near term specific directives included in FERC Order 706. The issue identified in your comment is an issue better suited for a later phase of this project. The SDT suggests that you review the changes proposed in the later phases of the project and resubmit your comments as appropriate if they have not been addressed.**		
CenterPoint Energy	No	An additional modification that was proposed by the SDT in R1.7 reduced the amount of time allowed for making changes and updates to the physical security plan from 90 days to 30 days. CenterPoint Energy strongly disagrees with this change. Furthermore, the Commission did not direct this change in Order 706 or Order 706A. CenterPoint Energy believes 30 days is too constraining and unwarranted, and that 90 days should be retained. If the SDT moves forward with the proposed reduction in time, CenterPoint Energy proposes 60 days to allow for a complete review of any physical security plan changes.

Organization	Yes or No	Question 5 Comment
Response: **The drafting team understands your concerns, however for consistency across all CIP standards, short term implementations were reduced from 90 days to 30 days.**		
Manitoba Hydro	No	The wording in R2 should be: "Cyber Assets used in the access control and/or monitoring and/or logging access to the Physical Security Perimeter(s)", to reflect similar wording in R3, and to include other devices or systems used in access control, such as authentication systems.
Response: **Issues such as clarifying the difference between logging and monitoring will be addressed in Phase 2. Please use the Phase 2 comment period if you feel that your concerns were not addressed.**		
Alberta Electric System Operator	Yes	R1.1 is missing the word, "critical" for Cyber Assets. There is no need to have a requirement for assets that are not critical.
Response: **Requirement 1.1 specifically addresses Cyber Assets and not the subset of Critical Cyber Assets. Any device that is within the same Electronic Security Perimeter as a Critical Cyber Asset must be within a Physical Security Perimeter and hence must be addressed within the Physical Security plan.**		
Dynegy	No	1. Recommend changing R1.2 to require identification of all "physical" access points. 2. Correct R1.4 to reference R4 instead of R3. 3. Eliminate "continuous" from R1.6. This term is not auditable.
Response: **1. Adding "physical" to access point in R1.2 - the drafting team feels that it is clear that the access points are "physical" since the requirement is directed at Physical Security Perimeters.** **2. The drafting team agrees and will implement this change.** **3. The drafting team feels that 'continuous' is a clarification of an active process of escorting as opposed to just being in the same room as an individual (i.e. escorted).**		

Organization	Yes or No	Question 5 Comment
Northern Indiana Public Service Company	No	In future drafts I would encourage the drafting team to enable track changes on the modifications to the requirements numbers as well as the text. Modifications to requirement numbers, especially in CIP-006-2 were not consistently red-lined to display where the content was formerly referenced in the existing CIP-006-1. Regarding CIP-006-2 R2 I would request a clarification on scope and depth of the cyber assets that authorize and/or log access to the PSP. The previous language would have limited the devices to those that performed control and monitoring of the PSP (traditional physical access control security systems, and localized panels that communicate with the main system). The new language provided in the draft under CIP-006-2 R2 modifies the scope to include cyber assets that authorize and/or log access to the PSP. I am concerned with the depth of devices involved in the authorization or logging chain. Specifically: log correlation servers, backup and recovery servers, camera's, badge printing workstations, camera monitoring stations, log printers, etc.. In the current draft it is unclear whether the device performing the authorization and/or logging is the only cyber asset that is subject to the requirements specified in CIP-006-2 R2.1-R2.2 or if all devices involved in authorization or logging are subject to those requirements specified in CIP-006-2 R2.1-R2.2. I feel that additional language needs to be provided to clarify the scope and depth of the devices to be included under the classification of cyber assets that authorize and/or log access to the PSP. Regarding CIP-006-2 R3 I reiterate my request for a clarification on scope and depth of the devices to be included in the access control and/or monitoring of the ESP. The previous language would have limited the devices to those that performed access control and monitoring of the ESP (traditional Firewalls, routers with ACL's, any IPS devices, VPN endpoints, etc.). The new language provided in the draft under CIP-005-2 R1.5 modifies the scope to include cyber assets used in the access control and/or monitoring of the ESP. I am concerned with the depth of devices involved in the monitoring chain that have no relevance on access control, but are an active component in the monitoring of the ESP. Specifically: log correlation servers, SNMP trap servers, SMTP relay servers for notification, pagers, blackberry's, enterprise email servers, backup and recovery servers for these extended devices, etc.. In the current draft it is unclear whether the device performing the monitoring is the only device that is subject to the requirements specified in CIP-005-2 R1.5 or if all devices involved in monitoring are subject to those requirements specified in CIP-005-2 R1.5. I feel that additional language needs to be provided to clarify the scope and depth of the devices to be included under the classification of cyber assets used in the monitoring of the ESP. When providing the scope and depth clarification of these cyber assets, the drafting team needs to give consideration in regards to an entities ability to satisfy the new CIP-006-2 R3 requirements of containing all of the cyber assets used in the access control and/or monitoring within an identified PSP. In regards to CIP-006-2 R4-R6, I believe the sub requirement identifiers were removed as they are not specific requirements, but rather a means to satisfy the requirement. I believe the bullet items need some level of identifier for reference purpose. Potentially a B4.1, B4.2, etc. this would allow for an entity to

Organization	Yes or No	Question 5 Comment
		reference the manner in which they satisfy the requirement.
Response: **The drafting team agrees that not all of the changes were clearly identified. However, the posted version (the one that was commented on) is the official version, and while the drafting team did renumber some of the requirements, these are consistent across the reliability standards.** **In relation to your comments on CIP-006-2 R2 and R3, the intent of the modification was to clarify that a device that performs either function must be included. However an unintended consequence of this change was to add ambiguity as to what constitutes a monitoring device. The intent is to only include devices that perform access control and/or monitoring as identified in CIP-005 R2 and R3 and not those devices that are receiving alerts.** **Phase 1 of this project includes necessary modifications to CIP-002-1 through CIP-009-1 to comply with the near term specific directives included in FERC Order 706. The issue identified in your comment is an issue better suited for a later phase of this project. The SDT suggests that you review the changes proposed in the later phases of the project and resubmit your comments as appropriate if they have not been addressed.** **With respect to your comments on CIP-006-2 R4-R6, while the drafting team did renumber some of the requirements, these are consistent across reliability standards. The changes from individual sub-requirements to bullets were made to correct an original error where requirements cannot be levied upon an item that may not be implemented.**		
CoreTrace		
Oncor Electric Delivery LLC	Yes	
Illinois Municipal Electric Agency		
Ontario Power Generation	No	Requirement R2.1 will limit the ability of entities to leverage existing personnel to perform such duties as allocating access cards to legitimate visitors. Such duties are frequently delegated to trained reception personnel. OPG believes that allowance must be made for workstations in reception areas and selected offices areas (e.g. Human Resources departments). Cyber controls such as dual authentication on the workstation would be sufficient to meet the protective needs of the system. As noted earlier with respect to CIP 005-2 R1.5, OPG believes that CIP-006-2 R3 creates issues where an entity may be using a third party to remotely monitor and administer Cyber Assets used in the control

Organization	Yes or No	Question 5 Comment
		or monitoring of the ESP. The new requirement will require the entity to police the physical security measures of any such third party to a degree not required for third parties who may support CCAs within the ESP. OPG suggests that the requirements for Cyber Assets used in the access control and / or monitoring of the ESP require protections to the same standards as those which are used to access CCAs. With respect to R1.6 there is concern that the addition of the new word "continuous" it will be difficult to demonstrate compliance. Requirements need to be enforceable. We recommend removing "continuous". We are concerned with the change in R1.7 reducing the time to update the Physical Security Plan from 90 to 30 calendar days. In a large organization this timeframe may not be achievable. Changes to CIP-006 R1.1 open up concerns about the protection of non- Critical Cyber Asset components such as cables. To eliminate this concern we request that the wording of the last sentence be returned to read "Where a completely enclosed ("six-wall") border cannot be established, the Responsible Entity shall deploy and document alternative measures to control physical access to the Critical Cyber Assets."
Response: **Any device that has the ability to authorize and or log access to Physical Security Perimeters must be physically protected per requirement CIP-006-2 R2.** **Relating to your comment on CIP-006-2 R3, the Requirements apply regardless of who performs the functions.** **The drafting team feels that 'continuous' is a clarification of an active process of escorting as opposed to just being in the same room as an individual (i.e., escorted).** **For consistency across all CIP standards, short term implementations were reduced from 90 days to 30 days.** **Requirement 1.1 specifically addresses Cyber Assets and not a subset of Critical Cyber Assets. Any device that is within the same Electronic Security Perimeter as a Critical Cyber Asset must be within a Physical Security Perimeter, and hence must be addressed within the Physical Security plan**		
American Electric Power	Yes	Refer to comments provided in questions 1 and 13.

Organization	Yes or No	Question 5 Comment
Response: **"Responsible Entity" is defined within the Applicability section of each CIP standard.** **The ERO Rules of Procedure include sections on dealing with confidential data associated with the Cyber Security standards, and recognize that there may be some evidence retained by the Responsible Entity. The data retention section of these standards was written to support this concept.** **Phase 1 of this project includes necessary modifications to CIP-002-1 through CIP-009-1 to comply with the near term specific directives included in FERC Order 706. The issue identified in your comment is an issue better suited for a later phase of this project. The SDT suggests that you review the changes proposed in the later phases of the project and resubmit your comments as appropriate if they have not been addressed.**		
Ontario IESO	No	With respect to individual bullet points: (i) R1: The reference to the Senior Manager should also refer to CIP-003 R2 to clarify the requirement. (ii) CIP-006 R1.6 should not require "continuous" escorted access, since demonstrating compliance with such requirement would be impossible. As an alternative, wording might indicate that visitors are to be escorted in a manner that ensures their actions can be supervised and unauthorized disclosures prevented, and/or only authorized employees can be escorts. (iii) We recommend changing R1.2 from "Identification of all access points" to "Identification of all physical access points" (iv) R1.4, reference to R3 should read R4.
Response: **(i) The drafting team feels we made this distinction by the change from "a Senior Manager" to "the Senior Manager".** **(ii) The drafting team feels that 'continuous' is a clarification of an active process of escorting as opposed to just being in the same room as an individual (i.e., escorted).** **(iii) The drafting team feels the statement is clear that the access points are "physical" since the requirement is directed at Physical Security Perimeters.** **(iv) The drafting team agrees and will implement this change.**		

Organization	Yes or No	Question 5 Comment
Ameren	Yes	
Consumers Energy Company	Yes	
Xcel Energy	No	Xcel Energy feels strongly that 30 days is too short of a time frame to get drawings updated, Sr. Management approval,..etc. every time there is a change to the plan. We feel that 60 calendar days is more attainable industry-wide.
Response: **The drafting team understands your concerns, however for consistency across all CIP standards, short term implementations were reduced from 90 days to 30 days.**		
ISO New England Inc	No	1) We recommend changing R1.2 from "Identification of all access points" to "Identification of all physical access points" 2) We request a correction to R1.4 which references R3. We believe this is now R4. 3) Regarding R1.6, we are concerned with the new word "continuous." it is subjective and will be difficult to demonstrate compliance. Requirements need to be auditable, measurable and enforceable. We request removing "continuous." 4) We recommend changing R1.7 from "within thirty calendar daysof the completion of any" to "within thirty calendar days of completion of the Entity's Change Process for any"
Response: **1) Adding "physical" to access point in R1.2 - the drafting team feels that it is clear that the access points are "physical" since the requirement is directed at Physical Security Perimeters.** **2) The drafting team agrees and will implement this change.** **3) The drafting team feels that 'continuous' is a clarification of an active process of escorting as opposed to just being in the same room as an individual (i.e. escorted).** **4) Phase 1 of this project includes necessary modifications to CIP-002-1 through CIP-009-1 to comply with the near term specific directives included in FERC Order 706. The issue identified in your comment is an issue better suited for a later phase of this project. The SDT suggests that you review the changes proposed in the later phases of the project and resubmit your**		

Organization	Yes or No	Question 5 Comment
comments as appropriate if they have not been addressed.		
American Transmission Company	Yes	
TVA	No	We agree with all except, CIP-006 R1.6. CIP-006 R1.6 requires a "continuous" escort. We agree that performing escort duties in a manner that ensures visitors actions are supervised and malicious attempts are prevented is critical. However, being able to provide auditable proof of "continuous" escorting creates a condition that is impossible to meet. We propose the following: R1.6: Policy and procedures describing roles, responsibilities, and corrective action in regard to escorting personnel not authorized for unescorted access within the Physical Security Perimeter. We would also recommend that Responsible Entitie obtain a signature for record from individuals performing escort duties demonstrating that they acknowledge and accept their role and responsibilities and understand what corrective actions will be taken for any breach in procedure.
Response: **The drafting team feels that 'continuous' is a clarification of an active process of escorting as opposed to just being in the same room as an individual (i.e., escorted).**		
Duke Energy	No	The language introduced in R2 and R3 has created an inconsistency with the use of the phrases "authorize and/or log access" and " access control and/or monitoring". This creates confusion and opportunity for differing interpretations of the requirements.
Response: **Issues such as inconsistencies will be addressed in Phase 2. Please resubmit your comments during the Phase 2 comment period if you feel that your concerns have not been addressed.**		
Brazos Electric Power Cooperative, Inc.	No	In R1.3, replace "the perimeter(s)" with "the Physical Security Perimeter(s)". In R8.3, need to clarify what "outage records" are. In M2, replace "shall make available documentation that" with "shall make available documentation showing how " In M3, replace "shall make available documentation that" with "shall make available documentation

Organization	Yes or No	Question 5 Comment
		showing how".
Response: **The drafting team feels it is clear that the perimeters are "physical" since the requirement is directed at Physical Security Perimeters. Requirement 1.3 is a sub requirement of R1, "Physical Security Plan".** **With respect to your comments on R8.3, M2, and M3 issues, these will be addressed in Phase 2. Please use the Phase 2 comment period if you feel that your concerns have not been addressed.**		
Progress Energy	Yes	CIP006R1.7 – We believe the reduction of 90 to 30 days for updates to the Physical Security Plan is inadequate when you consider the number and levels of approvals required to complete the updates. PE recommends leaving the 90 day time period.
Response: **For consistency across all CIP standards, short term implementations were reduced from 90 days to 30 days.**		
Standards Review Committee of ISO/RTO Council	No	(i) R1: We recommend revising "the Senior manager" to "a senior manager" as the requirement should not be job title specific. Further, the reference to "a Senior Manager" also should be made to CIP-003 R2 to clarify the requirement. (ii) CIP-006 R1.6 should not require "continuous" escorted access, insofar as that would create a condition that is impossible to prove to auditors. As an alternative, wording might indicate that visitors are to be escorted in a manner to ensure their actions can be supervised and unauthorized disclosures prevented, and/or only authorized employees can be escorts. (iii) We recommend changing R1.2 from "Identification of all access points" to "Identification of all physical access points" (iv) R1.4, reference to R3 should read R4.
Response: **(i) The drafting team feels it made this distinction by the change from "a Senior Manager" to "the Senior Manager".** **(ii) The drafting team feels that 'continuous' is a clarification of an active process of escorting as opposed to just being in the same room as an individual (i.e., escorted).**		

Organization	Yes or No	Question 5 Comment
(iii) The drafting team feels the statement is clear that the access points are "physical" since the requirement is directed at Physical Security Perimeters. **(iv) The drafting team agrees and will implement this change.**		
KEMA	Yes	In R4 and R6, access control and logging should include in and out of the Critical Facility in accordance to NERC's Security Guidelines for the Electricity Sector: Physical Security--Substations Dated 10-2004. Responsible entities should control and log in and out access to Critical Facilities to maintain a high level of access security to Critical Cyber Assets.
Response: **Phase 1 of this project includes necessary modifications to CIP-002-1 through CIP-009-1 to comply with the near term specific directives included in FERC Order 706. The issue identified in your comment is an issue better suited for a later phase of this project. The SDT suggests that you review the changes proposed in the later phases of the project and resubmit your comments as appropriate if they have not been addressed.**		
Austin Energy	No	The original stated intent of the Standards was to protect against 'cyber' attacks. Modifications to R2 would seem to overstep the intent in the case where a separate non-critical system was used the monitor assess to Critical Cyber Assets (CCA). Now if the CCA was itself incorporated into the physical assess monitoring then the modification to R2 is self evident. However, when a separate system is employed, it takes a coordinated effort by humans with a physical presence to pull off an attack. Although this may certainly qualify as espionage, there is nothing 'cyber' about it. It is proposed that an exception be made for cases where a separate system is used to monitor CCA.
Response: **The original standards were to protect the Cyber Assets from both cyber and physical attacks. While most of the standards deal with cyber protections, the easiest method to successfully attack a cyber asset is through physical means. The modifications in CIP-006 clarify cyber protections afforded to the systems that assist in the physical protection, including access and monitoring.** **The SDT will clarify that monitoring systems that do not authenticate and/or grant physical access are excluded from this requirement. An example would be a CCTV system that performs the monitoring role and also supports access logging, but does not control the Physical Security Perimeter access point.**		
Kansas City Power &	Yes	

Organization	Yes or No	Question 5 Comment
Light		
San Diego Gas and Electric Co.	No	SDG&E has the following comment to make about CIP-006-2 R2.1: This requirements states that cyber assets that authorize and/or log access to PSPs must be "protected from unauthorized physical access." In addition, R2.2 states that these cyber assets must be afforded the protective measures specified in, among others, CIP-006-2 R4, which addresses physical access control. Including both of these statements seems redundant. We recommend removing R2.1 and appending the text of R2.2 to R2 (thus allowing the deletion of R2.2)
Response: **The SDT respectfully disagrees with the comment. The Reference in R2.2 to CIP-006-2, R4, defines the procedural and operational control requirements for the Physical Security Perimeter access points (e.g., doors with card access readers or other access authentication processes). R2.1 refers specifically to protecting the authorization and logging systems, recognizing that in some cases it is not practical to require that the systems reside within a defined Physical Security Perimeter.**		

6. The CSO706 SDT is proposing the following modifications to **CIP 007-1:**

   - Add "implement" to CIP-007-1 Requirements R2, R3 and R7 to clarify that processes and procedures must be implemented as well as documented.
   - Remove the "acceptance of risk" language (per FERC Order 706, paragraph 622) in Requirements R2.3, R3.2 and R4.1.
   - Revise the timeframe for documenting changes to systems or controls to thirty days in Requirement R9.

   Do you agree with the proposed modifications? If not, please explain and provide an alternative to the proposed modification that would eliminate or minimize your disagreement.

Summary Consideration:

Organization	Yes or No	Question 6 Comment
Detroit Edison Company	Yes	
PacifiCorp	No	Other comment: R5.3 - Instead of prescribing specific password construction standards, it would be better to express desired outcomes in terms of measurable entropy. The standards should require a certain level of protection against password guessing and brute force "hash cracking" attacks, but leave specifics to the implementers. For example, the standard could simply require 24 bits min-entropy per NIST Special Publication 800-63.
Response: **R5.3 was not changed during this revision of the CIP standards. These types of issues will be addressed in Phase 2. Please resubmit your comments during the Phase 2 comment period if you feel that your concerns have not been addressed.**		
FirstEnergy Corp	Yes	
MidAmerican Energy Company	No	Comment: MidAmerican does not agree with the change within the Purpose section of the standard to change the term ?non-critical? to ?other.? MEC proposes the following language Purpose: Standard CIP-007-2 requires Responsible Entities to define methods, processes, and procedures for securing those systems determined to be Critical Cyber Assets, as well as the non-critical (delete other) cyber assets and cyber assets used in access control and/or monitoring within the Electronic Security Perimeter(s) . Standard CIP- 007-2 should be read as part of a group of standards numbered Standards CIP-002-2 through CIP-009-2.

Organization	Yes or No	Question 6 Comment
Response: **The word "non-critical" will be put back into the purpose statement within parentheses beside the word other [i.e "other (non-critical)"], which is similar to the structure in the implementation plan. The additional wording is meant to remove ambiguity.**		
Northeast Power Coordinating Council	No	We recommend changing R9 from "within thirty calendar days of the change being completed" to "within thirty calendar days of completion of the entity's change process."
Response: **Each entity's change process may be different and processes may include a number of steps to be performed after the actual change is completed over an extended period of time. The proposed wording would not drive a consistent approach to having documentation completed within thirty days of the actual modification to the systems or controls.**		
WECC Reliability Coordination	No	R2.3, R3.2 and R4.1 removes an organizations ability to accept minimal risk which cannot be compensated for.R9, we think 90 days is a reasonable time frame, 30 days is too restrictive.
Response: **FERC has directed the ERO to have the technical feasibility exception process supersede all instances of acceptance of risk. For example, Responsible Entities should implement the requirements for ports and services for all cyber assets within an electronic security perimeter or justify why it is not doing so pursuant to technical feasibility exceptions including reporting requirements and the implementation of compensating measures. The drafting team feels that one entity cannot accept risk for another entity in an interconnected power system. Where requirements cannot be met due to technical, safety, or operational limitations, those limitations are to be treated and documented according to a technical feasibility exception process (Please refer to FERC Order 706, Paragraph 151).** **(FERC Order 706 Paragraph 651) "… 30 days should provide sufficient time to update any necessary documentation with exceptions granted by the Regional Entity for extraordinary circumstances. The Commission believes that having correct documentation of methods, processes, and procedures for securing a responsible entity's system is necessary because if an event occurred before documentation was updated, an operator may not know of a change and could operate the system using out of date information. This puts reliability at risk by not informing operators of a method, process, or procedure to secure the system against a known risk." The SDT agrees with this position. Further, the 30 day period begins upon final implementation of the changes. At that point, much of the due diligence should already be completed related to the actual implementation with final documentation to follow within 30 days.**		
Southern Company	Yes	CIP-007 Section D - Compliance: 1.1.1 does not specify who is responsible for the enforcement authority.

Organization	Yes or No	Question 6 Comment
		CIP-007 Section D - Compliance: 1.4.1 - Indefinite retention is not feasible, overall cost of storage depending on scope could potentially be very large. Item should define an upper bound of the request (e.g. a maximum of 3 years) CIP-007 Section D - Compliance: 1.4.3 - Should have a time limit to reduce the overall liability of confidential information.
Response: **1.1.1 - The Regional Entity will serve as the Compliance Enforcement Authority for most entities. As the Regional Entity may not audit itself, the ERO will serve as the Compliance Enforcement Authority in auditing the Regional Entity. A third-party monitor without a vested interest in the outcome will serve as the Compliance Enforcement Authority for NERC. (Refer to NERC's Rules of Procedure, Paragraphs 404 and 405).** **1.4.1 – With the exception of retaining evidence in support of an investigation, the standard defines a finite retention period. The language that indicates the Compliance Enforcement Authority may direct the responsible entity to retain evidence for a longer period of time as part of an investigation is a restatement of what is included in the ERO Rules of Procedure. Reference the ERO Rules of Procedure Appendix 4C – Uniform Compliance Monitoring and Enforcement Procedures – Section 3.4.1 Compliance Violation Investigation Process Steps. While the duration of an investigation cannot be predicted, further clarification of the retention timeframe is outside the scope of the SDT.** **1.4.3 – This language supports the regularly scheduled audit intervals for all entities and supports the need to retain the confidentiality of some data. The audit data retention period is determined by the audit period for each Registered Entity.**		
Luminant Power	Yes	
Encari	No	1. We recommend striking the following language from the Purpose section - "those systems determined to be Critical Cyber Asset, as well as the other". – General Comments Pertaining to All Standards--Other modifications were also made to this standard that are not included as part of the question. 2. The wording of 1.1.1 is awkward and should be modified. 3. We also request further clarification regarding the Data Retention Requirement 1.4.2 as to which entity will be maintaining the last audit records and submitted subsequent audit records. As the statement is currently worded "in conjunction" leaves this open to interpretation.
Response: **1) The word non-critical will be added back into the purpose statement within parentheses beside the word other [i.e "other (non-**		

Organization	Yes or No	Question 6 Comment
		critical)"], which is similar to the structure in the implementation plan. The additional wording is meant to remove any ambiguity. 2) The intent of the wording in 1.1.1 is to clarify which entity will serve as the Compliance Enforcement Authority. For most standards, the Regional Entity serves as the Compliance Enforcement Authority and audits the performance of the Reliability Coordinator, Transmission Operator, Balancing Authority, Generator Operator, Generator Owner, etc. In this standard, the Regional Entity is responsible for some of the requirements – but an entity cannot audit its own performance. Where the Regional Entity is also the responsible entity, the ERO will audit the Regional Entity's performance. Where the ERO is the responsible entity, a third-party monitor without vested interest in the outcome will conduct the audit. 3) The data retention periods for the standard requirements are specified in the standards. If a standard does not specify any data retention period, then there are default periods in the Compliance Monitoring and Enforcement Procedures –and in general, the default data retention periods are longer than the periods specified in the standards. The compliance staff worked to develop guidelines that drafting teams could use to determine reasonable data retention periods – trying to balance the needs of the compliance program to have sufficient evidence to review to determine compliance, with the burden to responsible entities of collecting and retaining that evidence. The language of 1.4.2 indicates that the Compliance Enforcement Authority "in conjunction with" the Registered Entity will retain all audit records from the previous audit and all audit records submitted since the previous audit, until completion of the next audit. This supports the audit intervals for all entities and supports the need to retain the confidentiality of some data. The audit data retention period is determined by the audit period for each Registered Entity. The Reliability Coordinator, Transmission Operator and Balancing Authority are audited for each requirement once every three years – and all others are audited once every six years. The intent is to assure that, if there was an event and the performance of an entity was in question, there would be, at a minimum, at least one record showing the past performance of that entity.
TransAlta Centralia Generation, LLC	Yes	
Bonneville Power Administration	Yes	
Consolidated Edison Company of New York, Inc.	No	We recommend changing R9 from "within thirty calendar days of the change being completed" to "within thirty calendar days of completion of the Entity's Change Process." See comments to question 5.
Response: Since each entity's change process may be different and since processes may include a number of steps to be performed after the actual change is completed over an extended period of time, the newly proposed wording will not drive consistency in having documentation completed within thirty days of the actual modification to the systems or controls.		

Organization	Yes or No	Question 6 Comment
Southern California Edison Company	No	The change from 90 days to 30 days is difficult to achieve. SCE suggests 60 days to provide ample time for internal due diligence.
Response: **(FERC Order 706 Paragraph 651) "… 30 days should provide sufficient time to update any necessary documentation with exceptions granted by the Regional Entity for extraordinary circumstances. The Commission believes that having correct documentation of methods, processes, and procedures for securing a responsible entity's system is necessary because if an event occurred before documentation was updated, an operator may not know of a change and could operate the system using out of date information. This puts reliability at risk by not informing operators of a method, process, or procedure to secure the system against a known risk." The SDT agrees with this position. Further, the 30 day period begins upon final implementation of the changes. At that point, much of the due diligence should already be completed related to the actual implementation with final documentation to follow within 30 days.**		
Tampa Electric Company	No	Section 1.5 Regarding the removal of the language in Section 1.5: Additional Compliance Information: It is not clear if removal of this language is implying that authorized exceptions result in non-compliance. There are situations where requirements of this standard cannot be met, particularly for legacy equipment and associated vendor supplied systems. The following language should be reinstated in the standard: "Duly authorized exceptions will not result in non-compliance."
Response: **Situations where the standards requirements cannot be met will be handled through the Technical Feasibility Exception process under the NERC Rules of Procedure. The technical feasibility exception process will address the requirements for documenting, approving, and remediating the exception. Any sanction decisions will arise from the TFE process. It is not appropriate to assert that "duly authorized exceptions will not result in non-compliance" within Section D-1.5 of the standard.**		
Electric Market Policy	Yes	NERC (Step 4.1.10) and Regional Entity (Step 4.1.11) are not defined in the NERC Glossary of Terms or Functional Model.
Response: **NERC and Regional Entity are defined in NERC's corporate documents including, but not limited to, the Certificate of Incorporation and ByLaws.**		
PPL Corporation	Yes	We fully support the revisions in section B, Requirements.

Organization	Yes or No	Question 6 Comment
Response: **Thank you for your comment.**		
MRO NERC Standards Review Subcommittee	No	The MRO NSRS do not agree with the change within the Purpose section of the standard to change the term “non-critical” to “other.” The term "other" is too vague. The MRO NSRS proposes the following language: Purpose: Standard CIP-007-2 requires Responsible Entities to define methods, processes, and procedures for securing those systems determined to be Critical Cyber Assets, as well as the non-critical (delete other) cyber assets and cyber assets used in access control and/or monitoring within the Electronic Security Perimeter(s) . Standard CIP- 007-2 should be read as part of a group of standards numbered Standards CIP-002-2 through CIP-009-2.
Response: **The word non-critical will be added back into the purpose statement within parentheses beside the word other [i.e “other (non-critical)”], which is similar to the structure in the implementation plan. The additional wording is meant to remove any ambiguity.**		
Pepco Holdings, Inc - Affiliates		
United Illuminating Company	Yes	
Deloitte& Touche, LLP	Yes	With the adoption of "implement", will the drafting team release a FAQ on what entities and auditors should consider for evidence of compliance of implementation (i.e., a documentation of a formal security management program that has ownership, stakeholders, documented narratives & workflows, risk assessment and internal control testing).
Response: **Reliability standards are limited to specifying what to do, not how to do it.** **Please refer to NERC Rules of Procedure Appendix 4C Compliance Process.**		
Exelon	No	Recommendation to increase the timeframe in R9 to document changes to systems or controls to 60 days from 30 days. Reason for the recommendation is 30 days is not a sufficient time period to accomplish this level of change management on documentation.

Organization	Yes or No	Question 6 Comment
Response: **(FERC Order 706 Paragraph 651) "… 30 days should provide sufficient time to update any necessary documentation with exceptions granted by the Regional Entity for extraordinary circumstances. The Commission believes that having correct documentation of methods, processes, and procedures for securing a responsible entity's system is necessary because if an event occurred before documentation was updated, an operator may not know of a change and could operate the system using out of date information. This puts reliability at risk by not informing operators of a method, process, or procedure to secure the system against a known risk." The SDT agrees with this position. Further, the 30 day period begins upon final implementation of the changes. At that point, much of the due diligence should already be completed related to the actual implementation with final documentation to follow within 30 days.**		
Old Dominion Electric Cooperative		
City of Tallahassee (TAL)	Yes	Although the "acceptance of risk" ties in with the discusson above on business judgement.
Response: **The removal of "reasonable business judgment" was done in accordance with FERC Order 706. The revisions made to the standards in Phase 1 are intended to be responsive to specific FERC directives relevant to the onset of compliance audits in July 2009. The expansion of the Technical Feasibility Exception Process should address the concerns regarding the removal of reasonable business judgment and acceptance of risk.**		
BC Transmission Corporation	Yes	
Applied Control Solutions, LLC	Yes	
US Bureau of Reclamation	No	More rational is needed to explain the decision to remove "acceptance of risk" and "reasonable business judgement" language from CIP requirements while leaving the ability to identify "exceptions" through cyber security policy (CIP-003-2, R3.) With this exception in place, entities will be able to establish "policy" that will allow for deviation from the requirements outlined in the Standards. If the intent of the changes was to limit implementation disparity across all entities by removing "risk based decisions", the potential remains that an entity will establish exceptions through relaxed "policy" and the disparity will remain. If the intent was to remove any avenue for not meeting or implementing the requirements, entities may continue to accept "risk based decisions" (although not formally identified as such) by

Organization	Yes or No	Question 6 Comment
		pursuing relaxed policy via exceptions (CIP-003-2 R3).Further, entities may have numerous "systems" of differing capabilities and generations. To require that exceptions be documented in "policy" does not acknowledge the diversity of systems that may be in service in an organization in as effective a manner as documenting exceptions as a function of the system, its environment, and its criticality. Such documentation would be better addressed through specific risk-acceptance decisions tied to specific systems, rather than to an all-encompassing "policy. "Finally, as CIP-003 is amended, entities may not implement or meet certain requirements, as long as, they are identified and documented as "policy exceptions." Was this the intent of the authors? We recommend that risk-managed approaches to cyber security requirements be reinstated into the requirements, recognizing that such a change will require FERC to reassess their order.
Response: **The recommendation of using a risk-managed approach to cyber-security requirements is well appreciated and will be a significant topic in the next revision phase of the CIP Standards.** **The removal of "reasonable business judgment" was done in accordance with FERC Order 706. The revisions made to the standards in Phase 1 are intended to be responsive to specific FERC directives relevant to the onset of compliance audits in July 2009. The expansion of the Technical Feasibility Exception Process should address the concerns regarding the removal of reasonable business judgment and acceptance of risk.**		
Orange and Rockland Utilities Inc.	No	We recommend changing R9 from "within thirty calendar days of the change being completed" to "within thirty calendar days of completion of the Entity's Change Process."
Response: **Since each entity's change process may be different and since processes may include a number of steps to be performed after the actual change is completed over an extended period of time, the newly proposed wording will not drive consistency in having documentation completed within thirty days of the actual modification to the systems or controls.**		
CenterPoint Energy		
Manitoba Hydro	Yes	
Alberta Electric System Operator	Yes	
Dynegy	Yes	

Organization	Yes or No	Question 6 Comment
Northern Indiana Public Service Company	No	Within the purpose section of CIP-007-2 I would recommend the removal of the following language "those systems determined to be Critical Cyber Assets, as well as the non critical" as this language is redundant.
Response: **The word non-critical will be added back into the purpose statement within parentheses beside the word other [i.e "other (non-critical)"], which is similar to the structure in the implementation plan. The additional wording is meant to remove any ambiguity.**		
CoreTrace	No	The modifications above are acceptable, however R4.2, as written, implies that all anti-virus and malware prevention tools have signatures, which is not true. Specifically whitelisting or behavioral approaches do not require signature updates. Whitelisting in particular provides greater antivirus/antimalware protection than traditional signature based antivirus, including zero day protection, yet does NOT require "signatures". Whitelisting relies on a positive security model that complements CIP 003 Configuration Control Requirements. By clarifying that traditional signature based antivirus is not required, NERC opens up the range of platforms and systems that can be protected greatly. For example, traditional antivirus does not exist for most Unix based systems, however whitelisting does. Propose revising R4.2 to read as follows: R4.2. If the Responsible Entity chooses to implement signature based antivirus or malware prevention tools the Responsible Entity shall document and implement a process for the update of anti-virus and malware prevention ?signatures.? The process must address testing and installing the signatures. This requirement does not apply for non-signature based antivirus or malware prevention tools such as those based on whitelisting or behavioral analysis.
Response: **R4.2 was not changed during this revision of the CIP Standards. Please resubmit your comments during the Phase 2 comment period if you feel that your concerns have not been addressed.**		
Oncor Electric Delivery LLC	Yes	
Illinois Municipal Electric Agency		
Ontario Power Generation	No	Reducing the timeframe for documenting changes to systems or controls in R9 from 90 to 30 calendar days introduces a constraint that may not be achievable in a large organization.

Organization	Yes or No	Question 6 Comment
Response: **(FERC Order 706 Paragraph 651) "… 30 days should provide sufficient time to update any necessary documentation with exceptions granted by the Regional Entity for extraordinary circumstances. The Commission believes that having correct documentation of methods, processes, and procedures for securing a responsible entity's system is necessary because if an event occurred before documentation was updated, an operator may not know of a change and could operate the system using out of date information. This puts reliability at risk by not informing operators of a method, process or procedure to secure the system against a known risk." The SDT agrees with this position. Further, the 30 day period begins upon final implementation of the changes. At that point, much of the due diligence should already be completed related to the actual implementation with final documentation to follow within 30 days.**		
American Electric Power	Yes	Refer to comments provided in questions 1 and 13.
Response: **"Responsible Entity" is defined within the Applicability section of each CIP standard.** **The ERO Rules of Procedure include sections on dealing with confidential data associated with the Cyber Security standards, and recognize that there may be some evidence retained by the Responsible Entity. The data retention section of these standards was written to support this concept.** **Phase 1 of this project includes necessary modifications to CIP-002-1 through CIP-009-1 to comply with the near term specific directives included in FERC Order 706. The issue identified in your comment is an issue better suited for a later phase of this project. The SDT suggests that you review the changes proposed in the later phases of the project and resubmit your comments as appropriate if they have not been addressed.**		
Ontario IESO	Yes	
Ameren	No	Acceptance of risk for certain ports and services is within security best practices. Mitigating controls for certain ports and services could effect the reliable operation of the bulk electric system.
Response: **FERC directed the ERO to have a technical feasibility exception process supersede all instances of acceptance of risk. For example, Responsible Entities should implement the requirements for ports and services for all cyber assets within an electronic security perimeter or justify why it is not doing so pursuant to technical feasibility exceptions including reporting requirements and the implementation of compensating measures. The drafting team feels that one entity cannot accept risk for another entity in an interconnected power system. Where requirements cannot be met due to technical, safety, or operational limitations, those limitations are to be treated and documented according to a technical feasibility exception process (Please refer to FERC Order 706,**		

Organization	Yes or No	Question 6 Comment
Paragraph 151).		
Consumers Energy Company	Yes	
Xcel Energy	Yes	
ISO New England Inc	No	We recommend changing R9 from "within thirty calendar days of the change being completed" to "within thirty calendar days of completion of the Entity's Change Process."
Response: **Since each entity's change process may be different and since processes may include a number of steps to be performed after the actual change is completed over an extended period of time, the newly proposed wording will not drive consistency in having documentation completed within thirty days of the actual modification to the systems or controls.**		
American Transmission Company	Yes	
TVA	Yes	
Duke Energy	Yes	Regarding R2.3, R3.2 and R4.1, we understand that the Responsible Entity's action to document compensating measures is sufficient to achieve compliance with the requirements, and that the Responsible Entity does not need to also invoke the "Technical Feasibility" exception. Technical Feasibility is only applicable when the Responsible Entity cannot comply with a requirement. We also recommend that the Responsible Entity be required to perform an analysis of the residual risk after all compensating measures are applied. Add the words "and analysis of residual risk" to the end of R2.3, R3.2 and R4.1
Response: **FERC has directed the ERO to have the technical feasibility exception process supersede all instances of acceptance of risk. Where requirements cannot be met due to technical, safety, or operational limitations, those limitations are to be treated and documented according to a technical feasibility exception process. [Please refer to FERC 706, Paragraph 151]** **The Technical Feasibility Exception process is under development by NERC staff. Please readdress this issue during the Phase 2 comment period.**		

Organization	Yes or No	Question 6 Comment
Brazos Electric Power Cooperative, Inc.	No	1) In R5.1.1, replace "user accounts" with "user access privalges". 2) In R6.4, replace "all logs" with "all logs of system events related to cyber security". 3) In M2, replace "available documentation" with "available documentation of all ports and services".
Response: **1) All aspects of R5.1 are specific to individual and shared system accounts. User access privileges are covered in CIP-004.** **2) The requirement is to retain all logs from all applicable cyber assets for 90 days. Log retention of system events related to cyber security may be longer based on incident response and reporting plan as defined by CIP-008.** **3) The SDT reviewed and concluded that changing the wording as suggested would exclude the process documentation. It remains applicable to all documentation related to R2.**		
Progress Energy	Yes	CIP007R9 – The reduction from 90 to 30 days is inadequate. PE recommends leaving the 90 day time period (same justification as for CIP006-R1.7).
Response: **The FERC Order consistently requires a shortening of the update period and recommends 30 days. The SDT agrees with this position. Further, the 30 day period begins upon final implementation of the changes. At that point, much of the due diligence should already be completed related to the actual implementation with final documentation to follow within 30 days.**		
Standards Review Committee of ISO/RTO Council	Yes	
KEMA	Yes	
Austin Energy	Yes	
Kansas City Power & Light	Yes	
San Diego Gas and Electric Co.	Yes	

7. The CSO706 SDT modified **CIP-008-1** Requirement R1 to clarify the requirement to implement the plan in response to cyber security incidents, update the plan within thirty days of any changes, and clarify that tests of the plan do not require removing components or systems during the test.

   Do you agree with the proposed modifications? If not, please explain and provide an alternative to the proposed modification that would eliminate or minimize your disagreement.

Summary Consideration:

Organization	Yes or No	Question 7 Comment
Detroit Edison Company	No	The addition of "and implement the plan in response to Cyber Security Incidents." is awkward. This literally states that the plan will only be implemented upon a security incident, but the plan must be implemented in order to "characterize and classify" reportable Cyber Security Incidents. It might be clearer if written as " The Responsible Entity shall develop, implement and maintain a Cyber Security Incident Response Plan....and execute the plan in the event of a Cyber Security Incident." Remove the "Process for?." language in CIP-008-2 R1.4, R1.5, and R1.6 to be consistent with the language changes in CIP-006 R1.7 and R1.8. Suggested language is as follows: R1.4. Update of the Cyber Security Incident response plan within thirty calendar days of any changes.R1.5. Annual review of the Cyber Security Incident response plan.R1.6. Annual testing of the Cyber Security Incident response plan. A test of the Cyber Security Incident response plan can range from a paper drill, to a full operational exercise, to the response to an actual incident. Testing the Cyber Security Incident response plan does not require removing a component or system from service during the test.
Response: **Phase 1 of this project includes necessary modifications to CIP-002-1 through CIP-009-1 to comply with the near term specific directives included in FERC Order 706. The issue identified in your comment is an issue better suited for a later phase of this project. The SDT suggests that you review the changes proposed in the later phases of the project and resubmit your comments as appropriate if they have not been addressed.**		
PacifiCorp	Yes	
FirstEnergy Corp	Yes	
MidAmerican Energy Company	Yes	

Organization	Yes or No	Question 7 Comment
Northeast Power Coordinating Council	No	1) - We recommend changing R1 from "The Responsible Entity shall develop and maintain a Cyber Security Incident response plan and implement the plan in response to Cyber Security Incidents." to "The Responsible Entity shall develop, maintain and implement a Cyber Security Incident response plan. The plan shall be activated in response to a Cyber Security Incident." 2) - We recommend changing R1.4 from "Process for updating the Cyber Security Incident response plan within thirty calendar days of any changes" to "Process for updating the Cyber Security Incident response plan within thirty calendar days of completion of the entity's change process". 3) - Measure M1 appears to one of the few measures that specifies "dated." Please clarify "dated." Also, R1 does not specify dating a Plan. Besides inconsistency, it appears this measurement adds a requirement incorrectly.
Response: **1)-2) Phase 1 of this project includes necessary modifications to CIP-002-1 through CIP-009-1 to comply with the near term specific directives included in FERC Order 706. The issue identified in your comment is an issue better suited for a later phase of this project. The SDT suggests that you review the changes proposed in the later phases of the project and resubmit your comments as appropriate if they have not been addressed.** **3) The word "dated" will be removed at this time. The measures will be reviewed and considered in an upcoming drafting phase of these standards.**		
WECC Reliability Coordination	No	we feel that 90 days is a reasonable time frame.
Response: **The FERC Order consistently requires a shortening of the update period and recommends 30 days. The SDT agrees with this position. Further, the 30 day period begins upon final implementation of the changes. At that point, much of the due diligence should already be completed related to the actual implementation with final documentation to follow within 30 days.**		
Southern Company	Yes	CIP-008 Section D - Compliance: 1.1.1 does not specify who is responsible for the enforcement authority. CIP-008 Section D - Compliance: 1.4.1 - Indefinite retention is not feasible, overall cost of storage depending on scope could potentially be very large. Item should define an upper bound of the request (e.g. a maximum of 3 years) CIP-008 Section D - Compliance: 1.4.2 - Should have a time limit to reduce the overall liability of

Organization	Yes or No	Question 7 Comment
		confidential information.
Response: **1.1.1 - The Regional Entity will serve as the Compliance Enforcement Authority for most entities. As the Regional Entity may not audit itself, the ERO will serve as the Compliance Enforcement Authority in auditing the Regional Entity. A third-party monitor without a vested interest in the outcome will serve as the Compliance Enforcement Authority for NERC. (Refer to NERC's Rules of Procedure, Paragraphs 404 and 405).** **1.4.1 – With the exception of retaining evidence in support of an investigation, the standard defines a finite retention period. The language that indicates the Compliance Enforcement Authority may direct the responsible entity to retain evidence for a longer period of time as part of an investigation is a restatement of what is included in the ERO Rules of Procedure. Reference the ERO Rules of Procedure Appendix 4C – Uniform Compliance Monitoring and Enforcement Procedures – Section 3.4.1 Compliance Violation Investigation Process Steps. While the duration of an investigation cannot be predicted, further clarification of the retention timeframe is outside the scope of the SDT.** **1.4.2 – This language supports the regularly scheduled audit intervals for all entities and supports the need to retain the confidentiality of some data. The audit data retention period is determined by the audit period for each Registered Entity.**		
Luminant Power	Yes	
Encari	No	1. We are confused about the necessity to call out a specific "Cyber Security Incident" response team. Does this no longer require an entity to have a physical security incident response team? -- General Comments Pertaining to All Standards--Other modifications were also made to this standard that are not included as part of the question. 2. The wording of 1.1.1 is awkward and should be modified. 3. We also request further clarification regarding the Data Retention Requirement 1.4.2 as to which entity will be maintaining the last audit records and submitted subsequent audit records. As the statement is currently worded "in conjunction" leaves this open to interpretation.

Organization	Yes or No	Question 7 Comment
Response: **1. This standard relates to cyber security incident response only. An entity's physical security incident response may or may not be related.** **2) The intent of the wording in 1.1.1 is to clarify which entity will serve as the Compliance Enforcement Authority. For most standards, the Regional Entity serves as the Compliance Enforcement Authority and audits the performance of the Reliability Coordinator, Transmission Operator, Balancing Authority, Generator Operator, Generator Owner, etc. In this standard, the Regional Entity is responsible for some of the requirements – but an entity cannot audit its own performance. Where the Regional Entity is also the responsible entity, the ERO will audit the Regional Entity's performance. Where the ERO is the responsible entity, a third-party monitor without vested interest in the outcome will conduct the audit.** **3. The data retention periods for the standard requirements are specified in the standards. If a standard does not specify any data retention period, then there are default periods in the Compliance Monitoring and Enforcement Procedures –and in general, the default data retention periods are longer than the periods specified in the standards. The compliance staff worked to develop guidelines that drafting teams could use to determine reasonable data retention periods – trying to balance the needs of the compliance program to have sufficient evidence to review to determine compliance, with the burden to responsible entities of collecting and retaining that evidence.** **The language of 1.4.2 indicates that the Compliance Enforcement Authority "in conjunction with" the Registered Entity will retain all audit records from the previous audit and all audit records submitted since the previous audit, until completion of the next audit. This supports the audit intervals for all entities and supports the need to retain the confidentiality of some data.** **The audit data retention period is determined by the audit period for each Registered Entity. The Reliability Coordinator, Transmission Operator and Balancing Authority are audited for each requirement once every three years – and all others are audited once every six years. The intent is to assure that, if there was an event and the performance of an entity was in question, there would be, at a minimum, at least one record showing the past performance of that entity.**		
TransAlta Centralia Generation, LLC	Yes	
Bonneville Power Administration	Yes	
Consolidated Edison Company of New York, Inc.	No	1) - We recommend changing R1 from "The Responsible Entity shall develop and maintain a Cyber Security Incident response plan and implement the plan in response to Cyber Security Incidents." to "The Responsible Entity shall develop, maintain and implement a Cyber Security Incident response plan. The plan shall be activated in response to a Cyber Security Incident." 2) - We recommend changing R1.4 from "Process for updating the Cyber Security Incident response

Organization	Yes or No	Question 7 Comment
		plan within thirty calendar days of any changes" to "Process for updating the Cyber Security Incident response plan within thirty calendar days of completion of the Entity's Change Process" (see questions 5). 3) - The new sentence in R1.6 adds no value and may confuse - "Testing the Cyber Security Incident response plan does not require removing a component or system from service during the test." We recommend removing this new sentence 4) - Measure M1 is one of the few measures that specifies "dated." Please clarify "dated." Also, R1 does not specify dating a Plan. Besides inconsistency, it appears this measurement adds a requirement incorrectly.
Response: **1)-3) Phase 1 of this project includes necessary modifications to CIP-002-1 through CIP-009-1 to comply with the near term specific directives included in FERC Order 706. The issue identified in your comment is an issue better suited for a later phase of this project. The SDT suggests that you review the changes proposed in the later phases of the project and resubmit your comments as appropriate if they have not been addressed.** **4) The word "dated" will be removed at this time. The measures will be reviewed and considered in an upcoming drafting phase of these standards.**		
Southern California Edison Company	Yes	
Tampa Electric Company	No	Section 1.5 Regarding the removal of the language in Section 1.5 : Additional Compliance Information: It is not clear if removal of this language is implying that authorized exceptions result in non-compliance. There are situations where requirements of this standard cannot be met, particularly for legacy equipment and associated vendor supplied systems. The following language should be reinstated in the standard: "Duly authorized exceptions will not result in non-compliance."
Response: **Situations where the standards requirements cannot be met will be handled through the Technical Feasibility Exception process under the NERC Rules of Procedure. The technical feasibility exception process will address the requirements for documenting, approving, and remediating the exception. Any sanction decisions will arise from the TFE process. It is not appropriate to assert that "duly authorized exceptions will not result in non-compliance" within Section D-1.5 of the standard.**		
Electric Market Policy	Yes	NERC (Step 4.1.10) and Regional Entity (Step 4.1.11) are not defined in the NERC Glossary of Terms

Organization	Yes or No	Question 7 Comment
		or Functional Model.
Response: **NERC and Regional Entity are defined in NERC's corporate documents including, but not limited to, the Certificate of Incorporation and ByLaws.**		
PPL Corporation	No	The sentence added to the end of R1.6 would be more appropriate in a FAQ, guideline, or interpretation rather than in the standard itself.
Response: **Phase 1 of this project includes necessary modifications to CIP-002-1 through CIP-009-1 to comply with the near term specific directives included in FERC Order 706. The issue identified in your comment is an issue better suited for a later phase of this project. The SDT suggests that you review the changes proposed in the later phases of the project and resubmit your comments as appropriate if they have not been addressed.**		
MRO NERC Standards Review Subcommittee	No	The MRO NSRS questions the change in timing requirements for R1.4 from 90 days to 30 days. What is the justification for change? Do you have specific examples of problems that resulted from the plan not being updated within 90 days.
Response: **The FERC Order consistently requires a shortening of the update period and recommends 30 days. The SDT agrees with this position. Further, the 30 day period begins upon final implementation of the changes. At that point, much of the due diligence should already be completed related to the actual implementation with final documentation to follow within 30 days.**		
Pepco Holdings, Inc - Affiliates		
United Illuminating Company	Yes	
Deloitte& Touche, LLP	Yes	With the adoption of "implement", will the drafting team release a FAQ on what entities and auditors should consider for evidence of compliance of implementation (i.e. a documentation of a formal incident management program that has ownership, stakeholders, documented narratives & workflows, risk assessment and internal control testing).

Organization	Yes or No	Question 7 Comment
Response: **Reliability standards are limited to specifying what to do, not how to do it.** **Please refer to NERC Rules of Procedure Appendix 4C Compliance Process.**		
Exelon	No	Recommendation to increase the timeframe in R1.4 to document changes to the cyber security incident response plan to 60 days from 30 days. Reason for the recommendation is 30 days is not a sufficient time period to accomplish this level of change management on documentation.
Response: **The FERC Order consistently requires a shortening of the update period and recommends 30 days. The SDT agrees with this position. Further, the 30 day period begins upon final implementation of the changes. At that point, much of the due diligence should already be completed related to the actual implementation with final documentation to follow within 30 days.**		
Old Dominion Electric Cooperative		
City of Tallahassee (TAL)	Yes	
BC Transmission Corporation	Yes	
Applied Control Solutions, LLC	Yes	
US Bureau of Reclamation	Yes	
Orange and Rockland Utilities Inc.	No	1) We recommend changing R1 from "The Responsible Entity shall develop and maintain a Cyber Security Incident response plan and implement the plan in response to Cyber Security Incidents." to "The Responsible Entity shall develop, maintain, and implement a Cyber Security Incident response plan. The plan shall be activated in response to a Cyber Security Incident." 2) We recommend changing R1.4 from "Process for updating the Cyber Security Incident response plan within thirty calendar days of any changes" to "Process for updating the Cyber Security Incident response plan within within thirty calendar days of completion of the Entity's Change Process"

Organization	Yes or No	Question 7 Comment
		3) The new sentence in R1.6 adds no value and may confuse - "Testing the Cyber Security Incident response plan does not require removing a component or system from service during the test." We recommend removing this new sentence 4) Measure M1 appears to one of the few measures that specifies "dated." Please clarify "dated." Also, R1 does not specify dating a Plan. Besides inconsistency, it appears this measurement adds a requirement incorrectly.
Response: **1)-3) Phase 1 of this project includes necessary modifications to CIP-002-1 through CIP-009-1 to comply with the near term specific directives included in FERC Order 706. The issue identified in your comment is an issue better suited for a later phase of this project. The SDT suggests that you review the changes proposed in the later phases of the project and resubmit your comments as appropriate if they have not been addressed.** **4) The word "dated" will be removed at this time. The measures will be reviewed and considered in an upcoming drafting phase of these standards.**		
CenterPoint Energy	No	CenterPoint Energy strongly disagrees with the proposed modification in R1.4 reducing the amount of time allowed for making changes and updates to the Cyber Security Incident Response Plan from 90 days to 30 days. Furthermore, the Commission did not direct this change in Order 706 or Order 706A. CenterPoint Energy believes 30 days is too constraining and unwarranted, and that 90 days should be retained. If the SDT moves forward with the proposed reduction in time, CenterPoint Energy proposes 60 days to allow for a complete review of any changes.
Response: **The FERC Order consistently requires a shortening of the update period and recommends 30 days. The SDT agrees with this position. Further, the 30 day period begins upon final implementation of the changes. At that point, much of the due diligence should already be completed related to the actual implementation with final documentation to follow within 30 days.**		
Manitoba Hydro	Yes	
Alberta Electric System Operator	Yes	
Dynegy	Yes	
Northern Indiana Public	No	In CIP-008-2 R1.2, I would like a clarification of the additional language detailing Cyber Security Incident

Organization	Yes or No	Question 7 Comment
Service Company		response team requirements. This additional language implies Cyber Security specific training or a core set of knowledge requirements for the incident responders. What will be the measuring stick to determine if an incident responder is a Cyber Security Incident responder or a non-cyber security incident responder?
Response: **Team members should be able to effectively perform the roles and responsibilities outlined in the Cyber Security Incident Response Plan.** **Phase 1 of this project includes necessary modifications to CIP-002-1 through CIP-009-1 to comply with the near term specific directives included in FERC Order 706. The issue identified in your comment is an issue better suited for a later phase of this project. The SDT suggests that you review the changes proposed in the later phases of the project and resubmit your comments as appropriate if they have not been addressed.**		
CoreTrace	Yes	
Oncor Electric Delivery LLC	Yes	
Illinois Municipal Electric Agency		
Ontario Power Generation	No	Reducing the timeframe to update the Incident Response Plan from 90 to 30 calendar days introduces a constraint that may not be achievable in a large organization.
Response: **The FERC Order consistently requires a shortening of the update period and recommends 30 days. The SDT agrees with this position. Further, the 30 day period begins upon final implementation of the changes. At that point, much of the due diligence should already be completed related to the actual implementation with final documentation to follow within 30 days.**		
American Electric Power	Yes	Refer to comments provided in questions 1 and 13.
Response: **"Responsible Entity" is defined within the Applicability section of each CIP standard.** **The ERO Rules of Procedure include sections on dealing with confidential data associated with the Cyber Security standards, and recognize that there may be some evidence retained by the Responsible Entity. The data retention section of these standards was**		

Organization	Yes or No	Question 7 Comment
written to support this concept. **Phase 1 of this project includes necessary modifications to CIP-002-1 through CIP-009-1 to comply with the near term specific directives included in FERC Order 706. The issue identified in your comment is an issue better suited for a later phase of this project. The SDT suggests that you review the changes proposed in the later phases of the project and resubmit your comments as appropriate if they have not been addressed.**		
Ontario IESO	No	The new sentence in R1.6 is not a requirement and does not add any value; in fact, it may create confusion - "Testing the Cyber Security Incident response plan does not require removing a component or system from service during the test." We recommend removing this new sentence.
Response: **Phase 1 of this project includes necessary modifications to CIP-002-1 through CIP-009-1 to comply with the near term specific directives included in FERC Order 706. The issue identified in your comment is an issue better suited for a later phase of this project. The SDT suggests that you review the changes proposed in the later phases of the project and resubmit your comments as appropriate if they have not been addressed.**		
Ameren	Yes	
Consumers Energy Company	Yes	
Xcel Energy	Yes	
ISO New England Inc	No	1) - We recommend changing R1 from "The Responsible Entity shall develop and maintain a Cyber Security Incident response plan and implement the plan in response to Cyber Security Incidents." to "The Responsible Entity shall develop. and maintain a Cyber Security Incident response plan. The plan shall be activated in response to a Cyber Security Incident, when such an incident occurs." 2) - We recommend changing R1.4 from "Process for updating the Cyber Security Incident response plan within thirty calendar days of any changes" to "Process for updating the Cyber Security Incident response plan within within thirty calendar days of completion of the Entity's Change Process" 3) - The new sentence in R1.6 adds no value and may confuse - "Testing the Cyber Security Incident response plan does not require removing a component or system from service during the test." We recommend removing this new sentence 4) - Measure M1 appears to one of the few measures that specifies "dated." Please clarify "dated." Also, R1 does not specify dating a Plan. Besides inconsistency, it appears this measurement adds a

Organization	Yes or No	Question 7 Comment
		requirement incorrectly.
Response: **1)-3) Phase 1 of this project includes necessary modifications to CIP-002-1 through CIP-009-1 to comply with the near term specific directives included in FERC Order 706. The issue identified in your comment is an issue better suited for a later phase of this project. The SDT suggests that you review the changes proposed in the later phases of the project and resubmit your comments as appropriate if they have not been addressed.** **4) The word "dated" will be removed at this time. The measures will be reviewed and considered in an upcoming drafting phase of these standards.**		
American Transmission Company	Yes	
TVA	Yes	
Duke Energy	Yes	
Brazos Electric Power Cooperative, Inc.	No	In R1.3, replace "Process for reporting" with "Process for communicating reportable". In R1.4, replace "of any changes" with "of any procedural changes". In M2, replace "all documentation" with "all relevant documentation related to Cyber Security Incidents".
Response: **Phase 1 of this project includes necessary modifications to CIP-002-1 through CIP-009-1 to comply with the near term specific directives included in FERC Order 706. The issue identified in your comment is an issue better suited for a later phase of this project. The SDT suggests that you review the changes proposed in the later phases of the project and resubmit your comments as appropriate if they have not been addressed.**		
Progress Energy	Yes	CIP008R1.4 – The reduction from 90 to 30 days is inadequate considering the coordination and approvals necessary. PE recommends leaving the 90 day time period (same justification as for CIP006-R1.7).
Response: **The FERC Order consistently requires a shortening of the update period and recommends 30 days. The SDT agrees with this position. Further, the 30 day period begins upon final implementation of the changes. At that point, much of the due diligence should already be completed related to the actual implementation with final documentation to follow within 30 days.**		

Organization	Yes or No	Question 7 Comment
Standards Review Committee of ISO/RTO Council	No	The new sentence in R1.6 is not a requirement and does not add any value; in fact, it may create confusion - "Testing the Cyber Security Incident response plan does not require removing a component or system from service during the test." We recommend removing this new sentence.
Response: **Phase 1 of this project includes necessary modifications to CIP-002-1 through CIP-009-1 to comply with the near term specific directives included in FERC Order 706. The issue identified in your comment is an issue better suited for a later phase of this project. The SDT suggests that you review the changes proposed in the later phases of the project and resubmit your comments as appropriate if they have not been addressed.**		
KEMA	Yes	
Austin Energy	Yes	
Kansas City Power & Light	Yes	
San Diego Gas and Electric Co.	Yes	

8. The CSO706 SDT revised the timeframe to thirty days for communicating updates of recovery plans to personnel responsible for activating or implementing the plan in **CIP-009-1** Requirement R3.

   Do you agree with the proposed modifications? If not, please explain and provide an alternative to the proposed modification that would eliminate or minimize your disagreement.

Summary Consideration:

Organization	Yes or No	Question 8 Comment
Detroit Edison Company	Yes	
PacifiCorp	Yes	
FirstEnergy Corp	Yes	
MidAmerican Energy Company	Yes	
Northeast Power Coordinating Council	No	1) We recommend changing R3 from "Updates shall be communicated to personnel responsible for the activation and implementation of the recovery plan(s) within thirty calendar days of the change being completed." to "Updates shall be communicated to personnel responsible for the activation and implementation of the recovery plan(s) within thirty calendar days of completion of the entity's change process." 2) "Dated" is used only in the Measures (M1, M2, M3, M4, M5). Adding a requirement in the measures is inappropriate.

Response:

1) The FERC Order consistently requires a shortening of the update period and communication of the updates to personnel responsible for the activation, and the Order recommends 30 days. The SDT agrees with this position. Further, the 30 day period begins upon final implementation of the changes. At that point, much of the due diligence should already be completed related to the actual implementation with final documentation to follow within 30 days.

2) **The word "dated" will be removed at this time. The measures will be reviewed and considered in an upcoming drafting phase of these standards.**

Organization	Yes or No	Question 8 Comment
WECC Relibaility Coordination	No	We feel 90 days is a reasonable time frame.
Response: **The FERC Order consistently requires a shortening of the update period and communication of the updates to personnel responsible for the activation, and the Order recommends 30 days. The SDT agrees with this position. Further, the 30 day period begins upon final implementation of the changes. At that point, much of the due diligence should already be completed related to the actual implementation with final documentation to follow within 30 days.**		
Southern Company	Yes	
Luminant Power	Yes	
Encari	No	General Comments Pertaining to All Standards--Other modifications were also made to this standard that are not included as part of the question. 1) The wording of 1.1.1 is awkward and should be modified. 2) We also request further clarification regarding the Data Retention Requirement 1.4.2 as to which entity will be maintaining the last audit records and submitted subsequent audit records. As the statement is currently worded "in conjunction" leaves this open to interpretation.
Response: **1) The intent of the wording in 1.1.1 is to clarify which entity will serve as the Compliance Enforcement Authority. For most standards, the Regional Entity serves as the Compliance Enforcement Authority and audits the performance of the Reliability Coordinator, Transmission Operator, Balancing Authority, Generator Operator, Generator Owner, etc. In this standard, the Regional Entity is responsible for some of the requirements – but an entity cannot audit its own performance. Where the Regional Entity is also the responsible entity, the ERO will audit the Regional Entity's performance. Where the ERO is the responsible entity, a third-party monitor without vested interest in the outcome will conduct the audit.** **2) The data retention periods for the standard requirements are specified in the standards. The language of 1.4.2 indicates that the Compliance Enforcement Authority and the Registered Entity will retain all the audit records from the previous audit and all audit records submitted since the previous audit, until completion of the next audit. This supports the audit intervals for all entities. The audit data retention period is determined by the audit period for each Registered Entity.** **The phrase, "in conjunction with" was deliberately used to recognize that there may be some confidential records that fall into the category of "critical energy infrastructure information" as defined in the ERO Rules of Procedure – and the responsible entity**		

Organization	Yes or No	Question 8 Comment
has the right to retain control over these records. Most other records will be retained by the Compliance Enforcement Authority.		
TransAlta Centralia Generation, LLC	Yes	
Bonneville Power Administration	Yes	
Consolidated Edison Company of New York, Inc.	No	1) We recommend changing R3 from "Updates shall becommunicated to personnel responsible for the activation and implementation of the recoveryplan(s) within thirty calendar days of the change being completed." to "Updates shall becommunicated to personnel responsible for the activation and implementation of the recoveryplan(s) within thirty calendar days of completion of the Entity's change process." 2) "Dated" is used only in the Measures (M1, M2, M3, M4, M5). Adding a requirement in the measures is inappropriate
Response: **1) Phase 1 of this project includes necessary modifications to CIP-002-1 through CIP-009-1 to comply with the near term specific directives included in FERC Order 706. The issue identified in your comment is an issue better suited for a later phase of this project. The SDT suggests that you review the changes proposed in the later phases of the project and resubmit your comments as appropriate if they have not been addressed.** **2) The word "dated" will be removed at this time. The measures will be reviewed and considered in an upcoming drafting phase of these standards.**		
Southern California Edison Company	Yes	
Tampa Electric Company	No	Section 1.5 Regarding the removal of the language in Section 1.5 : Additional Compliance Information: It is not clear if removal of this language is implying that authorized exceptions result in non-compliance. There are situations where requirements of this standard cannot be met, particularly for legacy equipment and associated vendor supplied systems. The following language should be reinstated in the standard: "Duly authorized exceptions will not result in non-compliance."

Organization	Yes or No	Question 8 Comment
Response: **Situations where the standards requirements cannot be met will be handled through the Technical Feasibility Exception process under the NERC Rules of Procedure. The technical feasibility exception process will address the requirements for documenting, approving, and remediating the exception. Any sanction decisions will arise from the TFE process. It is not appropriate to assert that "duly authorized exceptions will not result in non-compliance" within Section D-1.5 of the standard.**		
Electric Market Policy	Yes	NERC (Step 4.1.10) and Regional Entity (Step 4.1.11) are not defined in the NERC Glossary of Terms or Functional Model.
Response: **NERC and Regional Entity are defined in NERC's corporate documents including, but not limited to, the Certificate of Incorporation and ByLaws.**		
PPL Corporation	Yes	
MRO NERC Standards Review Subcommittee	No	The MRO NSRS questions the change in timing requirements for R3 from 90 days to 30 days. What is the justification for change? Do you have specific examples of problems that resulted from the plan(s) not being updated within 90 days.
Response: **The FERC Order consistently requires a shortening of the update period and recommends 30 days. The SDT agrees with this position. Further, the 30 day period begins upon final implementation of the changes. At that point, much of the due diligence should already be completed related to the actual implementation with final documentation to follow within 30 days.**		
Pepco Holdings, Inc - Affiliates	No	It may not be possible to communicate updates of recovery plans to all personnel responsible for activating or implementing the plan within 30 days (e.g. family leave). Suggest adding exceptions.
Response: **The FERC Order consistently requires a shortening of the update period and communication of the updates to personnel responsible for the activation, and the Order recommends 30 days. The SDT agrees with this position. Further, the 30 day period begins upon final implementation of the changes. At that point, much of the due diligence should already be completed related to the actual implementation with final documentation to follow within 30 days.** **Phase 1 of this project includes necessary modifications to CIP-002-1 through CIP-009-1 to comply with the near term specific directives included in FERC Order 706. The issue identified in your comment is an issue better suited for a later phase of this**		

Organization	Yes or No	Question 8 Comment
project. The SDT suggests that you review the changes proposed in the later phases of the project and resubmit your comments as appropriate if they have not been addressed.		
United Illuminating Company	Yes	
Deloitte& Touche, LLP	Yes	
Exelon	No	Recommendation to increase the timeframe in R3 to require updates to be communicated within 60 days from 30 days. Reason for the recommendation is 30 days is not a sufficient time period to accomplish this level of change management activity.
Response: **The FERC Order consistently requires a shortening of the update period and communication of the updates to personnel responsible for the activation, and the Order recommends 30 days. The SDT agrees with this position. Further, the 30 day period begins upon final implementation of the changes. At that point, much of the due diligence should already be completed related to the actual implementation with final documentation to follow within 30 days.**		
Old Dominion Electric Cooperative	Yes	
City of Tallahassee (TAL)	Yes	
BC Transmission Corporation	Yes	
Applied Control Solutions, LLC	Yes	
US Bureau of Reclamation	Yes	
Orange and Rockland Utilities Inc.	No	1) We recommend changing R3 from "Updates shall becommunicated to personnel responsible for the activation and implementation of the recoveryplan(s) within thirty calendar days of the change being completed." to "Updates shall becommunicated to personnel responsible for the activation and

Organization	Yes or No	Question 8 Comment
		implementation of the recoveryplan(s) within thirty calendar days of completion of the Entity's change process." 2) "Dated" is used only in the Measures (M1, M2, M3, M4, M5). Adding a requirement in the measures is inappropriate
Response: **1) Phase 1 of this project includes necessary modifications to CIP-002-1 through CIP-009-1 to comply with the near term specific directives included in FERC Order 706. The issue identified in your comment is an issue better suited for a later phase of this project. The SDT suggests that you review the changes proposed in the later phases of the project and resubmit your comments as appropriate if they have not been addressed.** **2) The word "dated" will be removed at this time. The measures will be reviewed and considered in an upcoming drafting phase of these standards..**		
CenterPoint Energy	No	Regarding R3, CenterPoint Energy acknowledges that updates to a recovery plan and communication of those updates should be completed in a timely manner; however, CenterPoint Energy believes the SDT went too far in reducing the timeframe for communicating updates from 90 days to 30 days. CenterPoint Energy believes that 30 days is too constraining. Furthermore, in FERC Order 706, paragraph 731, the Commission separated the time allowed for updating recovery plans (30 days) and the time allowed for communicating those updates (90 days), and was willing to consider timeframes other than 30 days. CenterPoint Energy proposes a 60 day window for updating a recovery plan and retaining the 90 day window for communicating the updates to responsible personnel. This would allow adequate time for the appropriate documentation changes to be made and is still timely for communicating to personnel.
Response: **The FERC Order consistently requires a shortening of the update period and communication of the updates to personnel responsible for the activation, and the Order recommends 30 days. The SDT agrees with this position. Further, the 30 day period begins upon final implementation of the changes. At that point, much of the due diligence should already be completed related to the actual implementation with final documentation to follow within 30 days.**		
Manitoba Hydro	Yes	
Alberta Electric System Operator	Yes	
Dynegy	Yes	

Organization	Yes or No	Question 8 Comment
Northern Indiana Public Service Company	No	I do not agree with the reduction from 90 to 30 days. I would propose to provide uniformity and match the modified requirement under CIP-007-2 R9, which requires the modifications to be documented within 30 calendar days after completion versus the CIP-009-2 R3 language which requires the updates to be communicated within 30 calendar days after completion.
Response: **The FERC Order consistently requires a shortening of the update period and communication of the updates to personnel responsible for the activation, and the Order recommends 30 days. The SDT agrees with this position. Further, the 30 day period begins upon final implementation of the changes. At that point, much of the due diligence should already be completed related to the actual implementation with final documentation to follow within 30 days.**		
CoreTrace	Yes	
Oncor Electric Delivery LLC	Yes	
Illinois Municipal Electric Agency		
Ontario Power Generation	No	Reducing the timeframe to communicate updates to CCA recovery plans from within 90 to within 30 calendar days introduces a constraint that may not be achievable in a large organization.
Response: **The FERC Order consistently requires a shortening of the update period and communication of the updates to personnel responsible for the activation, and the Order recommends 30 days. The SDT agrees with this position. Further, the 30 day period begins upon final implementation of the changes. At that point, much of the due diligence should already be completed related to the actual implementation with final documentation to follow within 30 days.**		
American Electric Power	Yes	Refer to comments provided in questions 1 and 13.
Response: **"Responsible Entity" is defined within the Applicability section of each CIP standard.** **The ERO Rules of Procedure include sections on dealing with confidential data associated with the Cyber Security standards, and recognize that there may be some evidence retained by the Responsible Entity. The data retention section of these standards was**		

Organization	Yes or No	Question 8 Comment
written to support this concept. **Phase 1 of this project includes necessary modifications to CIP-002-1 through CIP-009-1 to comply with the near term specific directives included in FERC Order 706. The issue identified in your comment is an issue better suited for a later phase of this project. The SDT suggests that you review the changes proposed in the later phases of the project and resubmit your comments as appropriate if they have not been addressed.**		
Ontario IESO	Yes	
Ameren	Yes	
Consumers Energy Company	Yes	
Xcel Energy	Yes	
ISO New England Inc	No	1 - We recommend changing R3 from "Updates shall becommunicated to personnel responsible for the activation and implementation of the recoveryplan(s) within thirty calendar days of the change being completed." to "Updates shall becommunicated to personnel responsible for the activation and implementation of the recoveryplan(s) within thirty calendar days of completion of the Entity's change process." 2 - "Dated" is used only in the Measures. Adding a requirement in the measures is inappropriate.
Response: **1) The FERC Order consistently requires a shortening of the update period and communication of the updates to personnel responsible for the activation, and the Order recommends 30 days. The SDT agrees with this position. Further, the 30 day period begins upon final implementation of the changes. At that point, much of the due diligence should already be completed related to the actual implementation with final documentation to follow within 30 days.** **Phase 1 of this project includes necessary modifications to CIP-002-1 through CIP-009-1 to comply with the near term specific directives included in FERC Order 706. The issue identified in your comment is an issue better suited for a later phase of this project. The SDT suggests that you review the changes proposed in the later phases of the project and resubmit your comments as appropriate if they have not been addressed.** **2) The word “dated” will be removed at this time. The measures will be reviewed and considered in an upcoming drafting phase of these standards.**		

Organization	Yes or No	Question 8 Comment
American Transmission Company	Yes	
TVA	Yes	
Duke Energy	Yes	
Brazos Electric Power Cooperative, Inc.	No	In R3, replace "being completed" with "being effective".
Response: **Phase 1 of this project includes necessary modifications to CIP-002-1 through CIP-009-1 to comply with the near term specific directives included in FERC Order 706. The issue identified in your comment is an issue better suited for a later phase of this project. The SDT suggests that you review the changes proposed in the later phases of the project and resubmit your comments as appropriate if they have not been addressed.**		
Progress Energy	Yes	CIP009-R3 – The reduction from 90 to 30 days is inadequate considering the coordination and approvals necessary. PE recommends leaving the 90 day time period (same justification as for CIP006-R1.7).
Response: **The FERC Order consistently requires a shortening of the update period and communication of the updates to personnel responsible for the activation, and the Order recommends 30 days. The SDT agrees with this position. Further, the 30 day period begins upon final implementation of the changes. At that point, much of the due diligence should already be completed related to the actual implementation with final documentation to follow within 30 days.**		
Standards Review Committee of ISO/RTO Council	Yes	
KEMA	Yes	In R1, it should be added that the Recovery Plans must be stored on site and a second copy off-site for responders in case the primary site is inaccessible.
Response: **Phase 1 of this project includes necessary modifications to CIP-002-1 through CIP-009-1 to comply with the near term specific**		

Organization	Yes or No	Question 8 Comment
directives included in FERC Order 706. The issue identified in your comment is an issue better suited for a later phase of this project. The SDT suggests that you review the changes proposed in the later phases of the project and resubmit your comments as appropriate if they have not been addressed.		
Austin Energy	Yes	
Kansas City Power & Light	Yes	
San Diego Gas and Electric Co.	Yes	

9. The CSO706 SDT proposes the following for the **Effective Date**:

   The first day of the third calendar quarter after applicable regulatory approvals have been received (or the Reliability Standard otherwise becomes effective the first day of the third calendar quarter after BOT adoption in those jurisdictions where regulatory approval is not required).

   Do you agree with the proposed Effective Date? If not, please explain and provide an alternative to the proposed effective date that would eliminate or minimize your disagreement.

Summary Consideration:

Organization	Yes or No	Question 9 Comment
Detroit Edison Company	No	Does this mean that the current quarter must end, and then you start counting to the first day of the following 3 quarters, or do you include the current quarter in counting? Why not simplify things and use a number of days, such as: "120 calendar days after applicable regulatory approvals have been received . . . . . ."
Response: **The NERC Compliance program has requested the implementation date start on a calendar quarter (January 1, April, 1, July 1, October1). The proposed effective date for the Version 2 standards is the first day of the third calendar quarter (i.e., a minimum of two full calendar quarters, and not more than three calendar quarters). Calendar quarters are January-March, April-June, July-September, and October-December. For example, if regulatory approval is granted in June, the standards would become effective January 1 of the following year. If regulatory approval is granted in July, the standards would become effective April 1 of the following year.**		
PacifiCorp	No	This effective date as written could move the compliance date for our GO functions up 6 months from the previously published compliance schedule found in Table 3. PacifiCorp has been working toward compliance with the standards under the premise that the generation owner has until December 31, 2009, to become compliant with Version 1 standards. For significant changes proposed in Version 2, the generation owner will need time to address and comply.
Response: **The drafting team anticipates that the Phase 1 revisions to the standards will not be approved by the NERC Board of Trustees until the end of May 2009. Accordingly, the earliest possible effective date would be January 1, 2010. Regulatory agency approval processes could push this date out even further for Responsible Entities within those jurisdictions.**		

Organization	Yes or No	Question 9 Comment
FirstEnergy Corp	Yes	
MidAmerican Energy Company	No	Comment: This effective date as written could move the compliance date for our GO functions up 6 months from the previously published compliance schedule. MidAmerican Energy Company has been working toward compliance with the standards under the premise that the generation owner has till December 31, 2009, to become compliant with version 1 standards. For significant changes proposed in version 2, the generation owner will need time to address and comply. For applicable regulatory approvals received between January 1 and March 31, revised standards will be effective the following January 1.MEC proposes the following language: Effective Date: The first day of the calendar quarter after at least nine months following the applicable regulatory approvals have been received, as illustrated in the following table. Applicable regulatory approval received - Effective the following Jan. 1- Mar. 31 Jan. 1Apr. 1- June 30 Apr.1July 1- Sept. 30 July 1Oct. 1- Dec. 31 Oct. 1
Response: **The drafting team anticipates that the Phase I revisions to the standards will not be approved by the NERC Board of Trustees until the end of May 2009. Accordingly, the earliest possible effective date would be January 1, 2010. Regulatory agency approval processes could push this date out even further for Responsible Entities within those jurisdictions. The drafting team believes the six to nine month implementation plan is reasonable.**		
Northeast Power Coordinating Council	No	1) - Existing words are confusing. We recommend changing from "The first day of the third calendar quarter after applicable regulatory approvals have been received (or the Reliability Standard otherwise becomes effective the first day of the third calendar quarter after BOT adoption in those jurisdictions where regulatory approval is not required)" to "The first day after two full consecutive quarters after applicable regulatory approvals have been received (or the Reliability Standard otherwise becomes effective the first day after two full consecutive quarters after NERC Board Of Trustees adoption in those jurisdictions where regulatory approval is not required)". In addition, Canadian members of NPCC have concerns regarding the standards becoming effective at different dates in different jurisdictions. Coordination is required among government authorities to ensure that standards become effective at the same time in all jurisdictions. 2) - Request confirmation that these Effective Dates apply to these updates (Version 2). 3) - We request an addition to the Effective Date clause in CIP-002 - CIP-009 - "Compliance cannot require supporting documentation prior to the Standard's effective date." 4) - We request clarification on Compliance 1.1.1. Wording is confusing. 5) - While Regional Reliability Organization and Compliance Monitor are in the NERC Glossary, the

Organization	Yes or No	Question 9 Comment
		new terms are not (Regional Entity and Compliance Enforcement Authority). 6) - When will we have an opportunity to comment on the Violation Severity Levels (VSLs)? 7) - Clarification required for "the last audit records" and "subsequent audit records" in Data Retention 1.4.2. This comment applies to CIP-002 - CIP-009.

Response:

1) The NERC Compliance program has requested the implementation date start on a calendar quarter (January 1, April, 1, July 1, October1). The proposed effective date for the Version 2 standards is the first day of the third calendar quarter (i.e., a minimum of two full calendar quarters, and not more than three calendar quarters). Calendar quarters are January-March, April-June, July-September, and October-December. For example, if regulatory approval is granted in June, the standards would become effective January 1 of the following year. If regulatory approval is granted in July, the standards would become effective April 1 of the following year.

For some standards, such as standards that require entities in different organizations to work cooperatively with one another using a common set of rules or procedures to support reliability, we agree that there are benefits to having new or revised standards become effective at the same time in all jurisdictions. In situations where there is no coordination between entities in different regions or within an interconnection, then there is no apparent reliability benefit of delaying implementation until all governmental or regulatory authorities have approved the standard. We believe that the CIP standards fall into the second category – they primarily include requirements for entities to take in their own organizations.

2. The proposed effective dates on each standard (CIP-002-2 through CIP-009-2) are for these standards (Version 2) – not for the previous version that was already approved.

3. The requirements in the proposed standards would replace similar requirements in existing standards. If an entity were already expected to be compliant with a requirement in one of the "Version 1" CIP standards, then when the same requirement is replaced with its Version 2 equivalent, the expectation is that the entity has the evidence that was required under the Version 1 standard. Where entities need additional time to become compliant, this is noted in the implementation plan for the Version 2 standards.

4. 1.1.1 - The Regional Entity will serve as the Compliance Enforcement Authority for most entities. In situations where the Regional Entity is responsible for a requirement, the Regional Entity may not assess its own performance as part of an audit as this would serve as a conflict of interest. If the Regional Entity is responsible for a requirement, then the ERO will serve as the Compliance Enforcement Authority in auditing the Regional Entity.

5. The term, "Compliance Enforcement Authority" is used extensively in the ERO Rules of Procedure and replaced the term, "Compliance Monitor." This term has been used in standards under development since November of 2007 to more closely match the language used in the ERO Rules of Procedure – Appendix 4C – Uniform Compliance Monitoring and Enforcement Procedures.

Regional Entity is defined in NERC's corporate documents including, but not limited to, the Certificate of Incorporation and

Organization	Yes or No	Question 9 Comment
ByLaws. **6. The Violation Severity Levels (VSLs) are being developed by another Standards Drafting Team, and their schedule is outside the scope of the cyber security drafting team.** 7. **The "last audit record" would be the records from the last formal audit – if an entity were found noncompliant and there was a mitigation plan with milestones, then the subsequent audit records would include the mitigation plan and associated documentation.**		
WECC Reliability Coordination	Yes	
Southern Company	Yes	
Luminant Power	Yes	
Encari	No	This effective date is still open-ended as the process is not complete. Once additional comment periods have completed and the revisions have been refined we will provide comment as to the acceptability of this timeframe and the continued assurances of the reliability of the Bulk Electric System. We recommend that the standards become agreed upon and complete and then an effective implementation date be identified. This will provide proper assurances from asset owners that they can indeed meet the timeframe identified while continuing to assure the reliability of the BES. We also are confused regarding the term "calendar quarter" versus a concept of "fiscal quarter". Please provide a clarification.
Response: **The drafting team does not anticipate additional comment periods for the Phase 1 revisions to the CIP standards. The NERC Compliance program has requested the implementation date start on a calendar quarter (January 1, April, 1, July 1, October1). The proposed effective date for the Version 2 standards is the first day of the third calendar quarter (i.e., a minimum of two full calendar quarters, and not more than three calendar quarters). Calendar quarters are January-March, April-June, July-September, and October-December. For example, if regulatory approval is granted in June, the standards would become effective January 1 of the following year. If regulatory approval is granted in July, the standards would become effective April 1 of the following year.**		
TransAlta Centralia Generation, LLC	Yes	

Organization	Yes or No	Question 9 Comment
Bonneville Power Administration	Yes	
Consolidated Edison Company of New York, Inc.	No	1. Existing words are confusing. We recommend changing from "The first day of the third calendar quarter after applicable regulatory approvals have been received (or the Reliability Standard otherwise becomes effective the first day of the third calendar quarter after BOT adoption in those jurisdictions where regulatory approval is not required)" to "The first day after two full consecutive quarters after applicable regulatory approvals have been received (or the Reliability Standard otherwise becomes effective the first day after two full consecutive quarters after NERC Board Of Trustees adoption in those jurisdictions where regulatory approval is not required)" 2. Request confirmation that these Effectives Dates apply to these updates (Version 2) 3. We request an addition to the Effective Date clause in CIP-002 - CIP-009 - "Compliance cannot require supporting documentation prior to the Standard's effective date." 4. We request clarification on Compliance 1.1.1. Wording is confusing. 5. While Regional Reliability Organization and Compliance Monitor are in the NERC Glossary. The new terms are not (Regional Entity and Compliance Enforcement Authority). 6. When will we have an opportunity to comment on the Violation Severity Levels (VSLs)? 7. There appear to be two different meanings of "audit records" in Data Retention 1.4.2. We request clarification or less confusing words. This comment applies to CIP-002 - CIP-009

Response:

1. The proposed language does not differ significantly from the original language, so the benefit of the proposed modification is not clear. The suggested language was not adopted. The language in the "proposed effective date" section of the standard is the same language that has been used in proposed standards for the past several months, and most entities have indicated acceptance of this language.

For some standards, such as standards that require entities in different organizations to work cooperatively with one another using a common set of rules or procedures to support reliability, we agree that there are benefits to having new or revised standards become effective at the same time in all jurisdictions. In situations where there is no coordination between entities in different regions or within an interconnection, then there is no apparent reliability benefit of delaying implementation until all governmental or regulatory authorities have approved the standard. We believe that the CIP standards fall into the second category – they primarily include requirements for entities to take in their own organizations.

2. The proposed effective dates on each standard (CIP-002-2 through CIP-009-2) are for these standards (Version 2) – not for the

Organization	Yes or No	Question 9 Comment
previous version that was already approved. **3. The requirements in the proposed standards would replace similar requirements in existing standards. If an entity were already expected to be compliant with a requirement in one of the "Version 1" CIP standards, then when the same requirement is replaced with its Version 2 equivalent, the expectation is that the entity has the evidence that was required under the Version 1 standard. Where entities need additional time to become compliant, this is noted in the implementation plan for the Version 2 standards.** **4. 1.1.1 - The Regional Entity will serve as the Compliance Enforcement Authority for most entities. In situations where the Regional Entity is responsible for a requirement, the Regional Entity may not assess its own performance as part of an audit as this would serve as a conflict of interest. If the Regional Entity is responsible for a requirement, then the ERO will serve as the Compliance Enforcement Authority in auditing the Regional Entity.** **5. The term, "Compliance Enforcement Authority" is used extensively in the ERO Rules of Procedure and replaced the term, "Compliance Monitor." This term has been used in standards under development since November of 2007 to more closely match the language used in the ERO Rules of Procedure – Appendix 4C – Uniform Compliance Monitoring and Enforcement Procedures.** **Regional Entity is defined in NERC's corporate documents including, but not limited to, the Certificate of Incorporation and ByLaws.** **6. The Violation Severity Levels (VSLs) are being developed by another Standards Drafting Team, and their schedule is outside the scope of the cyber security drafting team.** 7. **The "last audit record" would be the records from the last formal audit – if an entity were found noncompliant and there was a mitigation plan with milestones, then the subsequent audit records would include the mitigation plan and associated documentation.**		
Southern California Edison Company	No	Wording is ambiguous. SCE suggests "six (6) months from date of approval."
Response: **The NERC Compliance program has requested the implementation date start on a calendar quarter (January 1, April, 1, July 1, October1). The proposed effective date for the Version 2 standards is the first day of the third calendar quarter (i.e., a minimum of two full calendar quarters, and not more than three calendar quarters). Calendar quarters are January-March, April-June, July-September, and October-December. For example, if regulatory approval is granted in June, the standards would become effective January 1 of the following year. If regulatory approval is granted in July, the standards would become effective April 1 of the following year.**		
Tampa Electric Company	Yes	

Organization	Yes or No	Question 9 Comment
Electric Market Policy	Yes	NERC (Step 4.1.10) and Regional Entity (Step 4.1.11) are not defined in the NERC Glossary of Terms or Functional Model.
Response: **NERC and Regional Entity are defined in NERC's corporate documents including, but not limited to, the Certificate of Incorporation and ByLaws.**		
PPL Corporation	Yes	
MRO NERC Standards Review Subcommittee	Yes	
Pepco Holdings, Inc - Affiliates	Yes	Please consider adding in parenthesis "approximately 270 days" after "the third calendar quarter" for clarification. "The first day of the third calendar quarter (approximately 270 days) after applicable approvals?"
Response: **The NERC Compliance program has requested the implementation date start on a calendar quarter January 1, April, 1, July 1, October1). The proposed effective date for the Version 2 standards is the first day of the third calendar quarter (i.e., a minimum of two full calendar quarters, and not more than three calendar quarters). Calendar quarters are January-March, April-June, July-September, and October-December. For example, if regulatory approval is granted in June, the standards would become effective January 1 of the following year. If regulatory approval is granted in July, the standards would become effective April 1 of the following year.**		
United Illuminating Company	Yes	
Deloitte& Touche, LLP	Yes	
Exelon	Yes	
Old Dominion Electric Cooperative	Yes	

Organization	Yes or No	Question 9 Comment
City of Tallahassee (TAL)	Yes	It is confusing though.
Response: **Thank you for your comment.**		
BC Transmission Corporation	Yes	
Applied Control Solutions, LLC	Yes	
US Bureau of Reclamation	Yes	
Orange and Rockland Utilities Inc.	No	1 - Existing words are confusing. We recommend changing from "The first day of the third calendar quarter after applicable regulatory approvals have been received (or the Reliability Standard otherwise becomes effective the first day of the third calendar quarter after BOT adoption in those jurisdictions where regulatory approval is not required)" to "The first day after two full consecutive quarters after applicable regulatory approvals have been received (or the Reliability Standard otherwise becomes effective the first day after two full consecutive quarters after NERC Board Of Trustees adoption in those jurisdictions where regulatory approval is not required)" 2 - Request confirmation that these Effectives Dates apply to these updates (Version 2) 3 - We request an addition to the Effective Date clause in CIP-002 - CIP-009 - "Compliance cannot require supporting documentation prior to the Standard's effective date." 4 - We request clarification on Compliance 1.1.1. Wording is confusing. 5 - While Regional Reliability Organization and Compliance Monitor are in the NERC Glossary. The new terms are not (Regional Entity and Compliance Enforcement Authority). 6 - When will we have an opportunity to comment on the Violation Severity Levels (VSLs)? 7 - There appear to be two different meanings of "audit records" in Data Retention 1.4.2. We request clarification or less confusing words. This comment applies to CIP-002 - CIP-009

Organization	Yes or No	Question 9 Comment

Response:

1. **The proposed language does not differ significantly from the original language, so the benefit of the proposed modification is not clear. The suggested language was not adopted. The language in the "proposed effective date" section of the standard is the same language that has been used in proposed standards for the past several months, and most entities have indicated acceptance of this language.**

   For some standards, such as standards that require entities in different organizations to work cooperatively with one another using a common set of rules or procedures to support reliability, we agree that there are benefits to having new or revised standards become effective at the same time in all jurisdictions. In situations where there is no coordination between entities in different regions or within an interconnection, then there is no apparent reliability benefit of delaying implementation until all governmental or regulatory authorities have approved the standard. We believe that the CIP standards fall into the second category – they primarily include requirements for entities to take in their own organizations.

2. **The proposed effective dates on each standard (CIP-002-2 through CIP-009-2) are for these standards (Version 2) – not for the previous version that was already approved.**

3. **The requirements in the proposed standards would replace similar requirements in existing standards. If an entity were already expected to be compliant with a requirement in one of the "Version 1" CIP standards, then when the same requirement is replaced with its Version 2 equivalent, the expectation is that the entity has the evidence that was required under the Version 1 standard. Where entities need additional time to become compliant, this is noted in the implementation plan for the Version 2 standards.**

4. **1.1.1 - The Regional Entity will serve as the Compliance Enforcement Authority for most entities. In situations where the Regional Entity is responsible for a requirement, the Regional Entity may not assess its own performance as part of an audit as this would serve as a conflict of interest. If the Regional Entity is responsible for a requirement, then the ERO will serve as the Compliance Enforcement Authority in auditing the Regional Entity.**

5. **The term, "Compliance Enforcement Authority" is used extensively in the ERO Rules of Procedure and replaced the term, "Compliance Monitor." This term has been used in standards under development since November of 2007 to more closely match the language used in the ERO Rules of Procedure – Appendix 4C – Uniform Compliance Monitoring and Enforcement Procedures.**

   Regional Entity is defined in NERC's corporate documents including, but not limited to, the Certificate of Incorporation and ByLaws.

6. **The Violation Severity Levels (VSLs) are being developed by another Standards Drafting Team, and their schedule is outside the scope of the cyber security drafting team.**

7. **The "last audit record" would be the records from the last formal audit – if an entity were found noncompliant and there was a mitigation plan with milestones, then the subsequent audit records would include the mitigation plan and associated**

Organization	Yes or No	Question 9 Comment
documentation.		
CenterPoint Energy		
Manitoba Hydro	Yes	
Alberta Electric System Operator		
Dynegy	Yes	
Northern Indiana Public Service Company	No	I have difficulty responding with acceptance or denial of an implementation schedule when I am not fully aware of what the final draft is going to consist of. Secondly, as this language stands I would like to see a proposed time line based on an example NERC BOT adoption date. I am unclear on weather the Version 2 standards would be implemented in parallel with the existing version 1 implementation schedule, in series, or only begin implementation after FERC approval as this draft is occurring due to FERC directed changes. I am also slightly confused on the audit process and which version of various CIP requirements would be applicable as the responsible entities move into an AC status, while the Version 2 standards could be BOT approved but not FERC approved.
Response: **The drafting team does not anticipate additional comment periods for the Phase 1 revisions to the CIP standards. The NERC Compliance program has requested the implementation date start on a calendar quarter (January 1, April, 1, July 1, October1). The proposed effective date for the version 2 standards is the first day of the third calendar quarter (i.e., a minimum of two full calendar quarters, and not more than three calendar quarters). Calendar quarters are January-March, April-June, July-September, and October-December. For example, if regulatory approval is granted in June, the standards would become effective January 1 of the following year. If regulatory approval is granted in July, the standards would become effective April 1 of the following year.** **The drafting team anticipates that the Phase 1 revisions to the standards will not be approved by the NERC Board of Trustees until the end of May 2009. Accordingly, the earliest possible effective date would be January 1, 2010. Regulatory agency approval processes could push this date out even further for Responsible Entities within those jurisdictions.** **The New Critical Cyber Asset Implementation Plan incorporates Table 4 of the Version 1 Implementation Plan and supersedes the**		

Organization	Yes or No	Question 9 Comment
Version 1 Implementation Plan. The New Critical Cyber Asset Implementation Plan states that "the Responsible Entity is expected to have all audit records required to demonstrate compliance (i.e., to be 'Auditably Compliant') one year following the [compliant] milestone listed in this Implementation Plan."		
CoreTrace	Yes	
Oncor Electric Delivery LLC	Yes	
Illinois Municipal Electric Agency		
Ontario Power Generation		
American Electric Power	Yes	To add further clarity, AEP suggests that the following text be added to the effective date statement above." . . . after applicable FERC approvals have been received and such approval is posted in the public registry (or the . . . "
Response: **The SDT does not feel that a change to the standard language is necessary. The US Federal Rulemaking Process requires that the effective date of the approval rule is contained in the text of the Final Rule that is published in the Federal Register.**		
Ontario IESO	Yes	
Ameren	Yes	
Consumers Energy Company	Yes	
Xcel Energy	Yes	
ISO New England Inc	No	1 - Existing words are confusing. We recommend changing from "The first day of the third calendar quarter after applicable regulatory approvals have been received (or the Reliability Standard otherwise becomes effective the first day of the third calendar quarter after BOT adoption in those jurisdictions

Organization	Yes or No	Question 9 Comment
		where regulatory approval is not required)" to "The first day after two full consecutive quarters after applicable regulatory approvals have been received (or the Reliability Standard otherwise becomes effective the first day after two full consecutive quarters after NERC Board Of Trustees adoption in those jurisdictions where regulatory approval is not required)" 2 - Request confirmation that these Effectives Dates apply to these updates (Version 2) 3 - We request an addition to the Effective Date clause in CIP-002 - CIP-009 - "Compliance cannot require supporting documentation prior to the Standard's effective date." 4 - We request clarification on Compliance 1.1.1. Wording is confusing. 5 - While Regional Reliability Organization and Compliance Monitor are in the NERC Glossary. The new terms are not (Regional Entity and Compliance Enforcement Authority). 6 - When will we have an opportunity to comment on the Violation Severity Levels (VSLs)? 7 - There appear to be two different meanings of "audit records" in Data Retention 1.4.2. We request clarification or less confusing words. This comment applies to CIP-002 - CIP-009.

Response:

1. **The proposed language does not differ significantly from the original language, so the benefit of the proposed modification is not clear. The suggested language was not adopted. The language in the "proposed effective date" section of the standard is the same language that has been used in proposed standards for the past several months, and most entities have indicated acceptance of this language.**

   For some standards, such as standards that require entities in different organizations to work cooperatively with one another using a common set of rules or procedures to support reliability, we agree that there are benefits to having new or revised standards become effective at the same time in all jurisdictions. In situations where there is no coordination between entities in different regions or within an interconnection, then there is no apparent reliability benefit of delaying implementation until all governmental or regulatory authorities have approved the standard. We believe that the CIP standards fall into the second category – they primarily include requirements for entities to take in their own organizations.

2. **The proposed effective dates on each standard (CIP-002-2 through CIP-009-2) are for these standards (Version 2) – not for the previous version that was already approved.**

3. **The requirements in the proposed standards would replace similar requirements in existing standards. If an entity were already expected to be compliant with a requirement in one of the "Version 1" CIP standards, then when the same requirement is replaced with its Version 2 equivalent, the expectation is that the entity has the evidence that was required under the Version 1 standard. Where entities need additional time to become compliant, this is noted in the implementation plan for the Version 2**

Organization	Yes or No	Question 9 Comment
		standards. **4. 1.1.1 - The Regional Entity will serve as the Compliance Enforcement Authority for most entities. In situations where the Regional Entity is responsible for a requirement, the Regional Entity may not assess its own performance as part of an audit as this would serve as a conflict of interest. If the Regional Entity is responsible for a requirement, then the ERO will serve as the Compliance Enforcement Authority in auditing the Regional Entity.** **5. The term, "Compliance Enforcement Authority" is used extensively in the ERO Rules of Procedure and replaced the term, "Compliance Monitor." This term has been used in standards under development since November of 2007 to more closely match the language used in the ERO Rules of Procedure – Appendix 4C – Uniform Compliance Monitoring and Enforcement Procedures.** **Regional Entity is defined in NERC's corporate documents including, but not limited to, the Certificate of Incorporation and ByLaws.** **6. The Violation Severity Levels (VSLs) are being developed by another Standards Drafting Team, and their schedule is outside the scope of the cyber security drafting team.** 7. **The "last audit record" would be the records from the last formal audit – if an entity were found noncompliant and there was a mitigation plan with milestones, then the subsequent audit records would include the mitigation plan and associated documentation.**
American Transmission Company	Yes	
TVA	Yes	
Duke Energy	Yes	
Brazos Electric Power Cooperative, Inc.	Yes	
Progress Energy	No	PE would like clarification on the effective date Section A.5. of each standard. Given the nature of some of the requirements to possibly include significant capital investment, we want to ensure there is adequate time given for budget cycle and outage planning. Also, the guidance for identification of CAs is still incomplete which could impact implementation timeframes. PE recommends allowing 12 months after the BOT approval for the effective date.

Organization	Yes or No	Question 9 Comment
Response: **The NERC Compliance program has requested the implementation date start on a calendar quarter (January, April, July, October). The proposed effective date for the Version 2 standards is the first day of the third calendar quarter (i.e., a minimum of two full calendar quarters, and not more than three calendar quarters). Calendar quarters are January-March, April-June, July-September, and October-December. For example, if regulatory approval is granted in June, the standards would become effective January 1 of the following year. If regulatory approval is granted in July, the standards would become effective April 1 of the following year. The drafting team believes the six to nine month implementation plan is reasonable. The New Critical Cyber Asset Implementation Plan is applicable to newly identified CAs and supersedes the Version 2 implementation schedule.**		
Standards Review Committee of ISO/RTO Council	Yes	
KEMA	Yes	
Austin Energy	Yes	
Kansas City Power & Light	Yes	
San Diego Gas and Electric Co.	Yes	

10. The CSO706 SDT is proposing a separate **CIP implementation plan** to address newly identified Critical Cyber Assets. In this plan, three specific classes of categories for newly identified Critical Cyber Assets are described. The plan provides an implementation schedule with "Compliant" milestones for each requirement in each category. All timelines are specified as an offset from the date when the Critical Cyber Asset has been newly identified.

    Do you agree with the approach proposed by the SDT for handling newly identified Critical Cyber Assets? If not, please explain and provide an alternative to the proposed milestones that would eliminate or minimize your disagreement.

Summary Consideration:

Organization	Yes or No	Question 10 Comment
Detroit Edison Company	Yes	
PacifiCorp	Yes	
FirstEnergy Corp	No	While we do agree with the overall objective the team is trying to achieve, we do not agree as presently written and offer the following comments: a) The description of Category 1 seems to imply that a Responsible Entity who has a CIP CA and CCA methodology, but did not identify any CCA assets may be given additional time to comply with the CIP standards when they have identified any CCAs on subsequent annual reviews. However, what is not clear is what triggered the new CCA being identified? The Category 1 description should be clear that it does not apply simply based on "error and ommission" if the Responsible Entity's methodologies for CA and CCA identification have not changed and the Responsible Entity simply overlooked an asset that should have been previously identified and protected. If these newly identified assets were in service during their initial CIP asset determination, then the entity was not compliant with their initial asset identification and it should be expected that the entity would file a Self Report and Mitigation Plan to obtain compliance. b) FE believes our above comment on Category 1 also applies to the Category 2 description as it indicates in the second paragraph that it refers to newly identified CCA assets but they are not associated with an addition or modification through construction, upgrade or replacement. Again, if the methodologies have not changed, if there was no merger or acquisition, then what triggered the newly identified existing asset? It should be clear that "error and ommission" do not apply. c) We agree with the provisions described for newly acquired assets through mergers and acquisitions when companies may have had differing methodologies.

Organization	Yes or No	Question 10 Comment
		d) We agree with item 3 regarding "Compliant upon Commissioning" for newly planned upgrades that result in new CA and CCA items. e) In general we found the information to be overly wordy and confusing to understand. We suggest the team attempt to greatly consolidate the information. f) Tables 2 should be adjusted such that it can be read and viewed stand alone to the extent possible from the remaining supporting text. For example, Table 2 has no indication that the numbers refer to "months".
Response: **a) The Implementation Plan does not evaluate why an asset becomes a newly identified Critical Asset. Changes in system conditions could result in the identification of an existing asset as a Critical Asset without modification to the Risk Assessment Methodology. An entity that misapplies its Risk Assessment Methodology could be in potential violation.** **b) The Implementation Plan does not evaluate why an asset becomes a newly identified Critical Asset. Changes in system conditions could result in the identification of an existing asset as a Critical Asset without modification to the Risk Assessment Methodology. An entity that misapplies its Risk Assessment Methodology could be in potential violation.** **c) Thank you for your comment.** **d) Thank you for your comment.** **e) The posted version is simplified from early drafts and must address the complexity of the problem.** **f) The tables will be updated to reflect the time period as being in months.**		
MidAmerican Energy Company	Yes	
Northeast Power Coordinating Council	No	1 - On the single page Implementation Plan, CIP-003 R2 is mandatory for all Entities. We suggested in answers to #1 and #2 that this Requirement move to CIP-002, which is already mandatory for these Entities. We agree that the CIP-003 R2 Requirement (wherever it is) should be 12 months. 2 - We request a clearer message that this new Implementation Plan applies to Version 1 and beyond Standards. It is too easy to believe this Plan applies to Version 2 because some refer to Version 2 (Table 2), and the Requirements do not match CIP-006-2. 3 - We recommend that the Implementation Plan consistently use Category 3 instead of interchanging with "Compliant upon commissioning." 4 - We request clarification on historical records for Category 3 (Compliant upon Commissioning) Critical

Organization	Yes or No	Question 10 Comment
		Cyber Assets. 5 - Second sentence of Category 2 (on page 3) is "The existing Critical Cyber Assets may remain in service while the relevant requirements of the CIP Standards are implemented." By their nature, CCAs must remain in service or have a detrimental effect on the grid. We recommend removal of this sentence. 6 - Category 2's second paragraph states "This category applies only when additional in-service Critical Cyber Assets or applicable other Cyber Assets are identified, not when they are added or modified through construction, upgrade or replacement." We recommend that emergency replacements be Category 2. This paragraph is different than the preceding flow chart. 7 - We recommend an additional scenario where a failed Cyber Asset in an emergency must be replaced with a Critical Cyber Asset, for example the original Asset used serial communications and the new Asset uses IP communications. We suggest this is Category 2. 8 - We recommend changing Category 3 (page 4) from "c) Addition of: "to "c) Planned addition of:" 9 - There is a discrepancy between the document's title and preamble (referring to CIP-003 and CIP-009) while Table 3 includes CIP-002. Please update or clarify.

Response:

1) All Entities must comply with all standards, and Entities that have no identified Critical Cyber Assets comply by invoking the exemption found in A.4.2.3 in each standard. Table 2 (Category 1) of the New Critical Cyber Asset Implementation Plan was in error and should have been N/A. Table 3 of the New Critical Cyber Asset Implementation Plan is invoked for a new Registered Entity, giving that Entity 12 months to comply.

2) The title of the document commonly referred to as the New Critical Cyber Asset Implementation Plan will be corrected to read "Implementation Plan for Cyber Security Standards CIP-002-2 through CIP-009-2 or Their Successor Standards." All references to Version 1 of the standards within the document will be similarly modified.

3) "Category 3" does not appear in the New Critical Cyber Asset Implementation Plan or the Version 2 Implementation Plan.

4) The New Critical Cyber Asset Implementation Plan describes only the Compliance Date, and no audit records are required for the Compliance Date.

5) The SDT agrees that the CCAs should remain in service to avoid a "detrimental effect on the grid." The inclusion of this sentence reinforces that belief. The SDT is concerned that if the sentence is removed, entities may remove the assets from service in order to not be found in non-compliance of the standard, resulting in a "detrimental effect on the grid." Similarly, changing the sentence to require that the assets must remain in service would not allow a brief maintenance outage to allow entities to implement changes associated with bringing the assets into compliance.

Organization	Yes or No	Question 10 Comment
6) Emergency provisions are described in Table 1 "Example Scenarios". The Figure 1 flowchart is a high-level process flow and does not contain the same level of detail. A special case of restoration as part of a disaster recovery situation (such as storm restoration) follows the emergency provisions of the Responsible Entity's policy required by CIP-003 R1.1. The SDT will modify the implementation plan to make it clear that the emergency provision is applicable to Category 2 as well as Compliant upon Commissioning. **7) The SDT will modify the implementation plan to make it clear that the emergency provision is applicable to Category 2 as well as Compliant upon Commissioning.** **8) The SDT agrees with the recommendation.** **9) The SDT agrees with the comment and will change the title of the document accordingly.**		
WECC Reliability Coordination	Yes	
Southern Company	Yes	
Luminant Power	Yes	
Encari	No	Due to the massiveness of the CCA process, we recommend that this approach needs to be partitioned in to its own comment period.
Response: **The drafting team does not anticipate additional comment periods for the Phase I revisions to the CIP standards.**		
TransAlta Centralia Generation, LLC	Yes	
Bonneville Power Administration	Yes	
Consolidated Edison Company of New York, Inc.	No	1 - On the single page Implementation Plan, CIP-003 R2 is mandatory for all Entities. We suggested in answers to #1 and #2 that this Requirement move to CIP-002, which is already mandatory for these Entities. We agree that theCIP-003 R2 Requirement (wherever it is) should be 12 months. 2 - We request a clearer message that this new Implementation Plan applies to Version 1 and beyond Standards. It is too easy to believe this Plan applies to Version 2 because some reference Version 2

Organization	Yes or No	Question 10 Comment
		(Table 2) and the Requirements do not match the CIP-006-2. 3 - We recommend that the Implementation Plan consistently use Category 3 instead of interchanging with "Compliant upon commissioning." 4 - We request clarification on historical records for Category 3 (Compliant upon commissioning) Critical Cyber Assets 5 - Second sentence of Category 2 (on page 3) is "The existing Critical Cyber Assets may remain in service while the relevant requirements of the CIP Standards are implemented." By their nature, CCAs must remain in service or have a detrimental effect on the grid. We recommend removal of this sentence 6 - Category 2's second paragraph states "This category applies only when additional in-service Critical Cyber Assets or applicable other Cyber Assets are identified, not when they are added or modified through construction, upgrade or replacement." We recommend that emergency replacements be Category 2. This paragraph is different than the preceding flow chart. 7 - We recommend an additional scenario where a failed Cyber Assets in an emergency must be replaced with a Critical Cyber Asset, for example the original Asset used serial and the new Asset uses IP. We suggest this is Category 2. 8 - We recommend changing Category 3 (page 4) from "c) Addition of: "to "c) Planned addition of:" 9 - There is a discrepancy between the document's title and preamble (referring to CIP-003 and CIP-009) while Table 3 includes CIP-002. Please update or clarify.

Response:

1) All Entities must comply with all standards, and Entities that have no identified Critical Cyber Assets comply by invoking the exemption found in A.4.2.3 in each standard. Table 2 (Category 1) of the New Critical Cyber Asset Implementation Plan was in error and should have been N/A. Table 3 of the New Critical Cyber Asset Implementation Plan is invoked for a new Registered Entity, giving that Entity 12 months to comply.

2) The title of the document commonly referred to as the New Critical Cyber Asset Implementation Plan will be corrected to read "Implementation Plan for Cyber Security Standards CIP-002-2 through CIP-009-2 or Their Successor Standards." All references to Version 1 of the standards within the document will be similarly modified.

3) "Category 3" does not appear in the New Critical Cyber Asset Implementation Plan or the Version 2 Implementation Plan.

4) The New Critical Cyber Asset Implementation Plan describes only the Compliance Date, and no audit records are required for the Compliance Date.

5) The SDT agrees that the CCAs must remain in service to avoid a "detrimental effect on the grid." The inclusion of this

Organization	Yes or No	Question 10 Comment
sentence reinforces that belief. **6) Emergency provisions are described in Table 1 "Example Scenarios". The Figure 1 flowchart is a high-level process flow and does not contain the same level of detail. A special case of restoration as part of a disaster recovery situation (such as storm restoration) follows the emergency provisions of the Responsible Entity's policy required by CIP-003 R1.1. The SDT will modify the implementation plan to make it clear that the emergency provision is applicable to Category 2 as well as Compliant upon Commissioning.** **7) The SDT will modify the implementation plan to make it clear that the emergency provision is applicable to Category 2 as well as Compliant upon Commissioning.** **8) The SDT agrees with the recommendation.** **9) The SDT agrees with the comment and will change the title of the document accordingly.**		
Southern California Edison Company	Yes	
Tampa Electric Company	Yes	
Electric Market Policy	Yes	1) "Responsible Entity" is not defined in the implementation plan. 2) On page 1 under Implementation Schedule, Item #3 should read: "A new or existing "Cyber" Asset becomes?" 3) On page 2, the first sentence should reference "other" Cyber Assets rather than "non-critical" Cyber Assets to be consistent with the red-line change to CIP-007-2 Purpose. 4) On page 4, bullet "b" perimeter needs to be capitalized.
Response: **1) Responsible Entity is defined in the language of each standard.** **2) The SDT agrees with the recommendation.** **3) The SDT agrees with the recommendation.** **4) The SDT agrees with the recommendation.**		
PPL Corporation	Yes	PPL agrees with different categories of newly identified Critical Cyber Assets and the different

Organization	Yes or No	Question 10 Comment
		implementation schedule for these classes of categories.
Response: **Thank you for your comment.**		
MRO NERC Standards Review Subcommittee	Yes	
Pepco Holdings, Inc - Affiliates	Yes	We specifically appreciate and support the CSO706 SDT efforts in closing the current gap in the CIP standards for compliance of newly identified Critical Cyber Assets by creating three categories with a related implementation schedule.
Response: **Thank you for your comment.**		
United Illuminating Company	Yes	
Deloitte& Touche, LLP	Yes	Will the drafting team include situations that occur through merger and acquisition(M&A)?
Response: **Merger and Acquisition is addressed in the New Cyber Asset Implementation Plan.**		
Exelon	Yes	The 6 month implementation milestones listed for CIP-004-2 Category 2 should instead reflect 6 months from when the new security boundaries and systems get implemented instead of 6 months from the identification of the newly identified Critical Cyber Asset. Entities will not be able to know all the affected personnel until the new physical and electronic security perimeters are defined and implemented.
Response: **The SDT agrees with the comment and will modify the timeframe to 18 months after the new CCA is identified for Category 2 for CIP-004 Requirements R2, R3 and R4.**		
Old Dominion Electric Cooperative	Yes	

Organization	Yes or No	Question 10 Comment
City of Tallahassee (TAL)	Yes	Although it can be confusing also.
Response: **The posted version is simplified from early drafts and must address the complexity of the problem.**		
BC Transmission Corporation	Yes	
Applied Control Solutions, LLC	Yes	
US Bureau of Reclamation	Yes	
Orange and Rockland Utilities Inc.	No	1 - On the single page Implementation Plan, CIP-003 R2 is mandatory for all Entities. We suggested in answers to #1 and #2 that this Requirement move to CIP-002, which is already mandatory for these Entities. We agree that theCIP-003 R2 Requirement (wherever it is) should be 12 months. 2 - We request a clearer message that this new Implementation Plan applies to Version 1 and beyond Standards. It is too easy to believe this Plan is applies to Version 2 because some references Version 2 (Table 2) and the Requirements do not match the CIP-006-2. 3 - We recommend that the Implementation Plan consistently use Category 3 instead of interchanging with "Compliant upon commissioning." 4 - We request clarification on historical records for Category 3 (Compliant upon commissioning) Critical Cyber Assets 5 - Second sentence of Category 2 (on page 3) is "The existing Critical Cyber Assets may remain in service while the relevant requirements of the CIP Standards are implemented." By their nature, CCAs must remain in service or have a detrimental effect on the grid. We recommend removal of this sentence 6 - Category 2's second paragraph states "This category applies only when additional in-service Critical Cyber Assets or applicable other Cyber Assets are identified, not when they are added or modified through construction, upgrade or replacement." We recommend that emergency replacements be Category 2. This paragraph is different than the preceding flow chart. 7 - We recommend an additional scenario where a failed Cyber Assets in an emergency must be

Organization	Yes or No	Question 10 Comment
		replaced with a Critical Cyber Asset, for example the original Asset used serial and the new Asset uses IP. We suggest this is Category 2. 8 - We recommend changing Category 3 (page 4) from "c) Addition of: "to "c) Planned addition of:" 9 - There is a discrepancy between the document's title and preamble (referring to CIP-003 and CIP-009) while Table 3 includes CIP-002. Please update or clarify.
Response: **1) All Entities must comply with all standards, and Entities that have no identified Critical Cyber Assets comply by invoking the exemption found in A.4.2.3 in each standard. Table 2 (Category 1) of the New Critical Cyber Asset Implementation Plan was in error and should have been N/A. Table 3 of the New Critical Cyber Asset Implementation Plan is invoked for a new Registered Entity, giving that Entity 12 months to comply.** **2) The title of the document commonly referred to as the New Critical Cyber Asset Implementation Plan will be corrected to read "Implementation Plan for Cyber Security Standards CIP-002-2 through CIP-009-2 or Their Successor Standards." All references to Version 1 of the standards within the document will be similarly modified.** **3) "Category 3" does not appear in the New Critical Cyber Asset Implementation Plan or the Version 2 Implementation Plan.** **4) The New Critical Cyber Asset Implementation Plan describes only the Compliance Date, and no audit records are required for the Compliance Date.** **5) The SDT agrees that the CCAs must remain in service to avoid a "detrimental effect on the grid." The inclusion of this sentence reinforces that belief.** **6) Emergency provisions are described in Table 1 "Example Scenarios". The Figure 1 flowchart is a high-level process flow and does not contain the same level of detail. A special case of restoration as part of a disaster recovery situation (such as storm restoration) follows the emergency provisions of the Responsible Entity's policy required by CIP-003 R1.1. The SDT will modify the implementation plan to make it clear that the emergency provision is applicable to Category 2 as well as Compliant upon Commissioning.** **7) The SDT will modify the implementation plan to make it clear that the emergency provision is applicable to Category 2 as well as Compliant upon Commissioning.** **8) The SDT agrees with the recommendation.** **9) The SDT agrees with the comment and will change the title of the document accordingly.**		
CenterPoint Energy		
Manitoba Hydro	No	The new implementation plan needs to clearly state that the categorization is only applied to newly

Organization	Yes or No	Question 10 Comment
		identified Critical Cyber Assets, and not to all Critical Cyber Assets. The new implementation plan should also state that the categorization of a Critical Cyber Asset expires and is no longer required when that Critical Cyber Asset becomes compliant. Table 2 needs to indicate that the milestones listed are in months. The title for Table 3 needs to be revised to indicate that the table is to be used for Registered Entities which have identified their first Critical Cyber Asset (Category 1), and for newly Registered Entities.
Response: **The New Critical Cyber Asset Implementation Plan repeatedly refers to "newly identified" Critical Cyber Assets. "Compliant Upon Commissioning" also includes Cyber Assets replacing existing Critical Cyber Assets. The categorization is only used to determine the applicable compliance schedule and has no meaning once the Critical Cyber Asset is compliant. The tables will be updated to reflect the time period as being in months.** **Table 2 is applicable to all Registered Entities that have now identified their first Critical Cyber Asset (Category 1) after registration.** **Table 3 is only applicable to newly Registered Entities whether or not they have identified a Critical Asset.**		
Alberta Electric System Operator		
Dynegy	No	Under the Category 2 heading, the proposed method for handling the case of a business merger or acquisition when any of the Responsible Entities involved had previously identified Critical Cyber Assets is inequitable and inconsistent with the proposed handling of the case when all Registered Entities have identified Critical Cyber Assets. Under the Category 2 heading, in the case of a business merger or acquisition when any of the Responsible Entities involved had previously identified Critical Cyber Assets, it really only matters if the acquiring or controlling Responsible Entity had previously identified Critical Cyber Assets. If the acquiring or controlling entity had not previously identified any Critical Cyber Assets it will have no CIP Compliance Program and it should be required to meet the same Category 1 (instead of Category 2) milestones established for the case where neither Registered Entity involved in merger had previously identified any critical Cyber Assets. In addition, in the case when all Registered Entities involved in a merger have identified Critical Cyber Assets the merged Responsible Entity is required to meet Category 2 milestones after one calendar year from the merger date. This provision in effect grants the Merged Responsibility Entity in this case the approximate equivalent of having to meet Category 1 milestones. This approach further justifies the revised approach suggested above for the former case.

Organization	Yes or No	Question 10 Comment
Response: **In the event of a merger or acquisition of a company resulting in a single registered entity, when both entities have existing programs, the Implementation Plan allows one year for the programs to be harmonized. When only one of the entities has an existing program, that program is expected to continue after the merger. In the case of acquisitions of assets resulting in a change in registered entity, if the acquiring company has a program and the acquired asset is already identified as critical, there is one year to harmonize the programs. If the acquiring company does not have a program and the acquired asset is already identified as critical, continuation of the program at the acquired asset is expected to be provided for in the acquisition process, assuming the asset continues to be critical.**		
Northern Indiana Public Service Company	No	Moving through the existing phases, I do not believe the steps provide for a situation in which a utility wishes to improve or strengthen the risk-based methodology. If a utility has an existing CCA and strengthens the methodology process which in turn produces a new CA and in turn new CCA's, the utility would find itself in immediate non-compliance. Based on this situation and using the flow chart contained within the proposed implementation schedule document, the responsible entity would already have an existing CCA, the Cyber assets of the new resulting CA would already be in service, and it would be a planned change as the utility chose to strengthen the existing methodology. The flow chart result would be compliant upon commissioning, and the cyber asset is already in service, therefore the real world result is immediate non-compliance. I believe this is counter productive as NERC and FERC would encourage an entity to strengthen the risk-based methodology. The current proposed implementation schedule would encourage a utility to not strengthen the risk-based methodology over time in order to remain in compliance. I believe additional provisions need to be made.
Response: **The described scenario is defined in Table 1 "Example Scenarios". The Figure 1 flowchart is a high-level process flow and does not contain the same level of detail.**		
CoreTrace		
Oncor Electric Delivery LLC	No	The timeframes in Table 2 are reasonable. However, CIP-002-1 currently specifies that an asset is not designated as a Critical Asset until the annual application of the Risk-Based Methodology. A cyber asset is not a Critical Cyber Asset unless it is essential to the operation of the Critical Asset. Category 3 "Compliant upon Commissioning" is not a current requirement of CIP-002-1 and represents a significant change to the current standard. This seems to imply that the Risk-Based Methodology must be applied continuously, not just annually. "Compliant upon Commissioning" should only apply to replacing existing Critical Cyber Assets. New Critical Cyber Assets identified by CIP-002-1 Requirement R3 should utilize the timeframes in Category 2

Organization	Yes or No	Question 10 Comment
Response: **CIP-002-2, Requirements R2 (Critical Asset identification) and R3 (Critical Cyber Asset identification) state "the Responsible Entity shall review this list at least annually, and update it as necessary." These requirements expect the entity to assess the new asset or Cyber Asset as part of the planning process.**		
Illinois Municipal Electric Agency		
Ontario Power Generation	No	We note that the implementation plan for newly identified Critical Cyber Assets specifies that it applies to "CIP-002-1 through CIP-009-1 and their successor standards". We further notice that in Milestone Category 2 an number of requirements have a six (6) month timeframe specified for compliance. In effect, the identification of a new CCA at an Entity today would be required to be fully compliant with respect to that new newly identified CCA before December 31, 2009 - the Compliant deadline for all other CCAs.
Response: **The drafting team anticipates that the Phase I revisions to the standards will not be approved by the NERC Board of Trustees until the end of May 2009. Accordingly, the earliest possible effective date would be January 1, 2010. Regulatory agency approval processes could push this date out even further for Responsible Entities within those jurisdictions.**		
American Electric Power	Yes	
Ontario IESO	Yes	We believe the proposed implementation plan is reasonable and appropriate.
Response: **Thank you for your comment.**		
Ameren	Yes	Would like to see a clarification on what is intended by phrase "planned change".
Response: **A "planned change" is any anticipated and planned for change to an asset or Cyber Asset.**		
Consumers Energy	Yes	

Organization	Yes or No	Question 10 Comment
Company		
Xcel Energy	Yes	
ISO New England Inc	No	1 - On the single page Implementation Plan, CIP-003 R2 is mandatory for all Entities. We suggested in answers to #1 and #2 that this Requirement move to CIP-002, which is already mandatory for these Entities. We agree that theCIP-003 R2 Requirement (wherever it is) should be 12 months. 2 - We request a clearer message that this new Implementation Plan applies to Version 1 and beyond Standards. It is too easy to believe this Plan applies to Version 2 because some references Version 2 (Table 2) and the Requirements do not match the CIP-006-2. 3 - We recommend that the Implementation Plan consistently use Category 3 instead of interchanging with "Compliant upon commissioning." 4 - We request clarification on historical records for Category 3 (Compliant upon commissioning) Critical Cyber Assets 5 - Second sentence of Category 2 (on page 3) is "The existing Critical Cyber Assets may remain in service while the relevant requirements of the CIP Standards are implemented." By their nature, CCAs must remain in service or have a detrimental effect on the grid. We recommend removal of this sentence 6 - Category 2's second paragraph states "This category applies only when additional in-service Critical Cyber Assets or applicable other Cyber Assets are identified, not when they are added or modified through construction, upgrade or replacement." We recommend that emergency replacements be Category 2. This paragraph is different than the preceding flow chart. 7 - We recommend an additional scenario where a failed Cyber Assets in an emergency must be replaced with a Critical Cyber Asset, for example the original Asset used serial and the new Asset uses IP. We suggest this is Category 2. 8 - We recommend changing Category 3 (page 4) from "c) Addition of: "to "c) Planned addition of:" 9 - There is a discrepancy between the document's title and preamble (referring to CIP-003 and CIP-009) while Table 3 includes CIP-002. Please update or clarify.

Response:

1) All Entities must comply with all standards, and Entities that have no identified Critical Cyber Assets comply by invoking the exemption found in A.4.2.3 in each standard. Table 2 (Category 1) of the New Critical Cyber Asset Implementation Plan was in error and should have been N/A. Table 3 of the New Critical Cyber Asset Implementation Plan is invoked for a new Registered Entity, giving that Entity 12 months to comply.

Organization	Yes or No	Question 10 Comment
2) The title of the document commonly referred to as the New Critical Cyber Asset Implementation Plan will be corrected to read "Implementation Plan for Cyber Security Standards CIP-002-2 through CIP-009-2 or Their Successor Standards." All references to Version 1 of the standards within the document will be similarly modified. **3) "Category 3" does not appear in the New Critical Cyber Asset Implementation Plan or the Version 2 Implementation Plan.** **4) The New Critical Cyber Asset Implementation Plan describes only the Compliance Date, and no audit records are required for the Compliance Date.** **5) The SDT agrees that the CCAs must remain in service to avoid a "detrimental effect on the grid." The inclusion of this sentence reinforces that belief.** **6) Emergency provisions are described in Table 1 "Example Scenarios". The Figure 1 flowchart is a high-level process flow and does not contain the same level of detail. A special case of restoration as part of a disaster recovery situation (such as storm restoration) follows the emergency provisions of the Responsible Entity's policy required by CIP-003 R1.1. The SDT will modify the implementation plan to make it clear that the emergency provision is applicable to Category 2 as well as Compliant upon Commissioning.** **7) The SDT will modify the implementation plan to make it clear that the emergency provision is applicable to Category 2 as well as Compliant upon Commissioning.** **8) The SDT agrees with the recommendation.** **9) The SDT agrees with the comment and will change the title of the document accordingly.**		
American Transmission Company	Yes	
TVA	Yes	
Duke Energy	Yes	
Brazos Electric Power Cooperative, Inc.		
Progress Energy	Yes	
Standards Review Committee of ISO/RTO Council	Yes	We believe the proposed implementation plan is reasonable and appropriate.

Organization	Yes or No	Question 10 Comment
Response: **Thank you for your comment.**		
KEMA	Yes	
Austin Energy	Yes	
Kansas City Power & Light	Yes	
San Diego Gas and Electric Co.	Yes	

11. Do you agree with the **compliance milestones** included in the proposed implementation plan for handling newly identified Critical Cyber Assets? If not, please explain and provide an alternative to the proposed milestones that would eliminate or minimize your disagreement..

Summary Consideration:

Organization	Yes or No	Question 11 Comment
Detroit Edison Company	No	Table 2 does not address CIP-006-2 R7 and R8. They should both be 24 for category 1 and 12 for category 2. Table 2 CIP-008-2 R2 category 2 should be changed from 0 to 6 which matches the timetable associated with R1. The 0 implies that a Responsible Entity needs to retain documents relating to requirement, R1.1, which that entity is not yet required to be compliant. Table 2 CIP-009-2 R2 and R3 category 2 should be changed from 0 to 12. Similarly to the comment around CIP-008-2 R2, a Responsible Entity cannot be compliant with exercising a plan that is not required to exist. Changing the timetable to 12 ensures the recovery plan is initially executed in the annual time frame required by R2.
Response: **Table 2 does not reflect the addition of two new requirements in CIP-006-2. The SDT will update the tables appropriately.** **The formal title and references to the CIP standards will be modified to refer to the Version 2 standards and their successors.** **The SDT will update Table 2 CIP-008-2 R2 category 2 to 6 months as recommended.** **The SDT will update Table 2 CIP-009-2 R2 and R3 category 2 to 12 months as recommended.**		
PacifiCorp	Yes	
FirstEnergy Corp	Yes	We agree with the Implementation Plan times described for Category 1 and Category 2, however, we believe clarification is need as to when these provisions apply. See our comments in Question 10.

Organization	Yes or No	Question 11 Comment
Response: **The Implementation Plan does not evaluate why an asset becomes a newly identified Critical Asset. Changes in system conditions could result in the identification of an existing asset as a Critical Asset without modification to the Risk Assessment Methodology. An entity that misapplies its Risk Assessment Methodology could be in potential violation.**		
MidAmerican Energy Company	Yes	
Northeast Power Coordinating Council	No	1 - We recommend that Table 2 clarify the units as months, per page 1. 2 - Table 2 CIP-008 R2 Category 2's value is 0. Since R2 depends on R1 which is 6 months, this appears to need work. We recommend R2 change to 6. 3 – Table 2 CIP-009 R2 and R3 Category 2's value is 0. Since R2 and R3 depend on R1 which is 6 months, this appears to need work. We recommend R2 and R3 change to 6.
Response: **1) The tables will be updated to reflect the time period as being in months.** **2) The SDT will update Table 2 CIP-008-2 R2 Category 2 to 6 months as recommended.** **3) The SDT will update Table 2 CIP-009-2 R2 and R3 Category 2 to 12 months.**		
WECC Reliability Coordination	Yes	
Southern Company	Yes	
Luminant Power	Yes	
Encari	No	Due to the massiveness of the CCA process, we recommend that this approach needs to be partitioned in to its own comment period. For instance, the current document details "existing" within CIP-003-2; however - newly identified CCAs may not immediately be able to compliant at zero day with CIP-003-2 requirements. For example R4 requires the information associated with the CCA to be protected. This information may still reside in a non-protected format prior to becoming a CCA - however the

Organization	Yes or No	Question 11 Comment
		implementation timeframe is "existing".
Response: **The drafting team does not anticipate additional comment periods for the Phase I revisions to the CIP standards.** **The SDT agrees with the example cited and will modify the Category 2 compliance time frame for CIP-003-2 Requirements R4, R5, and R6 to be 6 months.**		
TransAlta Centralia Generation, LLC	Yes	
Bonneville Power Administration	Yes	
Consolidated Edison Company of New York, Inc.	No	1 - We recommend that Table 2 clarifies the units as months, per page 12 - Table 2 CIP-008 R2 Category 2's value is 0. Since R2 depends on R1 which is 6 months, this appears to need work. We recommend R2 change to 6.3 - Table 2 CIP-009 R2 and R3 Category 2's value is 0. Since R2 and R3 depend on R1 which is 6 months, this appears to need work. We recommend R2 and R3 change to 6.
Response: **1) The tables will be updated to reflect the time period as being in months.** **2) The SDT will update Table 2 CIP-008-2 R2 Category 2 to 6 months as recommended.** **3) The SDT will update Table 2 CIP-009-2 R2 and R3 Category 2 to 12 months.**		
Southern California Edison Company	Yes	
Tampa Electric Company	Yes	
Electric Market Policy	Yes	On page 6, Table 2 Milestone Categories should indicate "months."

Organization	Yes or No	Question 11 Comment
Response: **The tables will be updated to reflect the time period as being in months.**		
PPL Corporation	No	PPL has concerns with the existing implementation schedule. Table 2 identifies some standard requirements as existing for Category 2 milestones. Having an Information Protection program does not mean that all information associated with a newly identified Critical Cyber Asset is immediately protected. For example, if an RE identifies an asset as critical with critical cyber assets, not all drawings and documentation will exist immediately marked as such. Even existing programs need to be applied to newly identified assets requiring an implementation schedule. The second concern is dependent on the outcome of the FERC Order for Clarification of CIP standards applicability to nuclear generating facilities. If the FERC Order results in nuclear facilities being included in the CIP applicability, this implementation plan should be noted to not include nuclear facilities affected by the pending FERC Order. The FERC Clarification Order needs to address the schedule for including nuclear facilities in the CIP applicability.
Response: **The SDT agrees with the example cited and will modify the Category 2 compliance time frame for CIP-003-2 Requirements R4, R5, and R6 to be 6 months.** **The issue of nuclear facilities is out of scope for this drafting team.**		
MRO NERC Standards Review Subcommittee	Yes	
Pepco Holdings, Inc - Affiliates		
United Illuminating Company	Yes	
Deloitte& Touche, LLP	Yes	
Exelon	No	The 6 month implementation milestones listed for CIP-004-2 Category 2 should instead reflect 6 months from when the new security boundaries and systems get implemented instead of 6 months from the

Organization	Yes or No	Question 11 Comment
		identification of the newly identified Critical Cyber Asset. Entities will not be able to know all the affected personnel until the new physical and electronic security perimeters are defined and implemented.
Response: **The SDT agrees with the comment and will modify the timeframe to 18 months after the new CCA is identified for Category 2 for CIP-004 Requirements R2, R3 and R4.**		
Old Dominion Electric Cooperative	Yes	
City of Tallahassee (TAL)	Yes	
BC Transmission Corporation	Yes	
Applied Control Solutions, LLC	Yes	
US Bureau of Reclamation	No	The agreement would be based on the response to the CIP-004 background check requirement timeframe. The milestones would require adjustment for more exhaustive background checks.
Response: **Personnel can be granted unescorted access as long as a personnel risk assessment has been conducted according to the requirements in CIP-004 R3.** **A more exhaustive background check is not required; therefore an adjustment to the implementation plan is not necessary..**		
Orange and Rockland Utilities Inc.	No	1 - We recommend that Table 2 clarifies the units as months, per page 1 2 - Table 2 CIP-008 R2 Category 2's value is 0. Since R2 depends on R1 which is 6 months, this appears to need work. We recommend R2 change to 6. 3 - Table 2 CIP-009 R2 and R3 Category 2's value is 0. Since R2 and R3 depend on R1 which is 6 months, this appears to need work. We recommend R2 and R3 change to 6.

Organization	Yes or No	Question 11 Comment
Response: **1) The tables will be updated to reflect the time period as being in months.** **2) The SDT will update Table 2 CIP-008-2 R2 Category 2 to 6 months as recommended.** **3) The SDT will update Table 2 CIP-009-2 R2 and R3 Category 2 to 12 months.**		
CenterPoint Energy		
Manitoba Hydro	No	CIP-003-2 R3, R4, and R5: The milestones should be changed to 6 months. Although the information protection, access control and change control and configuration management programs exist, the requirements also include implementation, which will require some time to meet compliance. CIP-008-2 R2: The milestone should be changed to 6 months, the same as R1. The documentation required in R2 is dependent upon the elements in the Cyber Security Incident Response Plan developed in R1. CIP-009-2 R2 and R3: The milestones should be changed to 6 months, the same as R1. The exercises and change control in R2 and R3 are dependent upon the elements in the Recovery Plan developed in R1.
Response: **The SDT interprets the comments to refer to Milestone Category 2.** **CIP-003, Requirement R3 has no implementation requirements, and thus the current timeframe is reasonable.** **The SDT will modify the Category 2 compliance timeframe for CIP-003-2 Requirements R4, R5, and R6 to be 6 months.** **The SDT will update Table 2 CIP-008-2 R2 Category 2 to 6 months as recommended.** **The SDT will update Table 2 CIP-009-2 R2 and R3 Category 2 to 12 months.**		
Alberta Electric System Operator		
Dynegy	Yes	

Organization	Yes or No	Question 11 Comment
Northern Indiana Public Service Company	No	I do not believe CIP-003-2 R3-R6 should be assumed to exist under Category 2 assets. An entity may need to identify exceptions, information, provide access control to that information and implement change control procedures on the newly identified asset. I also do not believe that it should be assumed that an entity can obtain the necessary financial capital to implement systems for compliance in any immediate fashion.
Response: **The SDT will modify the Category 2 compliance timeframe for CIP-003-2 Requirements R4, R5, and R6 to be 6 months.** **An entity that cannot comply within the implementation plan will be expected to submit a self-report of non-compliance with a mitigation plan that provides sufficient time to obtain funding.**		
CoreTrace		
Oncor Electric Delivery LLC	Yes	
Illinois Municipal Electric Agency		
Ontario Power Generation	No	We interpret that the plan seems to collapse together the Compliant and Auditably Compliant milestones. We note that it is not possible to identify a new CCA, bring it into a state or Compliant (as defined in the currently applicable standard) and have one year of data and records as required to be Auditably Compliant. We believe clarification is required in this area.
Response: **The New Critical Cyber Asset Implementation Plan states that "the Responsible Entity is expected to have all audit records required to demonstrate compliance (i.e., to be 'Auditably Compliant') one year following the [compliant] milestone listed in this Implementation Plan."**		
American Electric Power	Yes	
Ontario IESO	Yes	We believe the proposed implementation plan is reasonable and appropriate.

Organization	Yes or No	Question 11 Comment
Response: **Thank you for your comment.**		
Ameren	Yes	
Consumers Energy Company	Yes	
Xcel Energy	Yes	
ISO New England Inc	No	1 - We recommend that Table 2 clarifies the units as months, per page 2 - Table 2 CIP-008 R2 Category 2's value is 0. Since R2 depends on R1 which is 6 months, this appears to need work. We recommend R2 change to 6. 3 - Table 2 CIP-009 R2 and R3 Category 2's value is 0. Since R2 and R3 depend on R1 which is 6 months, this appears to need work. We recommend R2 and R3 change to 6.
Response: **1) The tables will be updated to reflect the time period as being in months.** **2) The SDT will update Table 2 CIP-008-2 R2 Category 2 to 6 months as recommended.** **3) The SDT will update Table 2 CIP-009-2 R2 and R3 Category 2 to 12 months.**		
American Transmission Company	Yes	
TVA	Yes	
Duke Energy	Yes	
Brazos Electric Power Cooperative, Inc.		

Organization	Yes or No	Question 11 Comment
Progress Energy	No	The implementation plan for new CAs and CCAs allows 6-12-24 months for compliance, as noted by standard for Category 1-2 programs. For Category 2 programs (CIP program in place), for those requirements needing capitol funding anything less than 18 months would be difficult due to funding requests/process for capital. PE recommends those requirements potentially requiring significant capitol investment allowing a minimum of 18 months for compliance.
Response: **An entity that cannot comply within the implementation plan will be expected to submit a self-report of non-compliance with a mitigation plan that provides sufficient time to obtain funding.**		
Standards Review Committee of ISO/RTO Council	Yes	We believe the proposed implementation plan is reasonable and appropriate.
Response: **Thank you for your comment.**		
KEMA	Yes	
Austin Energy	Yes	
Kansas City Power & Light	Yes	
San Diego Gas and Electric Co.	Yes	

12. The CSO706 SDT seeks input on whether to include the information contained in this **stand-alone implementation plan within the body of each standard.** This would likely entail a new requirement in CIP-002 to classify newly identified Critical Cyber Assets, and changes to the remaining standards to insert the milestone timeframes.

    Do you agree with including the information about newly identified Critical Cyber Assets and newly registered entity information within the body of the standards which would eliminate the stand-alone documents? If not, please explain.

Summary Consideration:

Organization	Yes or No	Question 12 Comment
Detroit Edison Company	Yes	
PacifiCorp	Yes	
FirstEnergy Corp	No	The stand alone document is sufficient and could be easily added as a reference document to each standard.
Response: **Thank you for your comment. The SDT will maintain the New Critical Cyber Asset Implementation Plan as a separate document for Phase I of the revisions and will consider incorporating the implementation plan into the standards in a subsequent revision.**		
MidAmerican Energy Company	Yes	
Northeast Power Coordinating Council	Yes	
WECC Reliability Coordination	Yes	
Southern Company	Yes	
Luminant Power	Yes	

Organization	Yes or No	Question 12 Comment
Encari	No	We agree that the requirement to identify new CCA should be included; however, we believe that a continued need to guide Responsible Entities in the selection of CAs and CCAs is still necessary as separate documents.
Response: **The SDT will maintain the New Critical Cyber Asset Implementation Plan as a separate document for Phase 1 of the revisions and will consider incorporating the implementation plan into the standards in a subsequent revision. Guidelines for the identification of Critical Assets and Critical Cyber Assets are currently being developed.**		
TransAlta Centralia Generation, LLC	Yes	
Bonneville Power Administration	No	Including the implementation plan information in the individual CIP standards would greatly increase the size and complexity of each standard. All NERC Reliability Standards, including CIP, must be interpreted using various stand-alone documents (e.g., NERC Glossary of Terms Used in the Reliability Standards, NERC Reliability Functional Model, Compliance Monitoring and Enforcement Program, etc.). It's not a problem having the Implementation Plan available as a separate link or as a companion document to the CIP Reliability Standards.
Response: **The SDT will maintain the New Critical Cyber Asset Implementation Plan as a separate document for Phase I of the revisions and will consider incorporating the implementation plan into the standards in a subsequent revision.**		
Consolidated Edison Company of New York, Inc.	Yes	
Southern California Edison Company	Yes	
Tampa Electric Company	Yes	
Electric Market Policy	Yes	

Organization	Yes or No	Question 12 Comment
PPL Corporation	Yes	
MRO NERC Standards Review Subcommittee	Yes	
Pepco Holdings, Inc - Affiliates	Yes	In response to the CSO706 SDT question, we agree that the implementation plan for newly identified Critical Cyber Assets should be incorporated into the cyber security standard and believe that it should be included as part of CIP-002-1.
Response: **The SDT will maintain the New Critical Cyber Asset Implementation Plan as a separate document for Phase I of the revisions and will consider incorporating the implementation plan into the standards in a subsequent revision.**		
United Illuminating Company	Yes	
Deloitte& Touche, LLP	Yes	
Exelon	Yes	
Old Dominion Electric Cooperative	Yes	I agree with including this information in the standards so everyone, user and Region, understands what is required. Leaving it in a stand alone document might allow for FERC to unilaterally change the implementation timeframe without stakeholder input. I hate to have to revise the CIP standards again, but this is important.
Response: **The SDT will maintain the New Critical Cyber Asset Implementation Plan as a separate document for Phase I of the revisions and will consider incorporating the implementation plan into the standards in a subsequent revision.**		
City of Tallahassee (TAL)	Yes	I am for eliminating stand alone documents, although this incorporation can be made in Version 3, since you have stated one will be done for the more contentious issues.
Response: **The SDT will maintain the New Critical Cyber Asset Implementation Plan as a separate document for Phase I of the revisions and will**		

Organization	Yes or No	Question 12 Comment
consider incorporating the implementation plan into the standards in a subsequent revision.		
BC Transmission Corporation	Yes	
Applied Control Solutions, LLC	Yes	
US Bureau of Reclamation	No	Inserting the information and time lines for newly identified Critical Cyber Assets and newly registered entity information into the body of the standards will cause unnecessary confusion regarding the implementation of the standards. By retaining the current stand-alone implementation plan it provides a ready reference and single point of information for all new Critical Cyber Assets and newly registered entities.
Response: **The SDT will maintain the New Critical Cyber Asset Implementation Plan as a separate document for Phase I of the revisions and will consider incorporating the implementation plan into the standards in a subsequent revision.**		
Orange and Rockland Utilities Inc.	Yes	
CenterPoint Energy		
Manitoba Hydro	Yes	Implementation plans which expire should be stand-alone documents from the standards. On-going implementation plans should be incorporated into the standards to create self-contained standards.
Response: **The SDT will maintain the New Critical Cyber Asset Implementation Plan as a separate document for Phase I of the revisions and will consider incorporating the implementation plan into the standards in a subsequent revision.**		
Alberta Electric System Operator		
Dynegy	Yes	

Organization	Yes or No	Question 12 Comment
Northern Indiana Public Service Company	Yes	
CoreTrace	No	To include the distinct procedures for newly identified Critical Cyber Assets would introduce a level of complexity and confusion into the current standard. As they stand today the CIP requirements are easy to understand and useful. A reference to the standalone implementation plan in the CIP body would be useful and sufficient and ensure that the information in the implementation plan was not overlooked.
Response: **The SDT will maintain the New Critical Cyber Asset Implementation Plan as a separate document for Phase I of the revisions and will consider incorporating the implementation plan into the standards in a subsequent revision.**		
Oncor Electric Delivery LLC	Yes	
Illinois Municipal Electric Agency		
Ontario Power Generation		
American Electric Power	Yes	AEP believes that there should be a statement in the standard providing a reference to the implementation plan and that the implementation plan be included in an appendix of the standard.
Response: **The SDT will maintain the New Critical Cyber Asset Implementation Plan as a separate document for Phase I of the revisions and will consider incorporating the implementation plan into the standards in a subsequent revision.**		
Ontario IESO	No	We believe that an implementation plan managed as a separate document is a more logical choice. Information is less likely to be repetitive and other standards can reference it as necessary. However, where an issue pertains to a single standard, it would be appropriate to include the pertinent implementation information within that standard.

Organization	Yes or No	Question 12 Comment
Response: **The SDT will maintain the New Critical Cyber Asset Implementation Plan as a separate document for Phase I of the revisions and will consider incorporating the implementation plan into the standards in a subsequent revision.**		
Ameren	Yes	
Consumers Energy Company	Yes	
Xcel Energy	Yes	
ISO New England Inc	Yes	
American Transmission Company	Yes	
TVA	Yes	
Duke Energy	Yes	
Brazos Electric Power Cooperative, Inc.		
Progress Energy	No	PE recommends referring to the implementation plan but not including it in the standard.
Response: **The SDT will maintain the New Critical Cyber Asset Implementation Plan as a separate document for Phase I of the revisions and will consider incorporating the implementation plan into the standards in a subsequent revision.**		
Standards Review Committee of ISO/RTO Council	No	We believe an implementation plan managed as a separate document is a more logical choice. Information is less likely to be repetitive and other standards can reference it as necessary. However, where an issue pertains to a single standard, it would be appropriate to include the pertinent implementation information within that standard.

Organization	Yes or No	Question 12 Comment
Response: **The SDT will maintain the New Critical Cyber Asset Implementation Plan as a separate document for Phase I of the revisions and will consider incorporating the implementation plan into the standards in a subsequent revision.**		
KEMA	No	Any change to the Standards is a long a laborious effort, so a change in implementation plan will have to go through the process. A separate document with the plan facilitites changes to the plan and not the Standard.
Response: **The SDT will maintain the New Critical Cyber Asset Implementation Plan as a separate document for Phase 1 of the revisions and will consider incorporating the implementation plan into the standards in a subsequent revision.**		
Austin Energy	No	I have a question as to why any newly installed asset would be anything but critical. Certainly existing assets can degrade to a point where they no longer fulfill a critical role, but why would a new asset be installed if there was not a need?
Response: **There may be multiple reasons for building a Bulk Electric System (BES) asset, including reliability or economic. Other reasons might include transmission to connect a new merchant generator (which may have economic benefit to the GO, but not necessarily the TO), or BES assets supporting increased retail or wholesale load. Alternatively, a parallel implementation to "modernize" a non-critical asset would still be non-critical. It is left up to the Responsible Entity to determine if the newly built asset is a Critical Asset based on its impact to the reliability of the BES. Similarly, a Cyber Asset might be installed within an Electronic Security Perimeter that is not determined to be a Critical Cyber Asset.**		
Kansas City Power & Light	Yes	This seems like the most logical place to put those requirements. Otherwise we'll end up with Standards that have to be cross-referenced against multiple sets of documents.
Response: **The SDT will maintain the New Critical Cyber Asset Implementation Plan as a separate document for Phase I of the revisions and will consider incorporating the implementation plan into the standards in a subsequent revision.**		
San Diego Gas and Electric Co.	No	For clarity, SDG&E prefers the stand-alone Implementation Plan documents as presented rather than integrating the information for newly identified CCAs and newly registered entities into the existing CIP standards. This will help eliminate confusion and keep the existing Standard requirements and new

Organization	Yes or No	Question 12 Comment
		CCAs/Registered Entity information separate.

Response:

The SDT will maintain the New Critical Cyber Asset Implementation Plan as a separate document for Phase I of the revisions and will consider incorporating the implementation plan into the standards in a subsequent revision.

13. Do you agree that the Phase I improvements addresses the **time-sensitive FERC Order directives**? If not, please explain.

Summary Consideration:

Organization	Yes or No	Question 13 Comment
Detroit Edison Company	Yes	
PacifiCorp	No	The new effective date goes above the requirements listed in Order 706 and adds undue burden on the industry that will create the need for multiple technical exceptions and mitigation plans.
Response: **The requirements in the proposed standards would replace similar requirements in existing standards. If an entity were already expected to be compliant with a requirement in one of the "Version 1" CIP standards, then when the same requirement is replaced with its Version 2 equivalent, the expectation is that the entity has the evidence that was required under the Version 1 standard. Where entities need additional time to become compliant, this is noted in the implementation plan for the Version 2 standards.** **The Standards Drafting Team believes that the six to nine month implementation plan is reasonable.**		
FirstEnergy Corp	Yes	For the most part we agree with the improvements except for our previous comments in questions 3, 10 and 11.Also, we offer the following additional suggested improvements:CIP-002-2 R3 - The phrase "automatic generation control" should be capitalized since it is a NERC defined term.CIP-003 M1 - The SDT should consider removing the second sentence "Additionally, the Responsible Entity shall demonstrate that the cyber security policy is available as specified in Requirement R1.2" since the language in the first sentence already covers the necessary measure.CIP-005 R2.4 - The word "strong" should be removed since it is not clearly defined and measurable.CIP-007 - R2,R3,R5 - The word "establish" should be removed consistant with the other CIP standards. All that should be required is to "implement and document".- R5.1.2 - Replace "establish" with "have".- R7 - Replace "establish" with "document.CIP-009 - The first sentence in "Sec. B Requirements" which states "The Responsible Entity shall comply with the following requirements of Standard CIP-009-2:" is not necessary and should be removed consistant with the other CIP revisions. FAQ Document - Is the SDT considering changes to the FAQ document to align with these proposed changed to the standards? Or is the FAQ document not a "living" document and was only to be used for the version 1 standards development? Regarding measures in CIP-002 through CIP-009, the drafting team should consider revising the measures to

Organization	Yes or No	Question 13 Comment
		include some guidance on the types of evidence or documentation that a responsible entity should and/or could have to demonstrate compliance. Throughout the standards the phrases "at least" and "at a minimum" are used and we fee that they are unnecessary. It is already understood that the standard requirements are the minimum expectations. Throughout the standards we suggest the SDT add the VRFs for each main requirement. Lastly, it would be appreciated if the SDT would use underlining in addition to the blue colored text to reflect inserted text for readability of black-n-white printed/copied material.
Response: **These types of issues will be addressed in Phase 2 of the CIP Standards; please use the Phase 2 comment period if you feel that your concerns have not been addressed.**		
MidAmerican Energy Company	No	The new effective date goes above the requirements listed in Order 706 and adds undue burden on the industry that will create the need for multiple technical exceptions and mitigation plans.
Response: **The requirements in the proposed standards would replace similar requirements in existing standards. If an entity were already expected to be compliant with a requirement in one of the "Version 1" CIP standards, then when the same requirement is replaced with its Version 2 equivalent, the expectation is that the entity has the evidence that was required under the Version 1 standard. Where entities need additional time to become compliant, this is noted in the implementation plan for the Version 2 standards.** **The Standards Drafting Team believes that the six to nine month implementation plan is reasonable.**		
Northeast Power Coordinating Council	Yes	We agree with the removal of "reasonable business judgment" and "acceptance of risk".
Response: **Thank you for your comment.**		
WECC Reliability Coordination	Yes	
Southern Company	Yes	

Organization	Yes or No	Question 13 Comment
Luminant Power	No	Luminant thanks the Standards Drafting Team for their work addressing improvements to the NERC CIP Standards CIP-002 through CIP-009. As indicated by our "yes" responses to the comment form, in general Luminant agrees with the drafting team regarding the phased approach, implementation plan and the changes to address the time-sensitive issues from the FERC Order. However, on each standard the drafting team changed the language under the Data Retention sections 1.4.1 and 1.4.2. Luminant agrees with the intent of the changes but does not believe the language provides sufficient clarity. Luminant respectfully submits the following suggested language for the aforementioned data retention sections on each standard. 1.4.1 The Responsible Entity shall keep documentation required by Standard CIP-002-2 for the current calendar year and the previous full calendar year unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation. The Responsible Entity shall keep documentation required by the Compliance Enforcement Authority for an investigation for one year after Compliance Enforcement Authority notice to the Responsible Entity that the investigation is completed.1.4.2 The Compliance Enforcement Authority and the Responsible Entity shall each retain all requested and submitted audit records from the most recent audit.
Response: **The language of 1.4.2 indicates that the Compliance Enforcement Authority "in conjunction with" the Registered Entity will retain all the audit records from the previous audit and all audit records submitted since the previous audit, until completion of the next audit. This supports the audit intervals for all entities and supports the need to retain the confidentiality of some data. The audit data retention period is determined by the audit period for each Registered Entity.**		
Encari	No	FERC provided directives on nearly all of the current requirements and guidance to include further requirements. The identification of what to modify in a time-sensitive manner was not open for public comment. We recognize the need to act swiftly to protect the assets; however, assurances also need to be made to protect system reliability. As an example, we feel that further clarifications around how to select critical assets and critical cyber assets would have provided a greater impact on the process and recommend that a public comment period be opened for the current draft guidelines. Therefore we recommend providing public comment periods to help the selection process of which FERC directives to introduce in the next phase of changes.
Response: **The Standards Drafting Team agrees that there are a variety of pressing needs such that a proritization process would be helpful. Once the time sensitive issues have been identified, the next step includes a discussion about the phased implementation approach**		

Organization	Yes or No	Question 13 Comment
to all of the FERC recommendations, while also considering industry needs.		
TransAlta Centralia Generation, LLC	Yes	
Bonneville Power Administration	Yes	
Consolidated Edison Company of New York, Inc.	Yes	We agree that Phase I addresses the time-sensitive FERC Order directives to remove "reasonable business judgment" and "acceptance of risk".
Response: **Thank you for your comment.**		
Southern California Edison Company	Yes	SCE hereby submits these additional general comments and questions (not related to or in response to Question 13): 1. What is the approval process for Violation Severity Levels? Will they be part of the standards? Will they be circulated for comment as part of the approval process? 2. In the Data Retention section of each Standard, a retention period is not specified for audit records. What is the retention period?
Response: **1) The Violation Severity Levels (VSLs) for Version 1 of the CIP Standards (CIP-002-1 through CIP-009-1) are being developed by another Standards Drafting Team, and their schedule is outside the scope of the cyber security drafting team. The VSLs for Version 2 of the CIP Standards (CIP-002-2 through CIP-009-2) associated with the changes being proposed by the Standards Drafting Team for this project are currently being coordinated with the other Standards Drafting Team and will be posted for Industry Comment. The schedule for doing so is currently unknown.** **2) The data retention periods for the standard requirements are specified in the standards. The language of 1.4.2 indicates that the Compliance Enforcement Authority "in conjuncgtion with" the Registered Entity will retain all the audit records from the previous audit and all audit records submitted since the previous audit, until completion of the next audit. This supports the audit intervals for all entities. The audit data retention period is determined by the audit period for each Registered Entity.**		

Organization	Yes or No	Question 13 Comment
Tampa Electric Company	Yes	
Electric Market Policy	Yes	
PPL Corporation	Yes	
MRO NERC Standards Review Subcommittee	No	The new effective date goes above the requirements listed in Order 706 and adds undue burden on the industry that will create the need for multiple technical exceptions and mitigation plans.
Response: **The requirements in the proposed standards would replace similar requirements in existing standards. If an entity were already expected to be compliant with a requirement in one of the "Version 1" CIP standards, then when the same requirement is replaced with its Version 2 equivalent, the expectation is that the entity has the evidence that was required under the Version 1 standard. Where entities need additional time to become compliant, this is noted in the implementation plan for the Version 2 standards.** **The Standards Drafting Team believes that the six to nine month implementation plan is reasonable.**		
Pepco Holdings, Inc - Affiliates	No	1. We understand that the SDT is proposing that Technical Feasibility Exceptions (TFE) Process (i.e. exception approval process) be modeled after the existing Self-Report and Mitigation Plan processes in the Compliance Monitoring and Enforcement Program (CMEP) which would require TFE review by the Regional Entity and NERC to assess the impact to the BES and then approve or not approve the exception. We also understand that as part of the NERC TFE approval process a mitigation plan would need to be submitted to the Regional Entity/NERC and completed for compliance. We understand that the Standards Drafting Team (SDT) is proposing that the TFE process be done through the NERC Rules of Procedure update process rather than through the standards process. Is it the intent of the SDT is to keep the TFE process outside of the compliance process (i.e., TFE requirement as part of the NERC Rules of Procedures)? 2. The existing Self-Report and Mitigation Plan process is for self-reporting and remedying a potential non-compliance. Is the intent of modeling the existing Self-Report and Mitigation Plan for the TFE process because the SDT considers Technical Feasibility Exceptions as non-compliance to the CIP standards? It was our understanding that TFEs are not a compliance issue. The existing FAQs state: Technical feasibility refers only to engineering possibility and is expected to be a "can/cannot" determination in every circumstance. It is also intended to be determined in light of the equipment and

Organization	Yes or No	Question 13 Comment
		facilities already owned by the Responsible Entity. The Responsible Entity is not required to replace any equipment in order to achieve compliance with the Cyber Security Standards. http://www.nerc.com/docs/standards/sar/Revised_CIP-002-009_FAQs_06Mar06.pdf 3. We believe that the TFE process needs to be included in the standards as well (e.g. CIP-003-2 R3). If the TFE is not coupled to the Standards (e.g. requirement to submit to RE and NERC for approval) we have concerns that there may be unintended gaps or conflicts. **(i)** For example what happens if a Registered Entity in following CIP-003-2 R3 (Exceptions) has a technical exception approved by the Sr. Manager but by a de-coupled TFE process NERC does not approve the exception? The Registered Entity is in compliance with the Standard but not with the TFE approval process. Would failure of a TFE procedure be considered non-compliance and therefore subject to fines? **(ii)** Another example of a potential gap or conflict is there could be conflicting effective dates of the standards and the TFE process (i.e. the requirement to submit to NERC for approval) if these are not linked together. **(iii)** Timing of the approvals by NERC could also create a gap or conflict. **(iv)** We encourage the SDT drafting team to consider including the requirement of RE/NERC review in the standards. The detailed process and procedures could be separate. **(v)** Finally we believe that the SDT needs to identify how the RE and/or NERC will perform the assessment of a TFE request on the impact to the BES (e.g. engineering judgement, load flow studies, stability studies,...) and identify the parameters that would be considered an approved exception versus an unapproved exception. 4. We understand and agree that NERC has the right to review TFE information and evidence of compliance but providing this information/data offsite may be considered a violation to the CIP requirement(s) and at the very least is a potential risk because if this information is compromised could show vulnerabilities to Critical Cyber Assets at a given Registered Entity. The confidentiality and security of the data/information needs to be considered. Potential options could include: • NERC could review information over a secure communication channel without NERC keeping the sensitive information

Organization	Yes or No	Question 13 Comment
Response: **1. The removal of "reasonable business judgment" was done in accordance with FERC Order 706. The revisions made to the standards in Phase 1 are intended to be responsive to specific FERC directives relevant to the onset of compliance audits in July 2009. The expansion of the Technical Feasibility Exception Process should address the concerns regarding the removal of reasonable business judgment and acceptance of risk.** **2. Situations where the standards requirements cannot be met will be handled through the Technical Feasibility Exception process under the NERC Rules of Procedure. The technical feasibility exception process will address the requirements for documenting, approving, and remediating the exception. Any sanction decisions will arise from the TFE process. It is not appropriate to assert that "duly authorized exceptions will not result in non-compliance" within Section D-1.5 of the standard.** **3. Phase 1 of this project includes necessary modifications to CIP-002-1 through CIP-009-1 to comply with the near term specific directives included in FERC Order 706. The issue identified in your comment is an issue better suited for a later phase of this project. The SDT suggests that you review the changes proposed in the later phases of the project and resubmit your comments as appropriate if they have not been addressed.** **4. Phase 1 of this project includes necessary modifications to CIP-002-1 through CIP-009-1 to comply with the near term specific directives included in FERC Order 706. The issue identified in your comment is an issue better suited for a later phase of this project. The SDT suggests that you review the changes proposed in the later phases of the project and resubmit your comments as appropriate if they have not been addressed.**		
United Illuminating Company	Yes	
Deloitte& Touche, LLP	Yes	
Exelon	Yes	
Old Dominion Electric Cooperative	Yes	
City of Tallahassee (TAL)	Yes	I may not agree with all changes but they do address the FERC Order directives, even though by making these directives, they violate the ANSI approved process that they have stated NERC is required to follow.

Organization	Yes or No	Question 13 Comment
Response: **Comments regarding the ANSI process are outside the scope of the SDT to address.**		
BC Transmission Corporation	Yes	
Applied Control Solutions, LLC	No	NIST Framework needs to be addressed NOW!
Response: **The Standards Drafting Team will consider the NIST risk management framework in future revisions of the standards.**		
US Bureau of Reclamation	No	The revisions are moving these standards away from "Critical Infrastructure Protection" towards "Cyber Infrastructure Protection." We believe this move strays from the original intent of Critical Infrastructure Protection as defined by the initial requirements. By focusing solely on the Cyber aspect, many important aspects of critical infrastructure protection will be lost. We reject any efforts to modify CIP from Critical Infrastructure Protection to Cyber Infrastructure Protection.
Response: **The Standard Drafting Team is focused on the cyber security aspects of critical infrastructure protection, a priority reflected in the SDT 706 SAR and driven by national security concerns about the adequacy of the industry's cyber security efforts as stated by Congressional Committees, FERC, and the new Obama Administration.** **Nonetheless, the SDT agrees that there is a critical need to address non-cyber critical infrastructure issues. If the commenter believes such an effort is warranted, we would recommend the submission of a SAR to specify the applicable issues.**		
Orange and Rockland Utilities Inc.	Yes	
CenterPoint Energy	No	See responses above to Q5, Q7, and Q8. In addition, the SDT changed the data retention wording in CIP-002 through CIP-009 such that "the Compliance Enforcement Authority in conjunction with the Registered Entity shall keep the last audit records and all requested and submitted subsequent audit records." CenterPoint Energy believes the retention time should be more defined and proposes adding

Organization	Yes or No	Question 13 Comment
		"until the next scheduled audit" to make it clear that data retention is on a rolling basis.
Response: **The data retention periods for the standard requirements are specified in the standards. The language of 1.4.2 indicates that the Compliance Enforcement Authority in conjunction with the Registered Entity will retain all the audit records from the previous audit and all audit records submitted since the previous audit, until completion of the next audit. This supports the audit intervals for all entities. The audit data retention period is determined by the audit period for each Registered Entity.**		
Manitoba Hydro	Yes	
Alberta Electric System Operator		
Dynegy	Yes	
Northern Indiana Public Service Company	Yes	Not sure if the question pertains to the CIP draft modifications or the proposed implementation schedule.
Response: **The Question pertains to both items.**		
CoreTrace		
Oncor Electric Delivery LLC	Yes	
Illinois Municipal Electric Agency		
Ontario Power Generation		
American Electric	Yes	As described above and following, AEP believes that there are a number of concepts that need to be

Organization	Yes or No	Question 13 Comment
Power		discussed and clarified in the standards. 1) AEP requests clarication be added about changes to Data Retention item 1.4.2. NERC reference materials suggest that the Compliance Enforcement Authority is solely responsible for keeping the last audit records. AEP does not believe that expanding the role of the Registered Entity, beyond that in any other standard, to include keeping audit documents is necessary or appropriate. However, there may be circumstances where confidential underlying data concerning critical infrastructure should only be retained only by the Registered Entity, but, even in such circumstances, auditing records should solely be retained under requirement by the Compliance Inforcement Authority. 2) Technical consideration should be given to determining the response to the "Compliance Monitoring Period and Reset Time Frame" section. The drafting team reference guide has suggested time periods aligning with audits cycles and less than monthly reset time frames. The response that it is not applicable does not appear consistent. 3) Lastly, item M1 under Measures has inadvertently dropped the "The" while the remaining M2 - M4 do contain "The" at the beginning of each sentence. In some of the following CIP standards, it is presented correctly, and, in others, it is not aligned within the M1 item.

Response:

1) The ERO Rules of Procedure include sections on dealing with confidential data associated with the Cyber Security standards, and recognize that there may be some evidence retained by the Responsible Entity. The data retention section of these standards was written to support this concept.

The language of 1.4.2 indicates that the Compliance Enforcement Authority "in conjunction with" the Registered Entity will retain all audit records from the previous audit and all audit records submitted since the previous audit, until completion of the next audit. This supports the audit intervals for all entities and supports the need to retain the confidentiality of some data.

The audit data retention period is determined by the audit period for each Registered Entity. The Reliability Coordinator, Transmission Operator and Balancing Authority are audited for each requirement once every three years – and all others are audited once every six years. The intent is to assure that, if there was an event and the performance of an entity was in question, there would be, at a minimum, at least one record showing the past performance of that entity.

2) The compliance monitoring period and reset timeframe were linked to an older version of the sanctions table, and have no relevance to the sanctions table currently in use. Until the Reliability Standards Development Procedure is updated, we cannot remove this heading from the standard template; until then all drafting teams are placing the phrase, "not applicable" under the heading, "Compliance Monitoring Period and Reset Time Frame" in the standard.

Organization	Yes or No	Question 13 Comment
3) The compliance staff assisted in developing a set of guidelines for developing measures and compliance elements in standards – and these guidelines do allow various data retention periods. **Phase 1 of this project includes necessary modifications to CIP-002-1 through CIP-009-1 to comply with the near term specific directives included in FERC Order 706. The issue identified in your comment is an issue better suited for a later phase of this project. The SDT suggests that you review the changes proposed in the later phases of the project and resubmit your comments as appropriate if they have not been addressed.**		
Ontario IESO	Yes	
Ameren	Yes	Would like to see a clarification on what is intended by phrase "shall make available" that is included in measures for each standard and whom an entity is supposed to make documents available to. The change from a three year retention for documents to a non-specific period will provide additional burden to the compliance process, since the region will have an arbitrary time length assigned per specific incident.
Response: **The phrase, "shall make available" means that the responsible entity must allow the Compliance Enforcement Authority to see the evidence. The evidence is made available to the Compliance Enforcement Authority** **The data retention periods for the standard requirements are specified in the standards. The language of 1.4.2 indicates that the Compliance Enforcement Authority in conjunction with the Registered Entity will retain all the audit records from the previous audit and all audit records submitted since the previous audit, until completion of the next audit. This supports the audit intervals for all entities. The audit data retention period is determined by the audit period for each Registered Entity.** **The audit data retention period is determined by the audit period for each Registered Entity. The Reliability Coordinator, Transmission Operator and Balancing Authority are audited for each requirement once every three years – and all others are audited once every six years. The intent is to assure that, if there was an event and the performance of an entity was in question, there would be, at a minimum, at least one record showing the past performance of that entity.**		
Consumers Energy Company	Yes	
Xcel Energy		
ISO New England Inc	Yes	1) - We agree with the removal of "reasonable business judgment" and "acceptance of risk."

Organization	Yes or No	Question 13 Comment
		2) - GENERAL COMMENT: As a general matter, NERC needs to explain how it plans on enforcing these standards. This is critical, because NERC is not defining what cyber-security practices are, in fact, acceptable. Therefore, if a company establishes a "high bar for its internal programs (e.g., training employees), and does not meet its own business practices, it can be fined by NERC. By contrast (and depending on how the standards are enforced) companies that set "low bars" for its internal programs will escape penalty. NERC could inadvertently, through its compliance and enforcement policy, incent companies to establish "lowest common denominator" practices.
Response: **1) The removal of "reasonable business judgment" was done in accordance with FERC Order 706. The revisions made to the standards in Phase 1 are intended to be responsive to specific FERC directives relevant to the onset of compliance audits in July 2009. The expansion of the Technical Feasibility Exception Process should address the concerns regarding the removal of reasonable business judgment and acceptance of risk.** **2) Phase 1 of this project includes necessary modifications to CIP-002-1 through CIP-009-1 to comply with the near term specific directives included in FERC Order 706. The issue identified in your comment is an issue better suited for a later phase of this project. The SDT suggests that you review the changes proposed in the later phases of the project and resubmit your comments as appropriate if they have not been addressed.**		
American Transmission Company	Yes	
TVA	Yes	
Duke Energy	Yes	
Brazos Electric Power Cooperative, Inc.	Yes	
Progress Energy	Yes	1) Overall comment - PE recommends the removal of "Reasonable business judgment" be replaced with the use of "good utility practice" as defined by FERC. 2) Overall comment - Section D – Data Retention – It is not practical to leave data retention period totally open ended at the sole discretion of the Compliance Enforcement Authority, there should at least be a capped limit, PE recommends a maximum of 3-years to allow time between audits.

Organization	Yes or No	Question 13 Comment
Response: **1) The removal of "reasonable business judgment" was done in accordance with FERC Order 706. The revisions made to the standards in Phase 1 are intended to be responsive to specific FERC directives relevant to the onset of compliance audits in July 2009. The expansion of the Technical Feasibility Exception Process should address the concerns regarding the removal of reasonable business judgment and acceptance of risk.** **2) The data retention periods for the standard requirements are specified in the standards. The language of 1.4.2 indicates that the Compliance Enforcement Authority in conjunction with the Registered Entity will retain all the audit records from the previous audit and all audit records submitted since the previous audit, until completion of the next audit. This supports the audit intervals for all entities. The audit data retention period is determined by the audit period for each Registered Entity.**		
Standards Review Committee of ISO/RTO Council	Yes	
KEMA	Yes	
Austin Energy	Yes	
Kansas City Power & Light	Yes	
San Diego Gas and Electric Co.	No	While the Standards Drafting Team has done a great job overall incorporating many of the issues raised in FERC Order 706 FERC, there appears to be two issues identified by FERC in Order 706 that have not been addressed by the Standards re-write team in these first revisions. FERC Order 706 directed in Paragraph 88 that features such as enhanced conditions on technical feasibility exceptions and oversight of critical asset determinations for CIP-002 are too important to the protection of the Bulk-Power System to wait until the 2009-2010 time period for the process to start. But no substantial modifications for CIP-002 in these areas are included from the SDT. In addition, FERC Order 706, in Paragraph 90, also directed the ERO, in its development of a work plan, to consider developing modifications to CIP-002-1 and the provisions regarding technical feasibility exceptions as a first priority, before developing other modifications required by the Final Rule. This doesn't appear to have been completed by the SDT as a first priority.

Organization	Yes or No	Question 13 Comment
Response: **In Paragraph 88, the Commission ordered revisions to the CIP standards not be delayed until completion of the Version 1 standards Implementation Plan, and specifically cited the CIP-002-1 and Technical Feasibility Exceptions (TFE) as priority revisions.** **The Commission at Paragraph 253 adopted the NOPR proposal requiring the ERO to provide additional guidance as to the features and functionality of an adequate risk-based assessment methodology, while leaving to the ERO's discretion whether to incorporate such guidance into the CIP Reliability Standard, develop it as a separate guidance document, or some combination of the two. The NERC Critical Infrastructure Protection Committee is in the process of developing specific Guidelines to address this requirement. The SDT believes the development of the Critical Asset and Critical Cyber Asset Identification Guidelines currently underway address the immediate concerns of the Commission. In addition, the SDT will be examining the entire risk management framework. Due to the complexity of this issue, the SDT decided to address risk management and its impact on CIP-002 early in Phase 2 in order to not delay the time-critical modifications directed elsewhere in the Final Order.** **The Commission at Paragraph 178 directed the ERO to develop a set of conditions or criteria that a responsible entity must follow when relying on the technical feasibility exception contained in specific Requirements of the CIP Reliability Standards. NERC Staff, with consultation with the SDT, has begun to develop a process for handling Technical Feasibility Exceptions (TFE) that is modeled after the existing self-report of non-compliance with mitigation plan process, as described in the NERC Rules of Procedure (ROP) Appendix 4C. The TFE process is not a "requirement" of a "standard" - it is a process for meeting requirements in standards. The TFE process is considered to be a compliance issue, although it is anticipated to be a way of being "compliant" with a standard in the event that an entity cannot meet the specific requirements of the standard. Because the TFE process is a compliance process, not development of requirements, it is outside the charter of the SDT. Therefore, the TFE process development and approval will be moving away from a direct SDT effort, to follow the established process for modifying the NERC ROP. As such, the SDT will not have a formal role in continued development of the process. The established ROP update process includes public comment and stakeholder input (including continued input from the SDT).**		

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Implementation Plan for Version 2 of Cyber Security Standards CIP-002-2 through CIP-009-2

Prerequisite Approvals

There are no other reliability standards or Standard Authorization Requests (SARs), in progress or approved, that must be implemented before this standard can be implemented.

Modified Standards

The following standards have been modified:
CIP–002–2 — Cyber Security — Critical Cyber Asset Identification
CIP–003–2 — Cyber Security — Security Management Controls
CIP–004–2 — Cyber Security — Personnel and Training
CIP–005–2 — Cyber Security — Electronic Security Perimeter(s)
CIP–006–2 — Cyber Security — Physical Security
CIP–007–2 — Cyber Security — Systems Security Management
CIP–008–2 — Cyber Security — Incident Reporting and Response Planning
CIP–009–2 — Cyber Security — Recovery Plans for Critical Cyber Assets

Red-line versions of the above standards are posted with this Implementation Plan. When these modified standards become effective, the prior versions of these standards and their Implementation Plan are retired.

Compliance with Standards

Once these standards become effective, the responsible entities identified in the Applicability section of the standard must comply with the requirements. These include:

- Reliability Coordinator
- Balancing Authority
- Interchange Authority
- Transmission Service Provider
- Transmission Owner
- Transmission Operator
- Generator Owner
- Generator Operator
- Load Serving Entity
- NERC
- Regional Entity

116-390 Village Blvd.
Princeton, NJ 08540
609.452.8060 | www.nerc.com

Newly registered entities must comply with the requirements of CIP-002-2 through CIP-009-2 within 24 months of registration. The sole exception is CIP-003-2 R2 where the newly registered entity must comply within 12 months of registration.

Proposed Effective Date

The proposed effective date for these modified standards is the first day of the third calendar quarter (i.e., a minimum of two full calendar quarters, and not more than three calendar quarters) after applicable regulatory approvals have been received (or the Reliability Standard otherwise becomes effective the first day of the third calendar quarter after BOT adoption in those jurisdictions where regulatory approval is not required).

For example, if regulatory approval is granted in June, the standards would become effective January 1 of the following year. If regulatory approval is granted in July, the standards would become effective April 1 of the following year.

Implementation Plan for Cyber Security Standards CIP-003-1~~2~~-2 through CIP-009-1~~2~~ or Their Successor Standards

Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities

This Implementation Plan identifies the schedule for becoming compliant with the requirements of NERC Standards CIP-003-1~~2~~ through CIP-009-1~~2~~ and their successor standards, for assets determined to be Critical Cyber Assets once an Entity's applicable 'Compliant' milestone date listed in the existing Implementation Plan has passed.

This Implementation Plan specifies only a 'Compliant' milestone. The Compliant milestone is expressed in this Implementation Plan table (Table 2) as the number of months following the designation of the newly identified asset as a Critical Cyber Asset, following the requirements of NERC Standard CIP-002-1~~2~~ or its successor standard.

For some requirements, the Responsible Entity is expected to be Compliant immediately upon the designation of the newly identified Critical Cyber Asset. These instances are annotated as '0' herein. For other requirements, the designation of a newly identified Critical Cyber Asset has no bearing on the Compliant date. These are annotated as *existing*.

In all cases where a milestone for compliance is specified (i.e., not annotated as *existing*), the Responsible Entity is expected to have all audit records required to demonstrate compliance (i.e., to be 'Auditably Compliant') one year following the milestone listed in this Implementation Plan. Where the milestone assumes prior compliance (i.e., is annotated as *existing*), the Responsible Entity is expected to have all documentation and records showing compliance (i.e., 'Auditably Compliant') based on other previously defined Implementation Plan milestones.

There are no Implementation Plan milestones specified herein for compliance with NERC Standard CIP-002. All Responsible Entities are required to be compliant with NERC Standard CIP-002 based on the existing Implementation Plan.

Implementation Schedule

There are three categories described in this Implementation Plan, two of which have associated milestones. They are briefly:

1. A Cyber Asset becomes the *first identified* Critical Cyber Asset at a responsible Entity. No existing CIP compliance program for CIP-003 through CIP-009 is assumed to exist at the Responsible Entity.
2. An existing Cyber Asset becomes subject to CIP standards, *not due to planned change*. A CIP compliance program already exists at the Responsible Entity.
3. A new or existing Cyber Asset becomes subject to CIP standards *due to planned change*. A CIP compliance program already exists at the Responsible Entity.

Note that the term 'Cyber Asset becomes subject to the CIP standards' applies to all Critical Cyber Assets, as well as ~~non-critical~~other (non-critical) Cyber Assets within an Electronic Security Perimeter.

Figure 1 shows an overall process flow for determining which milestone category a Critical Cyber Asset identification scenario must follow. Following the figure is a more detailed description of each category.

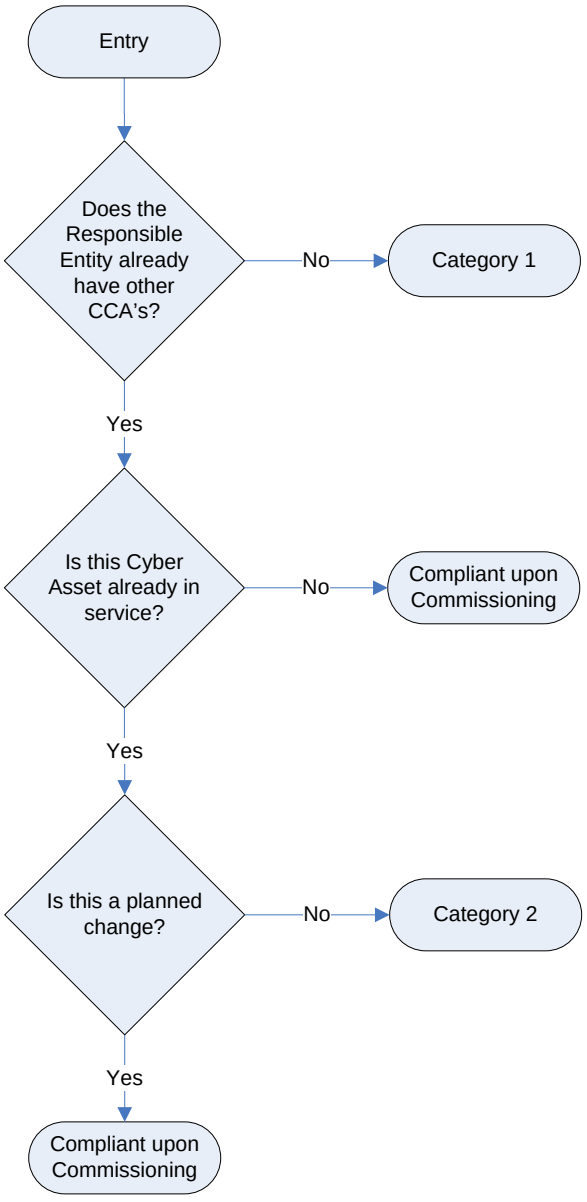


Figure 1: Category Selection Process Flow

The individual categories are distinguished as follows:

1. **Category 1**: A Responsible Entity that previously has undergone the CIP-002 Critical Asset identification process for at least one annual review and approval period without ever having identified any Critical Cyber Assets associated with Critical Assets, but has now identified one or more Critical Cyber Assets. The Compliant milestone specified for this Category shall be the same as Table 3 of this New Asset Implementation Plan. (Note that Table 3 of this New Asset Implementation Plan provides the same schedule as was provided in Table 4 of the original Implementation Plan for Standards CIP-003~~-1~~-2 through CIP-009~~-1~~-2.) As such, it is presumed that the Responsible Entity has no previously established cyber security program in force. Table 3 also shall apply in the event of a Responsible Entity business merger or asset acquisition where previously no Critical Cyber Assets had been identified by any of the Entities involved.

2. **Category 2**: A Responsible Entity has an established CIP Compliance program as required by an existing Implementation Schedule, and now has added additional items to its Critical Cyber Asset list. The existing Critical Cyber Assets may remain in service while the relevant requirements of the CIP Standards are implemented. Since the Responsible Entity already has a CIP compliance program, it needs only to implement the CIP standards for the newly identified Critical Cyber Asset(s).

   This category applies only when additional in-service Critical Cyber Assets or applicable other Cyber Assets are *identified*, not when they are added or modified through construction, upgrade or replacement.

   In the case of business merger or asset acquisition, if any of the Responsible Entities involved had previously identified Critical Cyber Assets, implementation of the CIP Standards for newly identified Critical Cyber Assets must be completed per Compliant milestones established herein under Category 2. In the case of an asset acquisition, where the asset had been declared as a Critical Asset by the selling company, the acquiring company must determine whether the asset remains a Critical Asset as part of the acquisition planning process.

   In the case of a business merger where all parties already have previously identified Critical Cyber Assets and have existing but different CIP Compliance programs in place, the merged Responsible Entity has one calendar year from the effective date of the business merger to continue to operate the separate programs and to determine how to either combine the programs, or at a minimum, combine the separate programs under a common Senior Manager and governance structure. At the conclusion of the one calendar year period, the Category 2 milestones will be used by the Responsible Entity to consolidate the separate CIP Compliance programs.

   A special case of restoration as part of a disaster recovery situation (such as storm restoration) shall follow the emergency provisions of the Responsible Entity's policy required by CIP-003 R1.1.

3. **Compliant upon Commissioning**: When a Responsible Entity has an established CIP Compliance program as required by an existing Implementation Schedule and implements a new or replacement Critical Cyber Asset associated with a previously identified or newly constructed Critical Asset, the Critical Cyber Asset shall be compliant when it is commissioned or activated. This scenario shall apply for the following scenarios:

    a) 'Greenfield' construction of an asset that will be declared a Critical Asset upon its commissioning or activation (e.g., based on planning or impact studies).
    b) Replacement or upgrade of an existing Critical Cyber Asset (or other Cyber Asset within an Electronic Security ~~perimeter~~Perimeter) associated with a previously identified Critical Asset.
    c) Planned a~~A~~ddition of:
        i. a Critical Cyber Asset, or,
        ii. an other (i.e., non-critical) Cyber Asset within an established Electronic Security Perimeter.

    In summary, this scenario applies in any case where a Critical Cyber Asset or applicable other Cyber Asset is being added or modified associated with an existing or new Critical Asset where that Entity has an established CIP Compliance Program as required by an existing Implementation Schedule.

    This scenario shall also apply for any of the above scenarios where relevant in the event of business merger and/or asset acquisition.

    A special case of a 'greenfield' construction exists where the asset under construction was planned and construction started under the assumption that the asset would not be a Critical Asset. During construction, conditions changed, and the asset will now be a Critical Asset upon its commissioning. In this case, the responsible Entity must follow the Category 2 milestones from the date of the determination that the asset is a Critical Asset.

    A special case of restoration as part of a disaster recovery situation (such as storm restoration) shall follow the emergency provisions of the Responsible Entity's policy required by CIP-003 R1.1.

    Since the assets must be compliant upon commissioning, no milestones are provided herein.

Note that there are no milestones specified for a Responsible Entity that has newly designated a Critical Asset, but no newly designated Critical Cyber Assets. This is because no action is required by the Responsible Entity upon designation of a Critical Asset without associated Critical Cyber Assets. Only upon designation of Critical Cyber Assets does a Responsible Entity need to become compliant with these standards.

As an example, Table 1 provides some sample situations, and provides the milestone category for each of the described situations.

Table 1: Example Scenarios

Scenarios	CIP Compliance Program:	
	No CIP Program (note 1)	Existing CIP Program
Existing Cyber Asset reclassified as Critical Cyber Asset due to change in assessment methodology	Category 1	Category 2
Existing asset becomes Critical Asset; associated Cyber Assets become Critical Cyber Assets	Category 1	Category 2
New asset comes online as a Critical Asset; associated Cyber Assets become Critical Cyber Asset	Category 1	Compliant upon Commissioning
Existing Cyber Asset moves into the Electronic Security Perimeter due to network reconfiguration	N/A	Compliant upon Commissioning
New Cyber Asset - never before in service and not a replacement for an existing Cyber Asset - added into a new or existing Electronic Security Perimeter	Category 1	Compliant upon Commissioning
New Cyber Asset replacing an existing Cyber Asset within the Electronic Security Perimeter	N/A	Compliant upon Commissioning
Planned modification or upgrade to existing Cyber Asset that causes it to be reclassified as a Critical Cyber Asset	Category 1	Compliant upon Commissioning
Asset under construction as an other (non-critical) ~~non-critical~~ asset becomes declared as a Critical Asset during construction	Category 1	Category 2
Unplanned modification such as emergency restoration invoked under a disaster recovery situation or storm restoration	N/A	Per emergency provisions as required by CIP-003 R1.1

Note: 1) assumes the entity is already compliant with CIP-002

Table 2 provides the compliance milestones for each of the two identified milestone categories.

Table 2: Implementation milestones for Newly Identified Critical Cyber Assets

CIP Standard Requirement	Milestone Category 1	Milestone Category 2
Standard CIP-002-2 — Critical Cyber Asset Identification		
R1	*N/A*	*N/A*
R2	*N/A*	*N/A*
R3	*N/A*	*N/A*
R4	*N/A*	*N/A*
Standard CIP-003-2 — Security Management Controls		
R1	24 months	*existing*
R2	~~1~~*N/A*	*existing*
R3	24 months	*existing*
R4	24 months	~~existing~~6 months
R5	24 months	6 months~~*existing*~~
R6	24 months	6 months~~*existing*~~
Standard CIP-004-2 — Personnel and Training		
R1	24 months	*existing*
R2	24 months	18~~6~~ months
R3	24 months	~~6~~18 months
R4	24 months	~~6~~18 months
Standard CIP-005-2 — Electronic Security Perimeter		
R1	24 months	12 months
R2	24 months	12 months
R3	24 months	12 months
R4	24 months	12 months
R5	24 months	12 months
Standard CIP-006-2 — Physical Security		
R1	24 months	12 months
R2	24 months	12 months
R3	24 months	12 months
R4	24 months	12 months
R5	24 months	12 months
R6	24 months	12 months
R7	24 months	12 months
R8	24 months	12 months

CIP Standard Requirement	Milestone Category 1	Milestone Category 2
Standard CIP-007-2 — Systems Security Management		
R1	24 months	12 months
R2	24 months	12 months
R3	24 months	12 months
R4	24 months	12 months
R5	24 months	12 months
R6	24 months	12 months
R7	24 months	12 months
R8	24 months	12 months
R9	24 months	12 months
Standard CIP-008-2 — Incident Reporting and Response Planning		
R1	24 months	6 months
R2	24 months	~~0~~6 months
Standard CIP-009-2 — Recovery Plans for Critical Cyber Assets		
R1	24 months	6 months
R2	24 months	~~0~~12 months
R3	24 months	~~0~~12 months
R4	24 months	6 months
R5	24 months	6 months

Table 3[1] Compliance Schedule for Standards CIP-002~~-1~~-2 through CIP-009~~-1~~-2 or Their Successor Standards For Entities Registering in 2008 and Thereafter				
	Upon Registration	Registration + 12 months	Registration + 24 months	Registration + 36 months
Requirement	**All Facilities**	**All Facilities**	**All Facilities**	**All Facilities**
CIP-002~~-1~~-2 Critical Cyber Assets or its Successor Standard				
All Requirements	**BW**	**SC**	**C**	**AC**
Standard CIP-003~~-1~~-2 — Security Management Controls or its Successor Standard				
All Requirements Except R2	**BW**	**SC**	**C**	**AC**
R2	**SC**	**C**	**AC**	**AC**
Standard CIP-004~~-1~~-2 — Personnel & Training or its Successor Standard				
All Requirements	**BW**	**SC**	**C**	**AC**
Standard CIP-005~~-1~~-2 — Electronic Security or its Successor Standard				
All Requirements	**BW**	**SC**	**C**	**AC**
Standard CIP-006~~-1~~-2 — Physical Security or its Successor Standard				
All Requirements	**BW**	**SC**	**C**	**AC**
Standard CIP-007~~-1~~-2 — Systems Security Management or its Successor Standard				
All Requirements	**BW**	**SC**	**C**	**AC**
Standard CIP-008~~-1~~-2 — Incident Reporting and Response Planning or its Successor Standard				
All Requirements	**BW**	**SC**	**C**	**AC**
Standard CIP-009~~-1~~-2 — Recovery Plans or its Successor Standard				
All Requirements	**BW**	**SC**	**C**	**AC**

[1] The phase in of compliance in this table is identical to the phase in for CIP-002-1 through CIP-009-1 identified in Table 4 of the 2006 CIP Implementation Plan.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Draft Meeting Summary

Cyber Security Order 706 SDT — Project 2008-06

March 10, 2009 | 1–5 p.m. EST
March 11, 2009 | 8 a.m.–5 p.m. EST
March 12, 2009 | 8 a.m.–noon EST
http://www.nerc.com/filez/standards/Project_2008-06_Cyber_Security.html

Meeting Summary Contents

116-390 Village Blvd.
Princeton, NJ 08540
609.452.8060 | www.nerc.com

EXECUTIVE SUMMARY

The Chair, Jeri Domingo-Brewer, welcomed Frank Kim, Power System IT oversight — Ontario Hydro as a new member of the SDT replacing Michael Winters. She also noted that this meeting will be Tom Hoffsetter's last meeting on the SDT as he will be taking a position with NERC in their compliance group. She also noted that Bryan Singer had resigned as he is unable to fully participate in the SDT. Finally, Kevin Perry, Vice Chair, noted that he would be taking up a new position as SPP director of Critical Infrastructure Protection.

Joe Bucciero conducted a roll call of members and participants, the Chair reviewed the meeting objectives and the facilitator, reviewed with the team and participants the proposed meeting agenda.

Mr. Bucciero reviewed with the team the need to comply with NERC's Antitrust Guidelines. The team reviewed and unanimously adopted on March 12 the SDT February 18–19, 2009 meeting summary. Stuart Langton, SDT facilitator, reviewed the current work plan and meeting schedule for both Phase 1 and Phase 2 development. At the conclusion of the meeting the SDT agreed on a schedule of meetings from July-December, 2009.

NERC staff indicated the Technical Feasibility Exception white paper is being prepared for posting for industry comment. If posted promptly, the TFE posting will occur within the 14 day window the SDT agreed to when it approved the Phase 1 products for industry review, and thereby permit industry balloting of the Phase 1 products to begin in early April 2009. Regional entities received an early preview and briefing of the TFE white paper for any compliance and resource implications associated with the TFEs. Michael Assante, CSO at NERC, met with FERC staff to brief them on the TFE and the SDT 706 Phase 1 products.

Dave Taylor set out the process for developing the Version 2 Violation Security Levels (VSLs) noting that NERC was seeking to post the VSLs by Monday, March 16 in coordination with the Version 1 VSLs. He noted the plan is to pre-ballot review for Version 2 (that applies to the SDT's Phase I products) by May 11, 2009 and provide a 30-day industry comment period. On day-three, David Taylor reviewed with the SDT the Violation Risk Factors (VRFs) associated with the Cyber Security standards, and these were unanimously adopted by the SDT.

Joe Bucciero reviewed the Phase 1 Response document that was circulated to the Team earlier in March and the SDT unanimously adopted the response document for posting.

The facilitators reviewed the Phase 2 concept development which was initiated in the fall of 2008 by the SDT. In November there were criteria suggested for the design of the process. In December there were presentations and discussions regarding risk management. In January and

February 2009 two concept papers were developed that looked at two approaches to Phase 2: one which worked within the current CIP and sought to integrate applicable NIST and other ideas; the other started with a review of the NIST approach and sought to bring some of the CIP elements into a NIST-like model. At the conclusion of the February 18-19, 2009 meeting, the SDT asked the two teams working on the concepts to produce an initial draft of a CIP-002 standard that would be consistent with their concepts. These CIP-002 concept papers were reviewed, compared, and considered for possibly merger.

Bill Winters and Phil Huff presented a CIP-002 strawman alternative (Strawman A) developed by one team since the February meeting. The concept suggested:

- Assign 'functions' to systems
- Identify BES cyber systems
- Engineering studies used to develop Impact Criteria
- Use criteria in calculation of impact (integrity, availability, confidentiality)
- Categorization process (hi, med, low, none)
- Categorized BES cyber systems.

The discussion that followed covered issues such as: Connectivity to Networks; Increase in the scope of the CIP; Role of RROs and REs; Focus on information security; Updates for the standards; Boundaries; and 3rd Party Review.

Jackie Collett presented a second CIP-002 strawman (Strawman B). She noted that the CIPC Risk Assessment Working Group's (RAWG) work and draft report were helpful in the preparation and thinking for the concept paper. The CIP-002 concept paper started with the connections to BES-which is an engineered system. Cyber assets support the reliability of the BES. She suggested the strawman approach builds on: industry work, experience and investments in compliance programs but noted that the identified risks will increase scope of compliance. The concept paper addresses facilities, equipment, and systems, but acknowledges a need to better define systems going forward. The approach is not a risk assessment, but an impact assessment of the reliability of the BES. The CIPC RAWG work focuses on "impacts." Cyber assets are one of many elements supporting the BES processes. The concept paper proposes that properly applying a top down approach will ensure the reliability of the BES. She suggested the SDT should consider including some concepts from the RAWG in the new CIP-002 standard where it makes sense. The approach included in the strawman avoids being prescriptive but considers categorization of the BES assets as critical or not. The approach also considers the impact of the associated cyber assets as (3) low, (2) moderate, (1) high, and possibly none. The oversight of critical asset lists remains an open question at this point. The approach suggests using and incorporating NIST controls as a good starting point.

The discussion that followed covered issues such as: degree of flexibility and prescription; engineering-based assessment; list of cyber assets; and implementation phase.

As a follow-up to the discussion, the SDT members were given a brief survey to evaluate the two proposed approaches. The SDT reviewed the results of the overnight member survey, which suggested that the strawman approaches were generally in alignment with the overriding principles and have more in common than they differ. The facilitators asked members to offer elements of the strawman approaches they felt were strengths: (1) the simplicity and the definitions of Strawman A; (2) the critical asset identification associated with the BES that addresses the interrelationships of engineering, electric, and cyber systems in Strawman B.

The SDT discussed and refined the following common propositions drawn from day one's discussion on the two CIP-002 strawman approaches:

1. Existing CIP language is insufficient for the future
2. Ground the approach in the context of NERC's 6 elements of reliability adding cyber security to each
3. Utilize the graduated levels (high, moderate, low, and "who cares") in the approach
4. Include systems, facilities, and equipment *(build on the CIPC Working Group Draft Guidelines)*
5. Provide for 3rd party oversight and accountability in the process
6. Address the external interfaces impacting on BES reliability
7. Build upon existing controls such as the NIST 800-53 suite of controls

The facilitators suggested several discussion questions following the presentations and discussion of the strawman options including:

- What is the best place for the CIP-002 approach to start? From facilities? From Systems? From either? From both?
- What is the best approach to 3rd party oversight and accountability?
- What is the best approach to addressing external interfaces?

After some discussion, the SDT members agreed to break into two small discussion groups on the morning of Day Two to explore and focus on the possible merger of the two strawman approaches and concepts. Following lunch, each group reported the results of their discussion and engaged in a full SDT discussion of the issues.

The proposed structure of the draft CIP-002 standard has the following six requirements:

R1 — Identification of BES Assets
R2 — Critical Asset Identification Method
R3 — Critical Asset Identification

R4 — Cyber Asset Identification
R5 — Categorization of Cyber Assets
R6 — Annual Approval

The small group looking at Requirement R1 explored the possibility of merging a "facilities vs. functional" approach. They agreed that the starting point should be to identify the functions necessary for the reliability of the BES. The group agreed that it would then be necessary to identify the systems or hardware used to perform those functions. It would then be necessary to incorporate the high, moderate, low impact threshold each into category.

The small group looking at Requirement R4 suggested that the "systems" references should be taken out of R1 and only the "functions" of the BES should be included in R1. Requirement R4 should then identify the systems that support and perform the R1 functions.

Scott Mix presented a strawman for an approach to CIP-002 Requirements R2 and R3 for consideration by the SDT. He suggested starting with the functions and mapping them to the physical equipment. Consider determining "Asset Impact" as high, moderate, low, and none and "Cyber impact" as high, moderate, low, and none for CIP 003-009. After discussion the SDT ranked the three proposals:

Proposal 1 Keep R2 + R3 with Scott's Language (Matrix) (Average 2.9 of 4)
Proposal 2 Move R2 & R3 into R5 (Vector Analysis) (Average 2.7 of 4)
Proposal 3 R2 + R3 Performed by External Entity (Average 1.8 of 4)

The SDT agreed these proposals needed further review and consideration in the context of a single, coordinated approach.

At the end of the second day, a small group agreed to work further to draft a common framework. The group included Phil Huff, John Lim, Scott Mix, Jackie Collett, Scott Rosenberg and John Varnell. Jackie Collett introduced a flow chart as a strawman designed to be flexible to allow for further development and refinements, and it focuses on cyber systems (not on assets) and does not offer a hierarchal model. The "vector" categorization- matrix offers some more granularity as to what we are meaning to accomplish. It offers a cyber impact analysis of the impacts on the functions.

Following the discussion, the SDT agreed to rank the acceptability of the following proposition:

The SDT should adopt this approach as a working conceptual model to develop and frame a concept white paper that includes a set of definitions/glossary, develops a list of functions, and uses lists of scenarios to test the concept.

Acceptability	*4 =*	*3 = acceptable, I*	*2 = not acceptable unless*	*1 = not*	*Avg.*

Ranking Scale	*acceptable, I agree*	*agree with minor reservations*	*major reservations addressed*	*acceptable*	
3-12 SDT rank	**15**	**3** *(1/2)*	**1**	**1**	**3.6 of 4**
Second Rank with D Norton's Concept	**15**	**3**	**2**	**0**	**3.65 of 4**

During the discussion of the approach going forward, concern was expressed about whether the SDT was the right group to develop the concepts for Requirements 1,2, and 3 (the left hand side). Planning and operations perspectives would be helpful. Dave Taylor volunteered and the SDT agreed that he should draft a white paper to present to the next meeting on a process for determining Requirements 1, 2, and 3.

CIP-002 Common Framework Concept

Identification of BES functions which support the reliability and operability of the BES

Need 1 layer of specificity below ALR

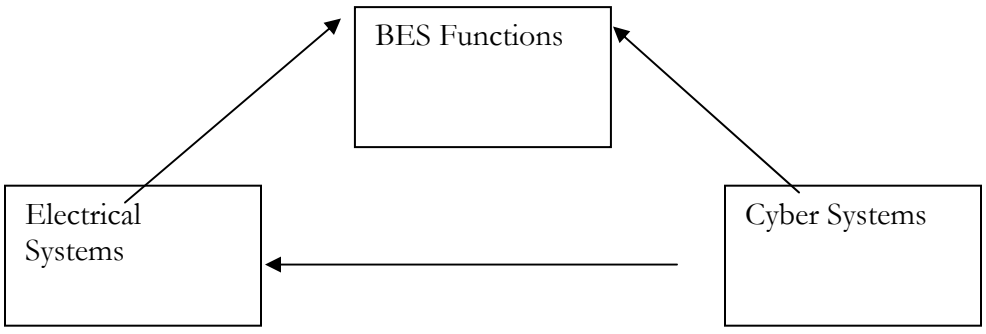
Cyber Impact — the local impact due to loss of CIA of the cyber asset for a BES element

System — a set of components which must work together

Electric System — a set of BES elements which must work together

Cyber System — a set of cyber components which must work together

Pre-Determined Functions			
R1	List of Electric Systems which support the BES functions	R4	List of Cyber Systems which support the Electric Systems and/or BES Functions
R2	Method of Categorization - impact to BES	R5	Method of Categorization - local impact to Electric System components
R3	List of Systems & Categories	R6	List of Systems & Categories
R7	Matrix: combines the 2 impact levels		
R8	Local Approval		
R9	Oversight		



Bill Winters requested the SDT rank the following proposition that if acceptable would be incorporated into the white paper going forward as the CIP-002 intent statement:

CIP-002 is intended to provide a discovery methodology that will lead to explicit identification and categorization of all cyber elements that perform or support BES functions. (3.9 of 4)

The SDT agreed that a helpful next step would be to refine the concept that was presented and tested on the third day to be in the form of a draft white paper. The chair asked Jackie Collett, John Lim, Bill Winters, and Phil Huff along with Scott Mix to take the lead in the development of the draft white paper in advance of the April meeting, building on the discussion and outcomes of this meeting. Other members would be welcome to send ideas and reactions as well as listen in and participate on the WebEx meetings that would be convened. The goal would be to share the white paper with the industry following either the May, 2009 or June, 2009 meeting.

The SDT members completed calendar forms regarding possible dates for future SDT meetings. Upon review of the forms and SDT member scheduling conflicts, the following dates and tentative locations were established and agreed to by the team.

Project 2008-06 — CSO 706 SDT
Proposed Dates and Locations for Future Meetings 2009

Dates in 2009	Location
April 14–16	Charlotte, NC
May 13–14	Boulder City, NV
June 17–18	Portland, OR
July 13–14	Toronto, CA
August 20–21	Chicago, IL
September 9–10	Denver, CO
October 20–22	New Orleans, LA
November 17–18	Atlanta, GA
December 15–17	Key West or FRCC (Tampa, FL)

The SDT agreed to seek to make a progress report to the MRC at its May meeting in Arlington, Virginia and provide a substantive briefing on the Phase 2 white paper for input at their August meeting. The team discussed the timing and objectives for a workshop. The SDT decided to hold open the question of convening an expert/stakeholder workshop pending the Chair and Vice Chair's discussion with Michael Assante, NERC Chief Security Officer, to gain a clearer understanding of the potential objectives, design, and timing of a workshop in light of the SDT's progress and schedule.

The facilitators offered some observations on the SDT's work over the past six months and suggested it would be timely to survey the team on the experience over the past six months to provide an opportunity for deeper shared reflections on the ways to improve the team's process.

The chair asked the facilitators to develop and distribute a survey to review the results at the April meeting.

The meeting adjourned at 11:30 a.m. on March 12, 2009.

I. Introductions, Agenda Review and Review of SDT Work plan

The Chair, Jeri Domingo-Brewer, welcomed the members. She welcomed Frank Kim, Power System IT oversight — Ontario Hydro as a new member of the SDT replacing Michael Winters. She also noted that this meeting will be Tom Hoffstetter's last meeting on the SDT as he will be starting work with NERC in their compliance group. She also noted that Bryan Singer had resigned as he was chairing a related group and had been unable to fully participate in the SDT. Finally, Kevin Perry, Vice Chair, noted that he would be taking up a new position as SPP director of Critical Infrastructure Protection.

Joe Bucciero conducted a roll call of members and participants in the room and on the conference call for each day *(See appendix #2*). The Chair reviewed the meeting objectives and Bob Jones, facilitator, reviewed with the team and participants the proposed meeting agenda.

Mr. Bucciero reviewed with the team the need to comply with NERC's Antitrust Guidelines. He urged the team and other participants in the process to carefully review the guidelines as they would cover all participants and observers. He urged all to avoid behaviors or appearance that would be anti-competitive nature and also reminded the group of the sensitive nature of the information under discussion.

The team reviewed and unanimously adopted on March 12 the SDT February 18–19, 2009 meeting summary.

Stuart Langton, SDT facilitator, reviewed the current work plan and meeting schedule for both Phase 1 and Phase 2 development. (*See Appendix #4)*

II. Technical Feasibility Exception Update and SDT Discussion

Scott Mix noted that NERC staff believes it is ready for posting for industry comment. Regional entities will receive an early preview of the TFE for any compliance and resource implications (March 6). Michael Assante, CSO at NERC met with FERC staff to brief them on the TFE and the SDT 706 Phase 1. He noted that Dave Cook, NERC General Counsel indicated that the target was to post the TFE at end of week. This would bring it within the 14 days the SDT agreed to when it approved the phase 1 products for industry review. This would allow industry balloting starting in early April.

SDT Member comments

- Any substantial change since December? As was discussed in the February 18-19 SDT meeting, the TFE can be claimed only where it is specifically allowed to be claimed under the FERC Order 706.
- SDT may support a TFE through a standard modification regarding operations and safety in phase II.

- Removing risk acceptance- didn't put back in where "technically feasible" requirement for compensating measures. Just not a procedure through the TFE. Like documenting the compensating controls.
- The SDT can deal with TFE in Phase 2 standards
- People in industry are worried- when will they get it? TFE not applicable to every standard and requirement.
- R5- would language have to exist in each sub-requirement? No, if in main requirement applies to all sub-requirements.
- Applicability model will be part of the posting for TFE? Yes it is there.

III. VSL and VSR Committee Update

Dave Taylor set out the process for developing the Version 2 VSLs. He noted that NERC was seeking to get the Version 1 VSL document posted by Monday, March 16. He noted the plan is to pre-ballot review for Version 2 VSL (i.e. Phase 1) by May 11, 2009 and provide a 30 day industry comment period.

SDT Member Comments on VSLs

- Interrelationship between the two VSLs need to be clarified for the industry.
- If industry doesn't approve version 2 (i.e. Phase I) CIPs OR the VSLs, NERC will have to file something with FERC. The NERC BOT has to approve any filing. May take a BOT override on the process.
- Along with VSL and standards timing. Industry needs to understand the TFE process. Many things to understand in terms of the inter-relationships.
- NERC planning to launch a separate web page and a separate announcement and a note in the NERC newsletter.
- NERC should consider making a "Gant chart" on web page- highlighting the timing for review and adoption with definitions of what they each do and why it is important that they happen in the right timing.
- Is NERC planning on providing information to the ballot body of the ramifications of a failed Phase I ballot? Industry should know what will happen if it fails to pass. Prefer to know beforehand what will happen.
- NERC needs to be careful about the perception of threatening the industry. NERC will do the bare minimum to meet FERC directive if the ballot doesn't pass.
- Can FERC be approached for an extension? No, it has already passed and it is now federal law.
- We need some kind of dialogue mechanism with the industry- blog, webinar, get information to the industry. Need to careful about managing expectations about the turnaround.
- Who would be responding to industry questions? With what authority? etc. NERC would have to dedicate a full time person to response.

- What happens if registered ballot body votes down version 2 standards. This is a non-trivial thing in the era of the ERO. "Smoldering anomaly." Ask FERC- what do we can/should do. We played the game and industry won't budge. There is precedent for BOT overruling a no vote in the period before the current ERO status. In the era of ERO will this fly?
- Same problem with FAC standards-. NERC understands and has to follow the ANSI process.
- The audit issue in July may pose a unique problem and NERC might be able to get through the filing process without raising too many eyebrows.
- If Phase I does fail, NERC and the SDT should look at responses before make decisions what to take to FERC.
- We should encourage NERC all with ideas for engagement with the industry stressing the importance of a consistent message- Will NERC be going to all regions?
- SDT 706 Slide presentation to timelines- send to all members- Scott Mix- Dave Taylor , Joe Bucciero and Kelly at NERC will do so. Also work with regions through the team.

On day-three, David Taylor reviewed with the SDT the VRFs and additional language for Requirement 1.8, noting that most reviews were judge to be "medium". He asked for feedback on the proposed levels. He noted that if the SDT approved they would be posted today along with the Version 1 VSLs. A motion for the SDT to accept the draft (John Lim, Bill Winters 2nd) and unanimously adopted by the SDT (18-0).

IV. Phase I Response and Timeline

Joe Bucciero noted that the Phase 1 Response document was circulated to the team earlier in March for their review. The chair entertained a motion (Freese, Edwards 2nd) and the SDT unanimously approved the response document for posting.

V. Phase II Concept Development

Stu Langton noted that the Phase 2 concept development was initiated in the fall of 2008 by the SDT. In November there were criteria suggested for the design of the process. In December there were presentations and discussions regarding risk management. In January and February two concept papers were developed that looking at two approaches to Phase 2: one which worked within the current CIP and sought to integrate applicable NIST and other ideas; the other which started with a review of the NIST approach and sought to bring some of the CIP elements into a NIST-like model. At the conclusion of the February 18–19 meeting the SDT agreed to ask the two teams working on the concepts to produce an initial draft of CIP-002 consistent with their concepts for review and comparison and possibly merger.

A. CIP 002 Strawman #A — Concept Proposal Presentation Overview

Bill Winters presented the drafting team's CIP-002 strawman (See Appendix # 6) as was agreed at the February 18–19 SDT meeting. SDT members participating on the team included: Jerry Domingo Brewer, Phil Huff, Kevin Perry, John Southern, Keith Stoffer and Bill Winters. He noted they used Kevin Perry's concept paper presented at the last meeting as the guide for

developing the CIP 002 and that this was a systems-based approach in terms of systems control and systems awareness which started with looking at core function systems/assets. He described a reverse "peeling of the onion" approach, starting from the insider out. The team started with a series of "nested" definitions of cyber asset, cyber system and control systems- all nested within cyber systems.

The team's intent was to try to simplify a systems approach — e.g. start at your SCADA server, what is connected to it providing data to it, continuing to walk out to your historically system and on to determine full scope of the system using in control and system awareness. They sought to define one or more security boundaries (R2) then identity security boundaries around systems. They introduce a categorization criteria model (low, med high) to apply to cyber systems (R4.) That would be approved and reviewed at regional level. The approach allows some flexibility, region-to-region. E.g. working groups within regional entities could work to define for each region. Then remaining CIP standards apply. Deal with mapping to low, medium and high. (R5) Implement a change- need to assess. How to capture interconnected external entities (R7)

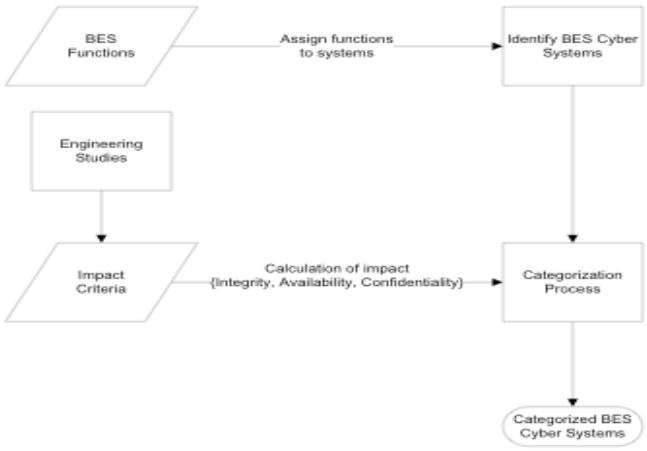
SDT Member Q & A and Discussion

- **Categorization at the regional level.** R4 — regional categorization? Which entity? The region itself. E.g. ERCOT. Do they have the capacity to do this? Regions will need to understand this approach going forward.
- Region would approve the criteria for the thresholds, e.g. less than 300 mw low, 300-800 moderate, above 800 high. Region wouldn't look at the cyber asset or system.
- **Confidentiality —** Are there confidentiality issues that need to be addressed with the approach? Establishing a framework for the categorization model- would be a risk impact model at a regional level.
- **Inconsistent regional interpretations —** If we regionalize decision making around R4- how does NERC deal with inconsistent interpretations?
- Regions might petition to NERC.
- Does R7 create a legal duty to do something? Why there? Concern we may have inconsistent responses across the regions, one entity take action against another?
- High medium and low- needs to be consistent across all regions and entities. What is in the standard is what is audited to. Sounds like a "fill in the blank" standard.
- **Connectivity to Networks —** Concern about idea of connectivity or network connectivity having been lost? Implies this evaluation of systems would have to take place on any equipment regardless of their connectivity to networks. Would all these have to be evaluated?
- Network communications was left out of the description because communications standards would take care of this. Systems approach looks at interconnection. Isolated item would be assessed for connectivity- unless it was in the "lower than low" category.
- Approach focuses on system and data exchanged within system and between systems.

- **Increase in scope —** A facility with serial connected devices collecting data would not be covered by the current CIP? This may pose a significant scope increase in terms of assessment.
- Terminology needs to be tightened. Ran into that in trying to implement and audit the current CIP standards. Need to make immediately obvious to anyone what is a reasonable understanding of what it is we are after in these standards.
- **RROs and REs —** Regional approval? Region doesn't exist- either RRO or RE. Is it a jurisdictional entity that requirements can be tied to? Regions RROs RE may not have technical competency to do this yet.
- **Focus on information security —** Are we focusing on hardware vs. information/data we need to perform functions that will come through different systems that are "data feeds?" Information security is the focus. Region is not where it is at. Reliability coordinators will need to decide this. Not operating in a vacuum. Region could have function of holding meetings of RCs.
- Look at the mission then look at the equipment. Different levels of requirement based on your threat profiles.
- There is a disconnect on how regions will apply this. One company can cover 5 regions. How will one system be treated with 5 regions telling us what to do. Needs to be applied the same. This is important and not sure how it will be taken care of in the "systems" approach.
- Jeri Domingo Brewer shared a presentation of how BOR does asset categorization process at the February 2-4 meeting in Phoenix. The same situation happened in the Federal sectors when they had to categorize their systems. There is a corporate impact that needs to be assessed if you lose functional capability.
- Address realities in how infrastructure is operated so that standards can be audited in a consistent manner.
- The SDT may be caught in the language. Focus instead on the approach that is being proposed. Fundamental to the approach is the way of arriving at which assets should be protected. IT marries a functional view with the traditional engineering approach. There will be follow on activities as to what to do with the standards.
- ERCOT region/ISO wide area visibility- criticality of any assets. ISO functioning as a RC? Lots of things to look at. If you declare assets to be critical that the responsible entity doesn't agree. Number of aspects are complicated need to recognize this.
- Acknowledge the point about addressing companies who straddle multiple regions. Didn't want NERC to mandate across the board what the threshold criteria would be. E.g. the nature of congestion of northeast may be different than that of the midwest etc.
- Engineering model applied to cyber asset vs. the other way around.
- **Updates —** Updating once every 3 years vs. annually. Consider all the assets that manage the grid. High moderate low and maybe "lower than low." After initial investment in the classification, the future efforts will be building on that.

- **Boundaries** — R2 — one or more boundaries allows flexibility. In concept paper did not represent telecommunications functioning- you can't manage or control it. Preserved the concept of it being out of scope-not including devices.
- Limit to Cyber systems that do something. Protect the data. Depending on where you draw your boundaries, scope of telecommunications.
- R7- doesn't exist in the standards today. Finds this to be a huge problem. Need to find a way to address. Calls for communication with external RE.
- **Critical** — The strawman doesn't use word critical. Current reliability standards — BPS — violation of risk factors high, medium low. Equivalency? Somebody has to protect anything that could possibly violate a requirement. Label that as a critical asset. If you violated that requirement because of cyber security incident.
- Look at existing tools and concepts used to try to determine how important things are.
- **3rd Party Review** — FERC order- appropriate 3rd party approval — region was an attempt. "appropriate 3rd party review to be determined"
- Description of the process proposed:
    - R1- scope your systems affecting BES. (kick out such things as customer service etc).
    - R4 Assess as low, medium, high.
    - Start with information — captures intent of CIP. 3rd party concept allows for not a solution but a requirement.
    - R3 prevent gaming.
    - R6 internal controls
    - R7- heartburn- negotiation and arbitration method to agree on a list- walk away equally unhappy.
    - "Networks" captured in cyber assets definition.
    - Better model for defining function.
    - Take approach for determining critical functions.
    - Public concern is with remote configuration capability (a la Aurora) engineering support and maintenance. Systems in place but with remote access.
    - Treatment — "my identify" password synchronization- HR system. Shut off access in a keystroke in Corporate IT land. What is a peripheral system?

On the afternoon of day two the following flowchart was presented and discussed:



Bill Winters presented the straw man A CIP-002 flow chart process and summarized the steps:

- Assign function to systems
- Identify BES cyber systems
- Engineering studies leading to Impact criteria
- Use criteria in Calculation of impact (integrity, available confidentiality)
- Categorization process (hi, med low, not)
- Categorized BES cyber systems.

SDT Member Comments on Strawman A Flowchart

- Incorporate engineering into categorization?
- Power systems and computer systems networks. 2 and 3 are power systems.
- Where do lists of functional impacts come from and at what point? (identify BES cyber systems)
- Shrink to cyber systems? Need to have all the pieces to perform a function? Shrink or whittled?
- Categorization to each cyber system on list- box? Oval- CIP standards on 002 applied to categorized BES cyber systems.

B. CIP-002 Strawman #B — Concept Proposal Presentation Overview — Jackie Collett, John Lim, Scott Rosenberg and John Varnell

Jackie Collett presented the team's CIP-002 strawman (*See Appendix #7).* She noted the ~~CIPSE~~CIPCCIPC Risk Assessment Working Group's (RAWG) work and draft report was helpful. Their concept started with the connection to BES — which is an engineered system. Cyber assets support the reliability of the BES. They address facilities, equipment and systems but acknowledge a need to define systems going forward. Their approach is not a risk but an impact assessment of the reliability of the BES. ~~CIPSE~~CIPCCIPC RAWG, focuses on "impacts." Cyber assets are one of many elements supporting the process. They propose that properly applying top down approach will ensure the reliability of the BES. She suggested the SDT should consider including some concepts from the RAWG in the standard where it makes sense. Their approach avoids a prescriptive approach but considers categorization of critical assets of BES — critical or not. Consider critical cyber assets: (3) low, (2) moderate, and (1) high and some that need no protection in transmission and generation. The oversight of critical asset lists- remains an open question at this point. Use and incorporate NIST controls that provide some good starting points.

She suggested the approach builds on: industry work, experience and investments in compliance programs but noted that the identified risks will increase scope of compliance. She then reviewed CIP 002 draft requirements and changes.

SDT Q & A Member Comments

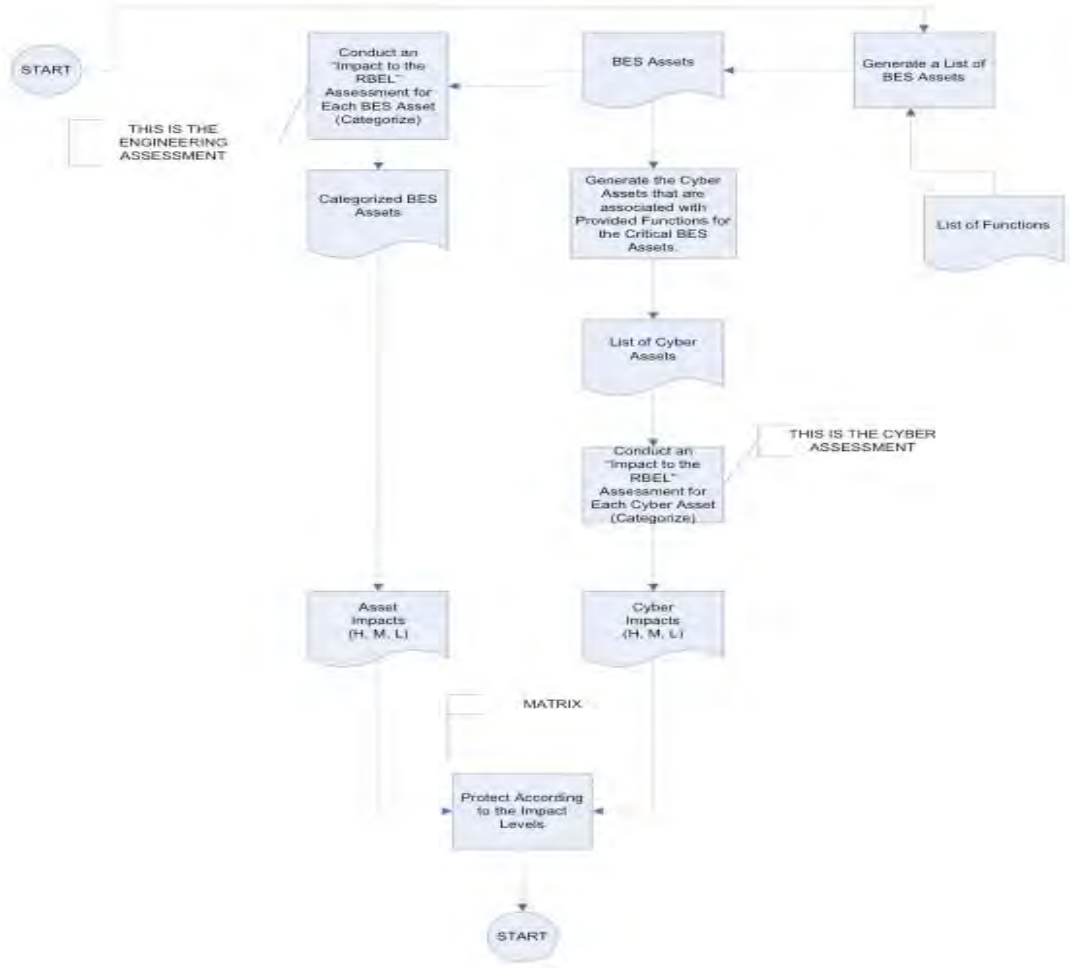
- What is the right balance between overly prescriptive and too loose?
- The six NEC principles of adequate levels of reliability can be core principles for developing standards. This will go a long way towards providing credibility for the SDT's proposed CIP standards.
- Didn't see a requirement for assessing the impact of the assets before assessing impact of cyber assets. This is a two-step process. Assess high, medium low none, on electrical assets

and then on cyber asset. Matrix: rigor for requirements. High and high highest level of rigor etc.

- Lends itself to NIST approach. Goes a long way
- The team agrees with these comments and left it out for simplicity case.
- The two strawman proposals (A & B) are not at polar opposites of positions. There are many commonalties with the main differences being the risk assessment vs. impact assessment.
- High impact? Critical asset that is also a cyber asset — current CIP don't address.
- EMS data system- cyber asset. Our control system (function) was the critical asset.
- Agree that there is a huge amount of judgment around identifying the assets.
- Why haven't we asked industry — to submit examples of excellent methodologies of categorizing assets? Did ask through the ~~CIPSE~~CIPCCIPC last year.
- Many are paid for methodologies and there is a reluctance to share methodologies based on issues of confidentiality.
- Cyber being a critical asset. Last drafting team- moved to function.
- Impact categorization- high medium low. Network automation-
- Substation lab with metering doesn't work through fire walls. Look at function of relay- may have some pieces not as important as others.
- Network automation "support" vs. "intrinsic" to the operation?
- How do we do this.
- A9- how far apart are we? End result of both approaches is a list of cyber assets. Both identify all. If critical assets — start with systems. Apply engineering criteria.
- Not all things considered as part of system. One looks first at physical then others supporting it.
- Both looking at impact of cyber system on reliability of the BES.
- Not just focusing on physical assets. Important to look at function. Inclusion of systems if they are assets related to that function.
- Strawman A suggests that threshold criteria for impact determination be set. Can we link criteria to adequate level of criteria?
- Difference from engineering look and then the other way around.
- Engineering based assessment is critical to both approaches. R4 — assess the risk of those systems. First criteria — what asset it supports 25 mw or 1000.
- Start with a list of systems or a list of assets. Starting point is the difference.
- Differences- one is bottom up and the other top down. Subtle differences in terminology. Asset vs. system.
- Consistent guidance in body of standards — white paper as an attachment to body of standard. De facto implementation guide. Consistent method of categorizing assets. Because it is part of standard, it becomes binding.
- E.g. operational standards — calculate ACE — formula is not in a requirement, but an attachment to a standard.

- It is during the implementation phase that we see big difference between approaches. If just securing systems, or facilities- limit the locale where we control access to computer rooms. Think if intent is to secure- both facilities and systems.
- Load study analysis as part of identifying critical asset list.
- 706 "guidelines"- white paper might serve as that? How to do things is a guideline. Do we write the guideline as a part of it? Who would do this? Not NERC staff. May need the standards, the implementation convention, guideline that talks about approaches. E.g. an attachment about what a high impact is.
- Prescriptive vs. non-prescriptive.
- Look at some existing standards- allowable method.
- Took "supporting functions" intent out of CIP 002 to not raise this? Can't audit an intent- intent can be in a white paper. Nature of guidelines — options

On the afternoon of day two the following flowchart was presented and discussed:



Jackie Collett presented a flow chart depicting their approach that included reference to Scott Mix's matrix.

SDT Member comments on the Strawman B 002 Flow Chart

- What is a cyber impact? Impact on the BES? Yes. Independent of impact on physical asset that it is controlling.
- Why bother generating list of cyber assets for low impact? Low represents some level of protection.
- The impact on that asset and impact on BES comes in through the use of the Mix matrix.

C. Strawman Proposals Alignment with Guiding Principles

At the end of the day the members agreed to complete a matrix that highlighted the degree of alignment of each strawman with the guiding principles developed by the SDT at its last meeting. The results were compiled overnight and were presented to launch the discussion on the second day.

The members suggested that the rankings supported the suggestion that the strawman approaches were generally in alignment with the principles and have more in common with each other.

SDT GUIDING PRINCIPLES	Strawman B – CIP-002 Lim et al.						Strawman A: CIP 002 Huff et al					
Alignment=	*Fully*	*Generally*	*Somewhat*	*Not*	*NA*	*Avg.*	*Fully*	*Generally*	*Somewhat*	*Not*	*NA*	*Avg.*
	4	*3*	*2*	*1*	*NA*	*Avg.*	*4*	*3*	*2*	*1*	*NA*	*Avg.*
1. Map CIPs to NIST 800-53 to help quantify and assess any gaps	**4**	**4**	**4**	**0**	**5**	**3.0**	**3**	**6**	**3**	**0**	**5**	**3.0**
2. Protection of communication devices outside the electronic security perimeters is out of scope.	**7**	**6**	**2**	**0**	**2**	**3.3**	**4**	**4**	**4**	**0**	**2**	**3.3**
3. Create non-prescriptive standards and employ a technical exception/ compensating measures documentation and guidance process to accommodate variations.	**2**	**9**	**0**	**0**	**3**	**3.2**	**0**	**8**	**6**	**0**	**3**	**2.6**
4. Strive to preserve existing security investments and build upon the existing CIP requirements.	**6**	**10**	**0**	**0**	**2**	**3.4**	**2**	**9**	**5**	**0**	**2**	**2.8**
5. Protect the integrity of data throughout its transit.	**4**	**4**	**5**	**1**	**3**	**2.8**	**4**	**5**	**4**	**1**	**3**	**2.9**
6. Consider the unique locational characteristics (e.g. substations, data centers, generation plant) and functional capabilities of the cyber assets to be protected in CIP requirements.	**4**	**8**	**0**	**0**	**0**	**3.3**	**7**	**6**	**3**	**1**	**0**	**3.1**
7. Use a consistent risk-based model to classify cyber assets (as critical/high impact, moderate impact, low impact) allowing for expansion of standards beyond "critical."	**7**	**7**	**2**	**1**	**0**	**3.2**	**7**	**6**	**3**	**1**	**0**	**3.1**
8. Consider the minimum security controls for high, moderate, low within NIST 800-53 to help model the CIP requirements for each level.	**6**	**6**	**1**	**1**	**3**	**3.2**	**4**	**7**	**3**	**0**	**3**	**3.1**

NOTE: The SDT acknowledges that currently an entity's cyber asset classification is subject to scrutiny by the compliance enforcement authority and applicable regulators. *(February 18, 2009)*

3–10 SDT Members Written Comments on Matrix Form:

- I like the Grid-based approach in principles 1-4. I believe the systems-based approach is the favored approach. I think the issue of starting point is key- i.e. what is it we are trying to protect.
- Principle #1- NIST is system-focused against mission, no asset based

- Principle #4 Both approaches end in a list of cyber assets

D. Strawman A & B Areas of Strengths and Commonalities

The facilitators asked members to offer elements of the strawman approaches they felt were strengths:

- Several liked critical asset identification of the Strawman B paper. Engineering. Electric and cyber system interrelated.
- Strawman B's identification of cyber assets touching BES. Deals with cherry picking today with cyber assets
- Strawman A's simplicity and definitions.

The facilitators offered the following straw common propositions drawn from day one's discussion on the two CIP 002 strawman approaches for the SDT's review and discussion:

1. The current CIP language is insufficient for the future.

~~1. The current CIP approach is not a sound basis going forward to protect cyber assets and BES reliability (as exhibited by the five issues identified by Jackie et al).~~

SDT Member comments and suggestions.

- Both groups agree but this statement is too negative
- We have a sound basis- need to improve upon. Started from ground zero. It was a starting point. Need to do better.
- Delete and substitute: "The current CIP language is insufficient for the future. "
- What is the starting point of the security standard? Focus on systems or facilities and systems?
- Do we need a different approach?
- Yes because the problem with current approach is inconsistent and non-uniform protection of cyber assets. Giving each responsible entity authority to devise various processes with no approval and oversight get to the crux of problem. Goal of standard should be to keep the lights on and protect the BES, not to maximize shareholder concern.
- Focus on closing the loop holes. Don't cut unnecessarily into innovation and flexibility.
- Have to look at and find agreement on the problems we are trying to solve so we can look at each option's ability to solve problems.

2. Ground the approach in the context of NERC's 6 elements of reliability adding cyber security to each.

SDT Member comments and suggestions

- This is not in Kevin's approach. Not documented.

- Probably need to add, “adding cyber security to each” at end of the statement.
- Protecting from cyber security attack might be the 7th element of reliability. Malicious compromise of an asset. Currently talk of “critical”- reliable enough to sustain a cyber attack. Thus need to address all electronic control devices- high medium low as to how
- Problem is not cyber attacks but configuration management.
- Knowledge of IT and info security is not widespread. Let’s ground this in problems we are facing.
- Who has a good inventory of what we each have and don’t have? Do we know what we are managing? Put emphasis here on “care and feeding”
- “Adequate level of reliability document”- cyber security not a 7th element of reliability. Adjunct to all other six elements. Cyber security so that… we can recover from contingency, etc.
- N-1 is a concept that can’t work in cyber security. What do you have to do for resiliency in the cyber world: confidentiality, integrity, availability. Probably not a 7th element.
- Address what is the minimum for reliable operations.
- Keep the goal in mind in terms of cyber- ensure reliable power withstand an attack. Believes should be a 7th element.
- “Support” – cyber security/ computing systems are integral. Primary critical- can’t run what we are doing without computers. Central to our thinking about the problem.
- What is the goal of standards? Mitigate the risk or deal with reliability in wake or presence of attack? Goal is to prevent, deflect or recover from the attack.
- Engineering vs. IT approaches. This was faced when the federal entities began dealing with NIST in 1998. They were mandated to protect both physical and cyber, interconnected network systems connected to physical infrastructures. Take digital world into account new threats grounded in engineering foundation. It takes both- CIO, engineering and CEO viewpoints to do the job and solve the problem.
- Smart grid discussions have identified 16 critical infrastructures
- What are we trying to protect? Where to focus our attention? On terror or hackers?
- Focus on impact to organization and assets/people mission when any of the triad is compromised. Don’t have good info on who we are trying to protect against. Get away from the vector causing the impact, focus instead on what to do to protect against impacts.
- Creating false divisions- IT won’t be doing the engineers’ jobs designing power system elements. Engineers need to understand IT principles.

- CIPS have done a good job opening eyes to engineers- they now appreciate IT security components. Build upon this—the CIPs that are good but need to get better. Even below 100KV is automating.
- CIP 002 is about classification- regardless of IT or engineering. Extend to IT systems or networks?
- Holistic approach to IT- many threats from inside network. Not focusing on who but on what and where.
- CIP has both engineering and IT portions. 3 layers of classification will be helpful to them. CIP 002 needs to do both. More of an engineering function.

3. Utilize the ~~NIST~~ graduated levels (high, moderate low, and "who cares") in the approach.
   SDT Member comments and suggestions
   - Is this in terms of controls?
   - We have lost FIPS 199 in that. Self-assessment of impact to mission.
   - Assessment of impact to mission.
   - JP: value of exploring categorization of critical assets. Covered in concept paper. Impact assessment- organizational or asset?
   - Need to add a "inconsequential" or "who cares" level, lower than low.
   - How many levels we need? 3 right approach. FIPS 199 is using 4.

4. Include systems, facilities and equipment *(build on the ~~CIPSE~~CIPCCIPC Working Group Draft Guidelines)*
   SDT Member comments and suggestions
   - Everyone needs to look at guideline before we can agree to "build on".
   - Focused on identifying critical assets- CIP 2 version 1. Would have to modify it for both approaches.

5. Provide for 3rd party oversight and accountability in approach

6. Address the external interfaces impacting on BES reliability
   SDT Member comments and suggestions
   - Is this addressed in Strawman A only? Strawman B team agrees with this and do reference in their concept paper.

7. Oversight is addressed

8. Build upon the NIST 800-53 suite of controls
   SDT Member comments and suggestions
   - Are there others that should be considered?
   - Drawing upon system identification by risk development working group.

- Configuration management: is the focus of CIP to address this or cyber security vulnerability? We weave these together without answering either.
- Should deal with both. Should identify separately.
- CM is a core element to what we have. Ground engineering approach in this cyber standard. What is original intent of CIP 002?
- Gaps- trying to close with CIP 002- clear path to capturing all system elements for evaluation to ensure protected at a minimal level.
- We have to get a grounding in our cyber security sector. Create a 7th element to help ensure
- One is a top down focusing on what you are trying to do, the other is bottom up. Is it best to spend resources on deciding which to protect or invest in the protection itself?
- Need to focus on differences. Look at the starting point for differences.
- Should we get away from where the vector comes in and instead look at whether there is an impact to my system?
- Strawman A focuses on control vs. addressing vulnerability.
- May not be an either/or. Create a merger between the 2.
- R1. 7 and .8 overlaps with Huff approach. Move to R4. Corollary to FIPS 199 process.
- Is there a place for R2 and 3?
- R4- merge the two. Look at 1.1. Merge the two together and discuss functional description of assets.
- Let's not talk about how. Let's focus on their function and effect on BPS. Nail this down. Then look at rest of standards. Good controls, effective, cover threats.
- Stay focused on what we should accomplish- good for cyber assets but ignore 1.1. We need to deal with these--are they in/out?
- Keep "critical assets" in there because of VSLs and compliance associated with these. Thinks merger suggestions are good.

E. Exploring the Merging of the Two Approaches- Merger Small Groups.

The facilitators suggested several discussion questions following the presentation and discussion of the strawman options including:

- What is the best place for the CIP 002 approach to start? From facilities? From Systems? From either? From both?
- What is the best approach to 3rd party oversight and accountability?
- What is the best approach to addressing external interfaces?

After some discussion, the SDT members agreed to break into two discussion groups on the morning of day two to discuss and focus on the possible merger of the approaches of the two

Strawman 002 concepts to Requirements 1 and 4. Following lunch, each group reported the results of their discussion and engaged in a full SDT discussion of the issues.

1. **Requirement #1 Small Group Report**
   (Participants: Gerry Freese, Kevin Perry, Sharon Edwards (scribe), Rich Kinas (reporter, moderator), John Lim, Jackie Collete, William Winter, David Revill and Scott Fixmer)

Rich Kinas presented to the full team a summary of the small group's discussion. The group reviewed how it would be possible to merge facilities vs. functional approach. They agreed that the starting point should be to identify the functions necessary for reliability of BES. There were questions as to whether that should be part of the standard. Some urged that there was a need to pre-define the functions. The group agreed that it would then be necessary to identify the systems or hardware used to perform those functions. It would then be necessary to incorporate the high, moderate, low threshold each into category.

SDT Member discussion comments

- Some look at systems approach vs. assets/hardware.
- Who identifies functions? It is not clear at this point would need to be addressed. It may be the SDT.
- Continue to land on fundamental differences- e.g. do we do a filter before systems assessment using BES components, or do we jump to cyber system and then roll into a component basis. May not matter that much which is the starting point. Important to get to appropriately identify systems so an entity could take either approach.
- Can we provide or point to a methodology?
- If go to a systems approach- Bill Winters might word smith an option
- Hardware-
- Define systems? Electrical vs. cyber systems.
- If "system" in R1 what is reason for R4?
- Function definition in R1 only. System to support function in R4. Keep at power stuff or functions level (e.g. AGC).
- Are reliability functions defined within reliability standards? Where is the right place to define these functions? Those requirements in operations horizon. Look for those in the High Violation risk factors?
- A control system- command and control function of controlling BES.
- Operator certification?
- Defined by other standards?
- A participant offered the following list of 9 functions for SCADA systems from their consulting work: 1. Core and Critical SCADA functions; 2. HMI & Information Network Equipment; 3. SCADA Master; Real-Time Communications Systems; 4. Data

Acquisition; 5. Automatic Generation Control; 6. Breaker Control; 7. Voltage Control; 8. State Estimation; and 9. Remote Configuration/Troubleshooting/Maintenance
- Concern about limiting to operations. Asset management. Configuration management, firm ware etc. inventory system
- SR: concept- look at already developed items to come up with a list. Look at the conceptual.
- From the R1 small group perspective: Thresholds are R3 and Cyber devices are R4.
- In the NERC Adequate Levels of Reliability document- all have standards associated with those functions.
- By using approved standards, do we have an asset list?

2. Requirement #4 Small Group Report

(Participants: Frank Kim, Phil Huff (scribe/presenter), Jeri Domingo Brewer, Scott Mix, John Varnell, Rob Antonishen, Jay Cribb, Mike Winters and Keith Stoffer

Phil Huff presented the small group's report offering the following summary points:

- The Small Group suggested taking "systems" references out of R1 and only include functions of BES in R1.
- R4 should identify the systems that support and perform the R1 functions
- Physical assets- stayed away from system categorization (R5)

3. SDT Discussion of Merging the Approaches

SDT Member Discussion Comments on Merging the Approaches

- Refreshing to see what the Strawman B did in R1- lets go forward.
- How do we identify functions? How many standards exist? About 120 standards with over 1000 Requirements. Is it realistic to point to them when defining the functions? Note, there are over 150 high risk factors.
- The OC/PC chairs- believe that the SDT is using the standards for something other than what they were designed for.
- Definition of adequate level of reliability by FERC- scope of the functions we are talking about. Characteristics.
- Concerned about ambiguity- of standard. Draft 2 of standards had numbers in it.
- Should we dictate assessment methodology in the standard?
- Standard says what- with parameters. "How" is placed elsewhere.
- Specificity has a place in certain standards. How to shed vs. when to shed.
- SDT must figure out where the specificity belongs keeping in mind that a standard is a "what" not a how. Guidelines are generally the place to lay out the "hows."
- Keep in mind we are now in the ERO era.
- Float as a white paper vs. a list of requirements?
- Adequate level of reliability paper-was it balloted?

- Will it be possible through a onetime process, to identify the functions that support the reliability of the electric system? This needs to be done. Perhaps it can be defined in standard and referred to as an appendix.
- Defining the criteria for high, mod, low, inconsequential, should be taken out of industry hands on a case by case basis and put in the standard. If REs make up their own rules, we will still have problems with consistency and uniformity of application of standards.
- The steps are: identify assets; map against functions; map against potential impact (criteria); and come up with a list of what protected to what degree.
- Don't need to define these functions- don't reiterate existing reliability standards. Cherry pick the key functions. Black and white filter may be needed here. Would simplify for end users and cut down on interpretation.
- Don't lose sight of the consensus reached in having the functions in R1, the systems in R4.
- Address the functional aspects of BES in R1. Recognize it is good to separate functional objectives of BES from systems and assets that support use.
- There is disagreement over whether the functions are defined in R1. They need to get defined as onetime process external to entities using them and then reference in standards.

F. CIP-002 Requirements 2 and 3 Critical Asset Identification Methodology (R2) and Identification (R3) Strawman

Scott Mix presented a strawman for an approach to CIP 002 Requirements 2 and 3 for consideration by the SDT. He suggested starting with functions and map to the physical equipment. Consider determining "Asset Impact" as high, moderate, low and none and "Cyber impact" as high, moderate, low and none for CIP 3-9.

Asset Impact -->	High	Medium	Low	None
Cyber Impact:				
High	5	4	3	1
Medium	4	3	2	1
Low	3	2	1	0
None	2	1	0	0

SDT Member comments on the strawman R2 and R3 matrix

- What about load shed for economic reasons? Conceptual level
- Have to come under standards since the risk is there and need to mitigate.
- The pre-supposes a lot. Look at asset based on function and rate. Take a more systems approach tied to function. When you do categorization, look at the threat vectors.
- Very ineffective security controls may result in undermining the intent of the standard.

- **Asset based impact —** likes approach. Availability- how would loss of asset affect BES? How would misuse of system affect?
- If you look at asset before this is done, it may lead to mistakes. Take information and fold into the categorization effort.
- Shouldn't include/exclude systems with a filter/matrix.
- This will cover more systems than are covered now under the CIP.
- Developing standards guiding production systems.
- If required to have zone protections. Shouldn't design standards to accommodate
- **Remapping from function to asset —** Keep this at the function impact. You may be opening this up for avoidance behavior.
- Redundant protection is tied to the adequate level of reliability
- We haven't talked yet about oversight and wide-area view component
- Asset and function may combine — Modify- level of effort to compromise device? vs. cyber impact. Impact divided by effort? Ratio- high risk of impact, little effort to compromise. Threshold of value to provide additional protection.
- Is there a potential for "gamesmanship"? Internal actor, external actor, etc.
- Start with the function — can't secure AGC, secure computer that calculates. Need to get to functional level.
- Just do cyber impact with criteria- may not have to go through asset impact drill.
- Framework is a good thing. If you do categorization impact- after identify functions.
- **Defining thresholds —** Need to make sure we don't start putting numbers to thresholds. They may increase and then you will have to revisit to deal with the changes needed.
- Is getting down to the BES element device necessary? Keep focus on system level.
- Not excluding assets, including the system.
- "Contingency reserve"
- Added impacts into asset classification R.2.3 (get from Joe/Scott)
- Helps with appropriate levels for controls
- Relate to specific standards to give people a sense of this. Create an attachment. Binding explanation of what "significant" means.
- Put as an attachment vs. a glossary.
- Categorization?
- "Support the reliable operation of the BES". Need to clarify this.
- E.g. insignificant devise?
- What is the correlation between R2 and R3 and cyber assets in R4? Connection between R4 and R1. Moved under R4. Come into play then? Cyber approach
- R1 and R2- are generally focused on electric R4 and R5 focus on cyber.
- Each requirement by itself a simple requirement to meet.
- Break line between R3 and R4? Do both. Proposing to maintain the hierarchical order?
- Anticipating "controls"

- Are these exclusive. Do we need R2 and 3 any more? Can't apply a control to a function.
- Control framework- requirements 003-009. NIST calls security controls. NERC
- Hierarchal ranking of assets-
- Look at functions, correlate to cyber systems, apply controls 003-009
- Without an engineering review of impact- R2.3 do it as overt operation that can be audited.
- Put in the relevant detail. Don't do before you know what cyber assets perform what functions.
- R2 and R3 are top down. Does each requirement stand alone? Each is building as a filter or additive. If leave out 2 and 3, then you can't build later the matrix.
- This may allow RE pick and choose and make up own rules? If we can define the threshold criteria identification importance. If you want RE to do, then leave 2 and 3 in. Determine in an appropriate manner.
- R 2.3 process. IROL caused by cyber asset? If remove R2.3- won't
- Pre suppose cyber assets everywhere.
- R1 now. Most are systems. R2 and R3 is part of categorization process. Need engineering criteria in R5.
- Use matrix approach — complex- 16 cells. Meld to high medium low or none.
- Options include: 1. Keep R2 and R3; 2. Keep with SM's language; 3.Move
- Need to clarify what "cyber impact" means. Cyber impact on a particular asset? Include going forward- components of connectivity, impact of cyber system on asset/function.
- Supports a 2 dimensional matrix.
- R2 and R3 — captured in the external engineering studies on Strawman A flow chart. Not a requirement in this because it would be done externally. R2 and R3 performed external to the entity process.
- Impact assessments: need to keep separate? Performing 1 impact analysis.
- Haven't had good results in getting new methodology out to the industry quickly. Will any of these be better than what we have today? Looking for more consistent answers from each utility.
- Similar enough to be the same flow chart. Are they the same flow if you move that one box?
- Is there agreement with moving the arrow will result in no 2 dimensional matrix? Cyber impacts may have not bearing on the functions.
- Cyber impact assessments — consider impact on physical assets of BES due to impacts of a cyber asset?
- Breaker control relay- cyber asset impacts the breaker associated with.
- What is a cyber impact? Impact on the BES. Independent of impact on physical asset that it is controlling? Why bother generating list of cyber assets for low impact? Low but some level of protection.
- Impact on that asset and impact on BES comes in through the matrix.

- We are looking at this from bottom up and top down.
- Left side of flow chart covers the impacts and consequences. Right side- cyber impacts as a vulnerability assessment. What kind of connectivity does it have etc. Sounds like 2 pieces of a risk score. Take the controls and apply to.
- Cyber impact is the impact to the operation of the specific asset using vector of protected system- does it cause the engineering asset to misbehave.
- We are struggling with a difference in terminology. Cyber impact on the Strawman B chart is blind to the broader system. Impacts on the Strawman A chart take holistic view of the system.
- Is the difference a vulnerability vs impact assessment?
- What happens with malicious behavior?
- Part of cyber assessment — assess use of un-authenticated relay.
- Interpretation of cyber impacts — what is the reach of cyber assets- how many units can it kill. How bad can it make things from its viewpoint?
- Should we make a decision based on that impact-
- Common mode impact from the guideline and put in standard to be become binding?
- Cyber impacts- how they impact the BES.
- Vulnerability assessment to R5-

The facilitators suggested polling on three proposals for going forward that emerged from the discussions:

Proposal 1 Keep R2 + R3 with Scott's Language (Matrix)
Proposal 2 Move R2 & R3 into R5 (Vector Analysis)
Proposal 3 R2 + R3 Performed by External Entity

1. **Proposal #1: Keep R2 + R3 with Scott's Language (Matrix)**

Acceptability Ranking Scale	*4 = acceptable, I agree*	*3 = acceptable, I agree with minor reservations*	*2 = not acceptable unless major reservations addressed*	*1 = not acceptable*	*Avg.*
Proposal 1- R 2& R3	**6**	**5**	**6** (5/1)	**1**	**2.9 of 4**

Comments after ranking:

- #1s: This is not right framework- misplaced. Concept of keeping R2 and R3. Placement is a big deal
- #2s: not convinced complexity of 2 way matrixes is necessary.
- #2s splitting the assessments — what physical are you looking at? Cyber impact doesn't have meaning within methodology.
- #2s Not seeing the meaning of the cyber impact assessment

- #2sTaking us as group we are not on the same page- we will have difficulty pushing concept to industry.
- #2sWhat if we split this into 2 analyses. May be a lot of work that may not matter in the long run. Better to have in 1 integrated process. Bring all into 1 assessment process.

SDT Comments

- Important to be clear about ultimate requirements that we write.
- Cyber impact- left hand side- what happens if BES asset is compromised, goes away.
- Right hand column- cyber impact- what bad things could be done with device if it were compromised on the target of evaluation.
- Next version of standards- keeping R2 and R3 asset ranking is necessary. Applying more gradations vs. roll into big process with cyber impact. Industry might prefer to keep 2 & 3.
- Didn't vote- didn't get any sense of a system- in this.
- Is the process based on theory? Why you can't take last arrow and connect to impact- not mapping functionally? What is the cyber assessment. Other flow chart- engineering studies.
- Ranking based on reality-
- Risk vs. impact analysis- e.g. vulnerabilities.
- Are we ever going to bring in vulnerability?—yes, when we get to 003-009 for the control selection phase but we have to determine how many and how tough need to be.
- Analogy- FIPS 199- before categorize, incorporate risk assessment and existing plan and previous assessment. Impacts how you rate the system. Impact has no meaning if you don't have risk appetite. Audited for insufficient risk assessment before categorize system- and picking controls.

2. Move R2 and R3 to R5 for a single vector analysis- concept

Acceptability Ranking Scale	*4 = acceptable, I agree*	*3 = acceptable, I agree with minor reservations*	*2 = not acceptable unless major reservations addressed*	*1 = not acceptable*	*Avg.*
Proposal 2- R 2& R3	**4** (3/1)	**5**	**9** (8/1)	**0**	**2.7 of 4**

Member comments after ranking

- 2's: value in evaluating BES independently of the cyber assets. May be easier for industry to get head around. May help with other standards.

3. Have R2 and R3 Performed by External Entity

Acceptability Ranking Scale	*4 = acceptable, I*	*3 = acceptable, I agree with minor*	*2 = not acceptable unless major reservations*	*1 = not acceptable*	*Avg.*

	agree	*reservations*	*addressed*		
Proposal 2- R 2& R3	**1**	**0**	**9**	**5**	**1.8 of 4**

G. Developing A Common Framework

At the end of the second day, a small group agreed to work further on a draft common framework. The group included Phil Huff, John Lim, Scott Mix, Jackie Collett, Scott Rosenberg and John Varnell. Jackie Collett introduced a flow chart as a strawman designed to be flexible to allow for further development and refinements. She understands that it will be important to clear up terminology so references are understood. Phil Huff offered that this concept captures the focus on cyber systems (not on assets) and does not offer a hierarchal model. The "vector" categorization- matrix offers some more granularity as to what we are meaning to accomplish. It offers a cyber impact analysis of impacts on the function. Still performing the same transitive impact analysis that is logically equivalent.

Concept

Identification of BES functions which support the reliability and operability of the BES

Need 1 layer of specificity below ALR

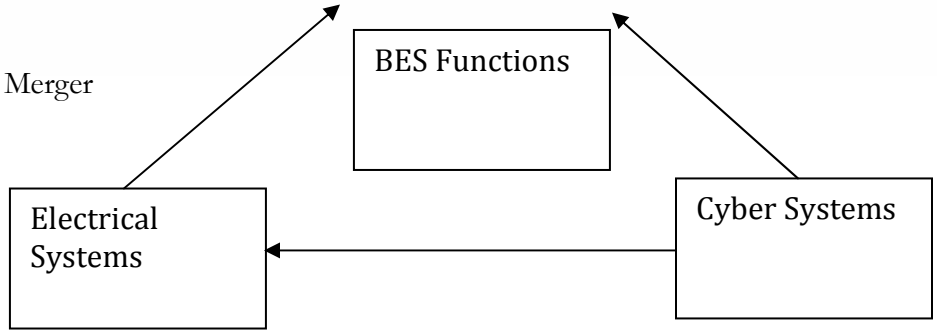
Cyber Impact — the local impact due to loss of CIA of the cyber asset for a BES element

System — a set of components which must work together

Electric System — a set of BES elements which must work together

Cyber System — a set of cyber components which must work together

Pre-Determined Functions			
R1	List of Electric Systems which support the BES functions	R4	List of Cyber Systems which support the Electric Systems and/or BES Functions
R2	Method of Categorization - impact to BES	R5	Method of Categorization - local impact to Electric System components
R3	List of Systems & Categories	R6	List of Systems & Categories
R7	Matrix: combines the 2 impact levels		
R8	Local Approval		
R9	Oversight		



Member comments on the Concept

- Is the definition of a cyber incident being only local? Does this suggest any difference of between cyber and electric.
- Haven't yet defined criteria. Connectivity on the cyber side might fit. They don't map well together. Cyber asset impact side put something in on connectivity.
- SM: formative stages. Focusing on local BES impact from a cyber stand point. Open to addressing network interconnectivity. Detail to be fleshed out later.
- Clarification- which bucket would a sweitzer 100 series relays (with a micro processor) fall in? What would industry think. Clarify what is a cyber asset. Helpful to have a one page on the guiding principles for the CIP effort.
- Network connectivity — weigh in on the cyber impact analysis
- Right side- call "control system" vs. "cyber system"? Direction can provide clarity. However, puts you in the weeds quickly.
- What is the object of the requirements?
- Terms should be fairly self explanatory. Not only systems that control, but also coordinate, alarm, situation awareness.
- Terminology- from different niches- "cyber" system is problematic. Move away from it.
- Go to control systems- nested definition sequence. Look at those definitions from Strawman A.
- Decouple- like the fact there is no discriminating filter. Solves that problem. Not convinced 2 matrixes. Willing to see how progresses. Key point in Huff approach-
- Detail didn't get to last night. There will be an oversight component. Difficult for 2 entities to talk with each other.
- Get captured in the pre determined function list that is built- e.g. exchange of data could be a function unto itself.
- System selections identified. Is intent to end with a list of systems that we've established an impact level of? Then identify elements you have to apply to? Put into additional CIP requirements.

- Don't part the sheep's from goats, blanket that covers everything but focuses attention are areas for greatest impact. May take 10-15 year timeframe to get there. There is a pile of assets we should worry about fixing in 2 years. Next level- have 5 years to do something with applying a lesser set of controls to a broader family of systems; another layer taking 10 years to get all of those done. At end, broad scope of coverage.
- How big a blanket? No agreement yet. However, more protection that what is currently implemented today.
- Identify an implementation time frame that would be reasonable to the industry.
- Use definitions- Alphabet soup draft- Cyber asset, system control systems.
- Any device that is programmable is in scope.
- Careful about using terms, mixing them up. Makes it confusing. Need come up with terms we agree on.
- Terminology-- careful we don't reuse terms- e.g. critical asset. Inventing new terms and using consistently. Do this sooner vs. later. NERC glossary — e.g. element.
- Note that this is a work in progress.
- Drafting team glossary before the next meeting. Beneficial.
- R1-3 pieces as planning type elements. R4-6 micro processor. Don't mix initially. Then combine.
- Other advantage — FERC 706 order — oversight is on the electrical side not on the cyber side. That's where there is oversight authority related to BES.
- "Big Iron" piece.
- Appreciation for this work. This concept is a benefit to entire effort. CIP standards are incomplete. Physical side needs to be developed. Leaves in that side that will address the physical side for the next SAR. I Like this.
- R1 and R4- how to scope down so not lists of 10 million? Will be scoped down on the identification of BES functions. "Generation control"
- Functions will be "pre determined" by the SDT.

Following the discussion the SDT agreed to rank the acceptability of the following proposition:

Adopt as a working conceptual model for SDT to develop frame and concept paper that includes a set of definitions/glossary, Develops a list of functions and uses list of scenarios to test the concept.

Acceptability Ranking Scale	*4 = acceptable, I agree*	*3 = acceptable, I agree with minor reservations*	*2 = not acceptable unless major reservations addressed*	*1 = not acceptable*	*Avg.*
3-12 SDT rank	**15**	**3** *(1/2)*	**1**	**1**	**3.6 of 4**
Second Rank with D Norton's Concept	**15**	**3**	**2**	**0**	**3.65 of 4**

Comments after the ranking

- Dave Norton ranked this with a 1 and explained it by presented a flow chart he had been working on *(See Appendix #9)* that was titled "Scoping Logic Synthesis Proposal"
- Rich Kinas gave it a 2 indicated his preference would be to create and compare a range of multiple competing approaches before settling on a framework for Phase 2.
- Voted 3: those working with both federal and NERC compliance at same time may find it hard to look at reliability from a cyber perspective- need to put in context. Hard for understanding each other. Federal experience suggests we will have a hard time with this.
- If on the cyber side we do a good job = functional description of systems and how relate to functions of BES.
- Good controls on cyber system to minimize risk. Demonstrate positive impact on BES. Setting stage for better dialogue with the industry.
- Could make it worse than now but on balance this is a good positive step.
- Voted 3- Shared Rich's view point. Taken aback- on the complexity of matrix approach. Left hand side- look to planners how are these falling out. Cyber side is right hand side is what is depicted. Complexity is an issue. Perception that standards are unnecessarily complex and wastes time. The more direct we make this the better.
- We can incorporate Dave Norton's ideas into this model. E.g. system restoration? Right hand or left side? Functions.
- There are lots of options but we should do something with this and see if it makes sense, see how this actually work in practice.
- DN ideas might fit in R4-6. Add this in.
- Standards should help provide everything in BES needs to be protected at some level.
- Engage in DN's next about how left and right side map.
- Voted 4 because it is a concept. DN's proposal is CIP 002 supported by concept paper. Where the criteria gets set is key. If criteria for categorizing set externally to RE, then single column can work and simplify the process.
- If RE's continue to make own rules, will strive to make low or none and it is hard
- R 1-3 what is the product of that? BES inventory run. Categorizing now with N-1, list will be automatically high. Leads to maximum controls. R3 is the documentation.

In the discussion of the approach going forward concern was expressed about whether the SDT was the right group to develop the concepts for Requirements 1,2, and 3 (the left hand side). Planning and operations perspectives would be helpful. The current SDT is 90% cyber folks. Dave Taylor volunteered and the SDT agreed that he should draft a white paper to present to the next meeting on a process for determining Requirements 1, 2 and 3.

Bill Winters requested the SDT rank the following proposition that if acceptable would be incorporated into the white paper going forward as the CIP 002 intent statement:

CIP 002 is intended to provide a discovery methodology that will lead to explicit identification and categorization of all cyber elements that <u>performs or supports</u> BES functions.

Acceptability Ranking Scale	*4 = acceptable, I agree*	*3 = acceptable, I agree with minor reservations*	*2 = not acceptable unless major reservations addressed*	*1 = not acceptable*	*Avg.*
3-12 SDT rank	**18** (16/2)	**1**	**0**	**0**	**3.9 of 4**

VI. NEXT STEPS and Assignments

A. Drafting Assignments

The SDT agreed that a helpful next step would be to refine the concept presented and tested on the third day in the form of a draft white paper. The chair asked Jackie Collett, John Lim, Bill Winters and Phil Huff along with Scott Mix to take the lead in the development of the draft white paper in advance of the April meeting building on the discussion and outcomes of this meeting. Other members would be welcome to send ideas and reactions as well as listen in and participate on the webex meetings that would be convened. The goal would be to be able to share the white paper with the industry following either the May, 2009 or June, 2009 meeting.

B. SDT Meetings Schedule, 2009

The SDT members completed calendar forms regarding possible dates for future SDT meetings. Upon review of the forms and SDT member scheduling conflicts, the following dates and tentative locations were established and agreed to by the team.

Proposed Dates and Locations for Future Meetings 2009

Dates in 2009	Location
April 14–16	Charlotte, NC
May 13–14	Boulder City, NV
June 17–18	Portland, OR
July 13–14	Toronto, CA
August 20–21	Chicago, IL
September 9–10	Denver, CO
October 20–22	New Orleans, LA
November 17–18	Atlanta, GA
December 15–17	Key West or FRCC (Tampa, FL)

The SDT agreed to seek to make a progress report to the MRC at its May meeting in Arlington, Virginia and provide a substantive briefing on the Phase II white paper for input at their August meeting.

The team discussed the timing and objectives for a workshop. Some members suggested it could be an opportunity to brief on the Phase II approach and receive input from experts from other standards bodies as well as FERC and Congressional members and staff. The chair noted that the NERC standards committee had carefully selected subject matter experts to serve as members.

The SDT decided to hold open the question of convening an expert/stakeholder workshop pending the Chair and Vice Chair's discussion with Michael Assante, NERC Chief Security

Officer, to gain a clearer understanding of the potential objectives, design and timing of a workshop in light of the SDT's progress and schedule.

C. Meeting and SDT Process Evaluation
The facilitators offered some observations on the SDT's team work over the past six months including:

- The SDT 706 team is larger that many SDTs
- The issues under review are complex and contentious technical and operational issues
- Contentious
- The members are highly knowledgeable and articulate with strong opinions.
- There has been measurable progress in proceeding on a two phase approach to their work.
- There has been a helpful sharing among the team members on what has been working and constructive suggestions on what could be improved.
- The facilitators should help to clarify within meetings the objectives sought for each session and check on the chair's, vice chair's and the team's sense of whether they have been met before transitioning to other sessions.
- The team members often in the context of reviewing and debating key issues will use experiences to illustrate points or test proposition which takes time and in some instances may not advance the discussion.
- The team and facilitators have been sensitive to the "violent agreement" rule but may need to manage that more assertively so that members know that it is being captured in the record and there may not be a need to repeat.

The facilitators suggested and the Chair and team agreed that it would be timely to survey the Team on the experience over the past six months to provide an opportunity for deeper shared reflections on the ways to improve the team's process.

The SDT adjourned at 11:45 a.m. on March 12.

Appendix 2 — Meeting Attendee List

Attending in Person — SDT Members

1. Rob Antonishen	Ontario Power Generation
2 Jeri Domingo-Brewer, Chair	**U.S. Bureau of Reclamation**
3. Jackie Collett	Manitoba Hydro
4. Jay S. Cribb	Information Security Analyst, Southern Company Services, Inc.
5. Sharon Edwards	Duke Energy
6. Scott Fixmer	Senior Security Analyst Exelon Corporate Security, Exelon Corp.
7. Gerald S. Freese	Director, Enterprise Information Security America Electric Power
8. Phillip Huff	Arkansas Electric Coop Corporation
9. John Lim	CISSP, Department Manager, Consolidated Edison Co. NY
10. Frank Kim	Ontario Hydro
11. Richard Kinas	Orlando Utilities Commission
12. David Norton	Policy Consultant, CIP Energy Corporation
13. **Kevin B. Perry, Vice Ch.**	Director, IT-Infrastructure, Southwest Power Pool
14. David S. Revill	Georgia Transmission Corporation
15. Scott Rosenberger	Luminant Energy
16.Keith Stouffer	National Institute of Standards & Technology
17. John D. Varnell	Technology Director, Tenaska Power Services Co.
18.Michael Winters	Ontario Hydro
19.William Winters	Arizona Public Service, Inc.
1. Roger Lampilla	*NERC*
2. David Taylor	*NERC*
3. Scott R. Mix	*NERC*
4. Joe Bucciero	*NERC/Bucciero Assoc.*
6. Robert Jones	*FSU/FCRC Consensus Center*
7. Stuart Langton	*FSU/FCRC Consensus Center*
Hal Beardall	*FSU/FCRC Consensus Center*

SDT Members Attending via WebEx and Phone

20. Tom Hoffstetter	Midwest ISO, Inc
21. Kevin Sherlin	Sacramento Municipal Utility District
22. Jonathan Stanford	Bonneville Power Administration

SDT Members Unable to Attend

1. Joe Doetzl	Manager, Information Security, Kansas City Power & Light Co.
2. Christopher A. Peters	ICF International

Others Attending in Person

Jim Breton	ERCOT
Roger Fradenburgh	Netsecctech
Judy Fry	ICFI
Darren Highfill	ENERNEX

Sam Morrell	CERT
Farzaneh Tafreshi	ICFI

Others Attending via WebEx and Phone

Chris Wright	
Dan Mishra	
David Batz	
Monica Coflin	
Karen Yoder	

Appendix 4 — Michael Winters Note to SDT

From: **WINTERS Michael**

To: **'CS_706_SDT@NERC.COM' <CS_706_SDT@NERC.COM>**

Sent: **Thu Mar 12 07:27:27 2009**

Subject: **All the best Fellow SDTers –**

I had to leave prior to us finishing up yesterday so I didn't get a chance to say goodbye.

It has been a pleasure working with each of you and being a part of this very important team. It goes without saying that these standards are much needed in our industry and the direction you are taking them is a good one. They have already served to introduce good information technology practices into power system engineering. These practices need to be applied at different degrees to all cyber assets used for power system operations (or at least allow for an explicit and auditable decision to not apply them to some assets).

I have learned a significant amount as part of this team and for that I thank you. I look forward to seeing where you take us.

All the best, Mike

Appendix 5

Cyber Security Order 706 SDT — Project 2008-06
January through June 2009 Draft Schedule

Short Term 2009 SDT Schedule Draft Criteria

- Follow the ANSI standard development process but use creative ways to efficiently secure input from the industry on emerging concepts and approaches to the CIP standards.
- Seek creative ways to get advice and input to the SDT from experts in cyber security.
- Seek creative ways to get focused input from industry stakeholders.
- Take advantage of input opportunities from related NERC committees that will be meeting in the first half of 2009 (e.g. working with the NERC Members Representative Committee, CIPC, BOT, and industry committees such as the Electricity Sector Coordinating Council, etc.)
- Seek, as soon as possible but no later than late Spring, 2009, to establish a consensus on the way forward for the SDT in its efforts to revise the CIP standards.
- Track any follow up to the "Securing Cyberspace for the 44th Presidency" report of the Commission on Cyber security for the 44th President.

SDT Draft Schedule — January through June 2009

OVERVIEW

- 7 SDT Face-to-Face Meetings
- Multiple SDT subgroup and subcommittees WebEx Meetings
- 1 Cyber Expert Workshop (March 10 or 11, 2009)
- 1 NERC CIPC presentation? (February 9, 2009)
- Industry Comments on CIP-002 White Paper (April 17 through June 3)
- 1 NERC Members Representative Committee, May 1, 2009
- Other Meetings?

1. **January 7–9, 2009 Meeting in Phoenix, AZ —** half, full, half day format **—** Wednesday through Friday
   - Review of Technical Feasibility Exceptions white paper
   - Review of Industry Comments on Phase 1 products- Establish and convene small groups
   - Review of Phase 2 White papers

January 15 WebEx meeting(s)

- Small group draft responses to industry.

- Phase 2 drafting concept group?

January 21 WebEx meeting(s)
- Small group draft responses to industry.
- Phase 2 drafting concept group?

2. **February 2–4, 2009 Meeting in Phoenix, AZ — half, full, half day format — Monday through Wednesday**
   - Review of Industry Comments on Phase 1 products and proposed revisions and adoption of Phase 1 products.
   - Review of Phase 2 White papers and Testing of a Phase 2 CIP-002 Concept going forward

February 9, 200 — CIPC Meeting — Update on SDT Progress and Input

3. **February 18–19, 2009 Meeting in Boulder City, NV**
   - Review of Phase 2 White papers and Adoption of a Phase 2 CIP-002 Concept for review by experts and stakeholders

February 25 WebEx meeting(s)
- Development of Phase 2 CIP 002 Workshop for review by experts and stakeholders

4. **March 10–11, 2009 Meeting in Tampa, FL, 2-day format**
   - **Invited Cyber Security Experts join SDT in a workshop** to provide expert feedback to draft CIP-002 concept.
   - Further SDT refinement of the CIP-002 proposed concept

March NERC Balloting on Phase 1 Products

March 18, Webex meeting(s)
- Phase 2 drafting concept group?

5. **April 14–16, 2009 Meeting in Charlotte NC — half, full, half day format — Wednesday through Friday**
   - Continue review and refinement of CIP-002 concept
   - Adopt White Paper on CIP-002 concept for Industry Comment

Industry Comment Period on White Paper — 45-days (April 17 through June 3)

*May 1, **NERC Member Representative Committee**, Presentation of the Phase 2 CIP-002 Approach for MRC input. (Agenda item, Possible Workshop?)*

6. May 13–14, 2009 Meeting in Dallas TX — 2-day format

- Respond to MRC input and further SDT refinement of the CIP-002 proposed concept and SDT CIP roadmap.
- Organize SDT in subcommittees to draft revisions to CIP-003-CIP-008 or to address key issue areas.

Early June WebEx meeting(s)

- SDT subcommittee meetings to review and draft responses to Industry comments on the CIP-002 concept.

7. June 17–18, 2009 Meeting — Location TBD — 2-day format

- Review Subcommittee responses to Industry comments on CIP-002 approach
- Charge subcommittees and conduct organizational meetings
- Subcommittees meet to draft revisions to CIP-003-CIP-008

June, 2009 WebEx meeting

- SDT Subcommittee meetings

July–December, 2009 — SDT and subcommittees meet and continue CIP drafting

Second Draft Phase 2 Roadmap Approach Assessment Criteria
(Presented, Revised and Added to by SDT in its review on November 14, 2008)

1. The approach is consistent with the SDT purpose statement and is responsive to the FERC 706 directives and the SAR.
2. The approach is achievable given the SDT schedule and work plan.
3. The approach does most to advance and enhance cyber security in the BES.
4. The approach helps the SDT address the foundational issues with the current standards.
5. The approach is capable of implementation.
6. The approach is capable of improving compliance.
7. The approach helps protect the current investments and wherever possible builds on what has already been done.
8. The approach helps to identify and mitigate risk on an ongoing basis.
9. The approach balances a “systems” orientation with a “facilities” orientation to asset protection.
10. The approach is capable of being extended into related interests by others (distribution, AMI, Smart Grid, etc.).

11. The approach enables the industry to provide the appropriate level of security (i.e. not over securing nor under securing the BES cyber assets).
12. The approach allows for discrimination among and targeting the various types of infrastructure that support the BES

Appendix 6 — CIP-002 Strawman A

(Phil Huff, Jeri Domingo Brewer, Kevin Perry, Keith Stoffer, and Bill Winters)

Definitions:

Cyber Asset — Programmable electronic devices and communication networks including hardware, software, and data. [NERC Glossary]

Cyber System — A discrete set of Cyber Assets organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. [Adapted from NIST SP 800-53 definition of Information Systems]

Control Systems — computer-based facilities, Cyber Systems, and equipment used to remotely monitor and control sensitive processes and physical functions. These systems collect sensor measurements and operational data from the field, process and display this information, then relay control commands to local or remote equipment. [Joint DOE/DHS Roadmap to Secure Control Systems in the Energy Sector – January 2006]

B. Requirements

R1. The Responsible Entity shall produce through an annually applied process, a list of Cyber Systems that are to be protected per the requirements of the CIP standards. The Responsible Entity shall at least annually:

R1.1. Identify all Control Systems that perform supervisory control functions (e.g. open/close breakers, raise/lower generation) for the Bulk Electric System or provide situational awareness of the state of the Bulk Electric System. This would include:

- Systems that provide situational awareness
- Systems performing EMS/SCADA functions
- Special Protection systems
- Systems essential to BES restoration
- Systems performing automatic load shedding
- Other systems that may perform a function directly related to BES system reliability

R1.2. Identify internal and external data interconnections between Cyber Systems that provide data necessary for the reliability functions of the previously identified Cyber Systems or Control Systems.

R2. The Responsible Entity shall define one or more security boundaries to encompass the identified Cyber Systems.

R3. The Responsible Entity shall review, update as necessary, and obtain Regional approval of its Cyber System categorization criteria at least once every three years.

R4. The Responsible Entity shall annually categorize each identified Cyber System as low, moderate, or high potential impact to the Bulk Electric System using Regionally-approved categorization criteria. The categorized list shall reflect the importance of integrity, availability, and confidentiality the Cyber System or data and the potential risk to the reliability of the Bulk Electric System in the event the Cyber System is lost or compromised.

R5. The Responsible Entity shall evaluate and categorize new and replacement Cyber Systems using the applied process and categorization criteria prior to being placed into service.

R6. The Responsible Entity shall designate a senior manager with the responsibility and authority to approve the categorized list of Cyber Systems.

R7. The Responsible Entity shall communicate and coordinate with the external Responsible Entity any identified external data interconnections between Cyber Systems and the potential impact to the reliability functions of the Responsible Entity.

Appendix 7 — CIP-002 Strawman B
(John Lim, Jackie Collett, Scott Rosenberger, and John Varnell)

Introduction

Title: Cyber Security — Cyber Asset Identification and Categorization

Number: CIP-002-3

Purpose: NERC Standards CIP-002-3 through CIP-009-3 provide a cyber security framework for the identification, categorization and protection of Cyber Assets to support the reliable operation of the Bulk Electric System.

These standards recognize the differing roles of each entity in the operation of the Bulk Electric System, the criticality and vulnerability of the assets needed to manage Bulk Electric System reliability, and the risks to which they are exposed.

Business and operational demands for managing and maintaining a reliable Bulk Electric System increasingly rely on Cyber Assets supporting critical reliability functions and processes to communicate with each other, across functions and organizations, for services and data. This results in increased risks to these Cyber Assets.

Standard CIP-002-3 requires the identification, categorization and documentation of the Cyber Assets associated with the Assets that support the reliable operation of the Bulk Electric System. These Assets are to be identified and categorized as Critical and non-Critical based on the application of an impact assessment.

Applicability:

Within the text of Standard CIP-002-2, "Responsible Entity" shall mean:

Reliability Coordinator.
Balancing Authority.
Interchange Authority.
Transmission Service Provider.
Transmission Owner.
Transmission Operator.
Generator Owner.
Generator Operator.
Load Serving Entity.
NERC.
Regional Entity.

The following are exempt from Standard CIP-002-2:

Facilities regulated by the U.S. Nuclear Regulatory Commission or the Canadian Nuclear Safety Commission.
Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

Effective Date:

The first day of the third calendar quarter after applicable regulatory approvals have been received (or the Reliability Standard otherwise becomes effective the first day of the third calendar quarter after BOT adoption in those jurisdictions where regulatory approval is not required)

Requirements

R.1 Identification of BES Assets – The Responsible Entity shall identify and document a complete list of BES Assets. Assets may be identified as facilities, equipment or systems. The Responsible Entity shall include, wherever applicable, the following:

Control centers and backup control centers performing the functions of the entities listed in the Applicability section of this standard.

Transmission substations that support the reliable operation of the Bulk Electric System

Generation resources that support the reliable operation of the Bulk Electric System.

Systems and facilities used for system restoration, including blackstart generators and substations in the electrical path of transmission lines used for initial system restoration.

Systems and facilities critical to automatic load shedding under a common control system capable of shedding 300 MW or more

Special Protection Systems that support the reliable operation of the Bulk Electric System.

Systems that support wide-area reliability through one or more of the following:

Situational awareness
Supervisory and control capability
Other systems that may perform a function directly related to the reliability or operability of the BES.

Any additional assets that support the reliable operation of the Bulk Electric System that the Responsible Entity deems appropriate to include in its assessment.

Critical Asset Identification Method — The Responsible Entity shall identify and document an impact assessment methodology to use to identify its Critical Assets.

(Note: This requirement assumes that the NERC guideline will provide more specific guidance in the development of the methodology. As suggested by Scott Mix, a change in terminology may reflect more accurately the nature of this methodology.)

The Responsible Entity shall maintain documentation describing its impact assessment methodology that includes procedures and evaluation criteria. The evaluation shall include consideration for Common Mode Impact and Adequate Level of Reliability.
The impact assessment shall be applied to the BES Assets identified in R1.

Critical Asset Identification — The Responsible Entity shall develop a list of its identified Critical Assets determined through an annual application of the impact assessment methodology required in R2. The Responsible Entity shall review this list at least annually, and update it as necessary.

Cyber Asset Identification — Using the list of Assets developed pursuant to Requirement R1, the Responsible Entity shall develop a list of associated Cyber Assets essential to the operation of the BES Assets.

Cyber Assets which support the following shall be included:

The operation and control of these BES Assets

The monitoring and alerting functions for the reliable operation of these BES assets

The data acquisition equipment and systems which support automated or operator assisted real-time reliable operation of these BES assets

Any cyber asset which directly interfaces with these Cyber Assets, and which is not identified as a Cyber Asset performing the functions in R4.1 on a BES Asset, will be identified.

The intent here to identify cyber assets which interface with BES Cyber Assets, in most cases for providing data for non-realtime analysis (such as PI data servers or data base servers. These may warrant adequate protection because of their relationship with BES Assets.

The Responsible Entity shall review this list at least annually, and update it as necessary.

Huff R1.1. Identify all Control Systems that perform supervisory control functions (e.g. open/close breakers, raise/lower generation) for the Bulk Electric System or provide situational awareness of the state of the Bulk Electric System. This would include:

Systems that provide situational awareness

Systems performing EMS/SCADA functions

Special Protection systems

Systems essential to BES restoration

Systems performing automatic load shedding

Other systems that may perform a function directly related to BES system reliability

Huff R1.2. Identify internal and external data interconnections between Cyber Systems that provide data necessary for the reliability functions of the previously identified Cyber Systems or Control Systems.

Categorization of Cyber Assets — The Responsible Entity shall apply the following criteria to categorize the identified Cyber Assets:

(In a perfect world, entities should be allowed to determine on their own which cyber assets are high, medium or low. Unfortunately, the current enforcement model does not lend itself to this kind flexibility and requires a more prescriptive categorization scheme.)

High Impact Cyber Assets — All identified Cyber Assets which perform the functions in R4.1 for Critical Cyber Assets shall be included in this category.

Other High Impact Cyber Assets may be identified as a result of further standards.

Medium Impact Cyber Assets — All identified Cyber Assets which directly interface with a High impact system in a protected ESP is a Medium impact cyber asset. Interface is defined as an application based data exchange across an ESP access point.

(Note: Other Medium Impact Cyber Assets will be categorized when the ESP is defined as part of CIP-005 and “incidental” cyber assets in the same perimeter as High Impact cyber assets will be categorized as Medium Impact systems).

Low Impact Cyber Assets — Any cyber asset not categorized as either High or Medium Impact shall be categorized as a Low Impact Cyber Asset.

Annual Approval — The senior manager or delegate(s) shall approve annually the impact assessment methodology, the list of Critical Assets and the list Cyber Assets and their categorization. The Responsible Entity shall keep a signed and dated record of the senior manager or delegate(s)'s approval of the impact assessment methodology, the list of Critical Assets and the list of Cyber Assets and their categorization.

Appendix 8 — CIP-002-3 Strawman (Scott Mix)

Standard CIP–002–3 — Cyber Security — Cyber Asset Identification and Categorization

A. Introduction

1. **Title:** Cyber Security — Cyber Asset Identification and Categorization

2. **Number:** CIP-002-3

3. **Purpose:** NERC Standards CIP-002-3 through CIP-009-3 provide a cyber security framework for the identification, categorization and protection of Cyber Assets to support the reliable operation of the Bulk Electric System.

   These standards recognize the differing roles of each entity in the operation of the Bulk Electric System, the criticality and vulnerability of the assets needed to manage Bulk Electric System reliability, and the risks to which they are exposed.

   Business and operational demands for managing and maintaining a reliable Bulk Electric System increasingly rely on Cyber Assets supporting critical reliability functions and processes to communicate with each other, across functions and organizations, for services and data. This results in increased risks to these Cyber Assets.

   Standard CIP-002-3 requires the identification, categorization and documentation of the Cyber Assets associated with the Assets that support the reliable operation of the Bulk Electric System. These Assets are to be identified and categorized as Critical and non-Critical based on the application of an impact assessment.

4. **Applicability:**

   4.1. Within the text of Standard CIP-002-2, "Responsible Entity" shall mean:

   - **4.1.1** Reliability Coordinator.
   - **4.1.2** Balancing Authority.
   - **4.1.3** Interchange Authority.
   - **4.1.4** Transmission Service Provider.
   - **4.1.5** Transmission Owner.
   - **4.1.6** Transmission Operator.
   - **4.1.7** Generator Owner.
   - **4.1.8** Generator Operator.
   - **4.1.9** Load Serving Entity.
   - **4.1.10** NERC.
   - **4.1.11** Regional Entity.

   4.2. The following are exempt from Standard CIP-002-2:

   - **4.2.1** Facilities regulated by the U.S. Nuclear Regulatory Commission or the Canadian Nuclear Safety Commission.
   - **4.2.2** Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

5. **Effective Date:** The first day of the third calendar quarter after applicable regulatory approvals have been received (or the Reliability Standard otherwise becomes effective the first day of the third calendar quarter after BOT adoption in those jurisdictions where regulatory approval is not required)

Author
Comment: NEED NRC language – Systems …

Author
Comment: Need to determine how to eliminate this clause

Strawman – March 2009 – Collett, Lim, Rosenberger, Varnell
1

B. Requirements

R1. Identification of BES Assets – The Responsible Entity shall identify and document a complete list of BES Assets. Assets may be identified as facilities, equipment or systems. The Responsible Entity shall include, wherever applicable, the following:

Author
Comment: How to determine?

R1.1. Control centers and backup control centers performing the functions of the entities listed in the Applicability section of this standard.

R1.2. Transmission substations that support the reliable operation of the Bulk Electric System.

Author
Comment: How to determine?

R1.3. Generation resources that support the reliable operation of the Bulk Electric System.

Author
Comment: How to determine?

R1.4. Systems and facilities used for system restoration, including blackstart generators and substations in the electrical path of transmission lines used for initial system restoration.

R1.5. Systems and facilities critical to automatic load shedding under a common control system capable of shedding 300 MW or more.

R1.6. Special Protection Systems that support the reliable operation of the Bulk Electric System.

Author
Comment: How to determine?

R1.7. Systems that support wide-area reliability through one or more of the following:

R1.7.1. Situational awareness

R1.7.2. Supervisory and control capability

R1.7.3. Other systems that may perform a function directly related to the reliability or operability of the BES.

R1.8. Any additional assets that support the reliable operation of the Bulk Electric System that the Responsible Entity deems appropriate to include in its assessment.

R2. Critical Asset Identification Method — The Responsible Entity shall identify and document an impact assessment methodology to use to *classify* ts Critical Assets *based on each asset's impact to reliable operations of the BES*.

Author
Deleted: identify i

(Note: This requirement assumes that the NERC guideline will provide more specific guidance in the development of the methodology. As suggested by Scott Mix, a change in terminology may reflect more accurately the nature of this methodology.)

R2.1. The Responsible Entity shall maintain documentation describing its impact assessment methodology that includes procedures and evaluation criteria. The evaluation shall include consideration for Common Mode Impact and Adequate Level of Reliability.

R2.2. The impact assessment shall be applied to *all* BES Assets identified in R1.

Author
Deleted: the

R2.3. The impact assessment shall describe methods or thresholds for assigning one of the following impact levels to each asset:

Author
Formatted: Bullets and Numbering

- *High Impact – loss damage or misuse of the identified asset results in significant impact or significant potential impact to reliable operations of the BES*
- *Medium Impact – loss damage or misuse of the identified asset results in moderate impact or significant potential impact to reliable operations of the BES*
- *Low Impact – loss damage or misuse of the identified asset results in minimal, but identifiable, impact or potential impact to reliable operations of the BES*

Author
Comment: need to define

Author
Comment: need to define

Author
Comment: need to define

- *No Impact – loss damage or misuse of the identified asset results in no identifiable impact or potential impact to reliable operations of the BES*

R3. Critical Asset Identification — The Responsible Entity shall develop a list of its Critical Assets *and their impact classification, as* determined through an annual application of the impact assessment methodology required in R2. The Responsible Entity shall review this list at least annually, and update it as necessary.

R3.1. *The resultant list shall include both the identification of each Asset, as well as its classification level using the impact levels described in Requirement R2.3*

R4. Cyber Asset Identification — Using the list of Assets developed pursuant to Requirement R1, the Responsible Entity shall develop a list of associated Cyber Assets essential to the operation of the BES Assets.

R4.1. Cyber Assets which support the following shall be included:

R4.1.1. The operation and control of these BES Assets

R4.1.2. The monitoring and alerting functions for the reliable operation of these BES assets

R4.1.3. The data acquisition equipment and systems which support automated or operator assisted real-time reliable operation of these BES assets

R4.2. Any cyber asset which directly interfaces with these Cyber Assets, and which is not identified as a Cyber Asset performing the functions in R4.1 on a BES Asset, will be identified.

The intent here to identify cyber assets which interface with BES Cyber Assets, in most cases for providing data for non-realtime analysis (such as PI data servers or data base servers. These may warrant adequate protection because of their relationship with BES Assets.

R4.3. The Responsible Entity shall review this list at least annually, and update it as necessary.

R5. Categorization of Cyber Assets – The Responsible Entity shall apply the following criteria to categorize the identified Cyber Assets:

(In a perfect world, entities should be allowed to determine on their own which cyber assets are high, medium or low. Unfortunately, the current enforcement model does not lend itself to this kind flexibility and requires a more prescriptive categorization scheme.)

R5.1. High Impact Cyber Assets - All identified Cyber Assets which perform the functions in R4.1 for Critical Cyber Assets shall be included in this category.

Other High Impact Cyber Assets may be identified as a result of further standards.

R5.2. Medium Impact Cyber Assets – All identified Cyber Assets which directly interface with a High impact system in a protected ESP is a Medium impact cyber asset. Interface is defined as an application based data exchange across an ESP access point.

(Note: Other Medium Impact Cyber Assets will be categorized when the ESP is defined as part of CIP-005 and "incidental" cyber assets in the same perimeter as High Impact cyber assets will be categorized as Medium Impact systems).

Author
Deleted: identified

Author
Comment: how to identify?

Author
Formatted: Bullets and Numbering

Author
Comment: how to identify?

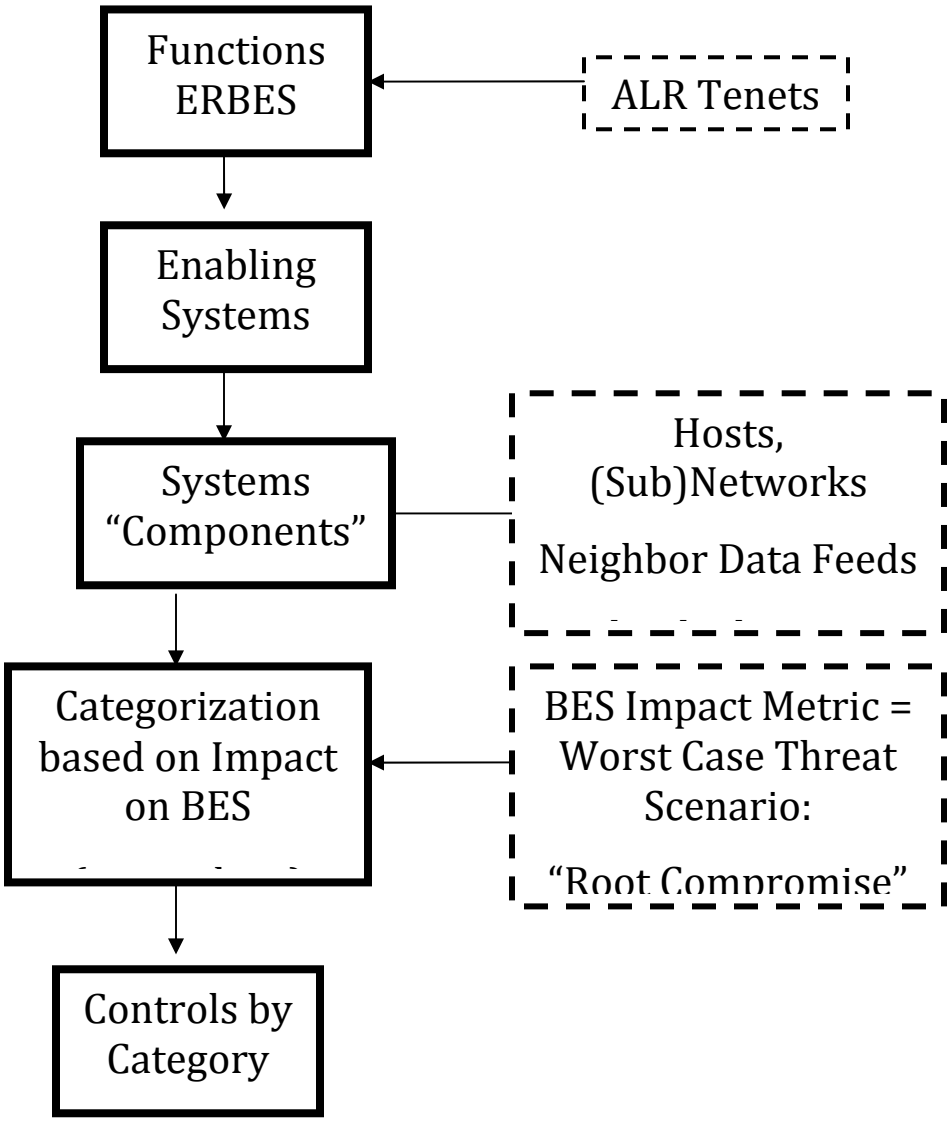
Author
Comment: 2-step process: Cyber asset impact AND Cyber-asset-impact to Asset impact

R5.3. Low Impact Cyber Assets – Any cyber asset not categorized as either High or Medium Impact shall be categorized as a Low Impact Cyber Asset.

R6. Annual Approval — The senior manager or delegate(s) shall approve annually the impact assessment methodology, the list of Critical Assets *and their categorization,* and the list Cyber Assets and their categorization. The Responsible Entity shall keep a signed and dated record of the senior manager or delegate(s)'s approval of the impact assessment methodology, *a signed and dated record of* the list of Critical Assets and *a signed and dated record of* the list of Cyber Assets and their categorization. *The Region / RC must approve the methodology and list of Assets and their characterization.*

Author
Comment: Need external oversight and approval per FERC order

Scoping Logic Synthesis Proposal



SDT 706 Meeting Schedule 2009 Calendar Form

NAME:_____

CHECK ONLY THOSE DATES ON WHICH YOU HAVE A CONFLICT!

Instructions: The SDT will set the dates for its July-December, 2009 at the March 10-12 Meeting. You can email you completed form as an attachment to: rmjones@fsu.edu by COB March 9. OR if you plan to attend the meeting you can bring your completed form which will be collected at the end of day one (March 10). We will announce the meeting dates based on the fewest number of member conflicts. Locations are TBD.

July 2009

WEEK OF July 13	Mon July 13	Tues. July 14	Wed. July 15	Thurs. July 16	Fri. July 17
WEEK OF July 20	Mon July 20	Tues. July 21	Wed. July 22	Thurs. July 23	Fri. July 24
WEEK OF July 27	Mon July 27	Tues. July 28	Wed. July 29	Thurs. July 30	Fri. July 31

August 2009

WEEK OF August 3	Mon Aug 3	Tues. Aug 4	Wed. Aug 5	Thurs. Aug 6	Fri. Aug 7
WEEK OF August 10	Mon Aug 10	Tues. Aug 11	Wed. Aug 12	Thurs. Aug 13	Fri. Aug 14
WEEK OF August 17	Mon Aug 17	Tues. Aug 18	Wed. Aug 19	Thurs. Aug 20	Fri. Aug 21
WEEK OF August 24	Mon Aug 24	Tues. Aug 25	Wed. Aug 26	Thurs. Aug 27	Fri. Aug 28
WEEK OF August 31	Mon Aug 31	Tues. Sept 1	Wed. Sept 2	Thurs. Sept 3	Fri. Sept 4

September 2009

WEEK OF September 7	Mon Sept 7 Labor Day	Tues. Sept 8	Wed. Sept 9	Thurs. Sept 10	Fri. Sept 11
WEEK OF September 14	Mon Sept 14	Tues. Sept 15	Wed. Sept 16	Thurs. Sept 17	Fri. Sept 18
WEEK OF September 21	Mon Sept 21	Tues. Sept 22	Wed. Sept 23	Thurs. Sept 24	Fri. Sept 25

WEEK OF September 28	Mon Sept 28	Tues. Sept 29	Wed. Sept 30	Thurs. Oct 1	Fri. Oct 2

October 2009

WEEK OF October 5	Mon Oct 5	Tues. Oct 6	Wed. Oct 7	Thurs. Oct 8	Fri. Oct 9
WEEK OF October 12	Mon Oct 12 Thanksg CA	Tues. Oct 13	Wed. Oct 14	Thurs. Oct 15	Fri. Oct 16
WEEK OF October 19	Mon Oct 19	Tues. Oct 20	Wed. Oct 21	Thurs. Oct 22	Fri. Oct 23
WEEK OF October 26	Mon Oct 26	Tues. Oct 27	Wed. Oct 28	Thurs. Oct 29	Fri. Oct 30

November 2009

WEEK OF November 2	Mon Nov 2	Tues. Nov 3	Wed. Nov 4	Thurs. Nov 5	Fri. Nov 6
WEEK OF November 9	Mon Nov 9	Tues. Nov 10	Wed. Nov 11 Vet/Rem. Day	Thurs. Nov 12	Fri. Nov 13
WEEK OF November 16	Mon Nov 16	Tues. Nov 17	Wed. Nov 18	Thurs. Nov 19	Fri. Nov 20
WEEK OF November 23	Mon Nov 23	Tues. Nov 24	Wed. Nov 25	Thurs. Nov 26 US Thanksgiv.	Fri. Nov 27
WEEK OF November 30	Mon Nov 30	Tues. Dec 1	Wed. Dec 2	Thurs. Dec 3	Fri. Dec 4

December 2009

WEEK OF December 7	Mon Dec 7	Tues. Dec 8	Wed. Dec 9	Thurs. Dec 10	Fri. Dec 11
WEEK OF December 14	Mon Dec 14	Tues. Dec 15	Wed. Dec 16	Thurs. Dec 17	Fri. Dec 18
WEEK OF December 21	Mon Dec 21	Tues. Dec 22	Wed. Dec 23	Thurs. Dec 24	Fri. Dec 25

NERC

NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Draft Meeting Summary

Cyber Security Order 706 SDT — Project 2008-06

February 18, 2009 | 8 a.m.– 5 p.m. EST
February 19, 2009 | 8 a.m.– 5 p.m. EST

Robert Jones and Stuart Langton, Facilitation and Meeting Design

FCRC Consensus Center, Florida State University

QuickTime™ and a
decompressor
are needed to see this picture.

http://www.nerc.com/filez/standards/Project_2008-06_Cyber_Security.html

116-390 Village Blvd.
Princeton, NJ 08540
609.452.8060 | www.nerc.com

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Cyber Security Order 706 Standard Drafting Team
Draft Seventh Meeting Summary,
February 18-19, 2009
Fairfax, VA

MEETING SUMMARY CONTENTS

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Cyber Security Order 706 Standard Drafting Team
Draft Seventh Meeting Summary,
February 18-19, 2009
Fairfax, VA

EXECUTIVE SUMMARY

The Vice Chair, Kevin Perry welcomed the members. NERC consultant Joe Bucciero conducted a roll call of members and participants in the room and on the conference call/webex. He then reviewed with the Team the need to comply with NERC's Antitrust Guidelines**.** Mr. Perry reviewed with the Team and participants the proposed meeting agenda and objectives. The facilitators reviewed with the Team the consensus guidelines adopted at the SDT November 2008 Little Rock meeting. The Team reviewed and unanimously adopted the SDT February 2-4, 2009 meeting summary with corrections suggested by David and Michael Winter. The Team adopted unanimously the revised January 7-9, 2009 SDT summary. Stuart Langton, SDT facilitator, reviewed the current workplan and meeting schedule for both Phase I and Phase II development.

For the Phase I review, the SDT reviewed and unanimously adopted the Response report that has been developed at the February 2-4 meeting and was finalized and circulated to the SDT on February 13. Dave Taylor noted that Maureen was reviewing the response document and once completed it would be submitted to the Standards Committee possibly at their February 20 conference call.

Scott Mix, NERC staff provided the Team with an update on the status of the Technical Feasibility Exception white paper that the SDT last reviewed in December, 2008 and the effort to convert it into a compliance document under NERC Rules of Procedure. He noted that NERC attorneys have been reviewing and that there are no "show stoppers" as of this point. Prior to posting, NERC will share with the SDT. They anticipate posting for NERC industry wide input in the coming weeks for a 45-day posting period. The SDT discussion stressed the importance linking the posting of the TFE along with the Phase I ballot issues in terms of the industry's response to Phase I standards/requirements proposals. Following a broad discussion of issues and concerns, the SDT took a straw poll (11 in favor, 1 opposed) on the proposition to move forward as planned and agreed to on February 4, 2009. On Thursday morning the SDT unanimously (18-0) adopted a motion to proceed forward on the agreed upon Phase 1 timeline and all related documents.

Dave Taylor talked to standards process manager earlier in the week and it appears that NERC will propose the standards process manager work with subset of SDT and VSL SDT to craft the VSLs for version 2 and be responsible for responding comments. The comments submitted by SDT 706 members urging the VSL SDT address both Version 1 and Version 2 VSLs to the VSL SAR were received but not accepted by the committee. VSL version 1 and Version 2 will for industry

comment simultaneously. Kevin Perry suggested that Dave Taylor distribute it to all SDT members and invite their review and comments. Kevin Perry and Jackie Collett agreed to take the lead.

Michael Winters presented a 2nd draft of guiding principles for SDT consideration that were initially ranked but not discussed by the SDT on February 2. He reviewed the changes he made and suggested the SDT rank the revised principles. The SDT agreed that these should be considered by the Team and industry as a work in progress and preliminary and should be prefaced in our summaries in that fashion. The set of preliminary guiding principles as revised and ranked Are as follows:

These SDT draft guiding principles are a **work in progress** and have been reviewed ranked and refined by the SDT. The SDT will use these principles as it develops its approach and strategies for revising the CIP standards. The SDT expects that these principles will continue to be refined going forward in its standards development process. The draft guidelines are listed below in order of greatest average acceptability (*using a 4 point acceptability scale with 4= acceptable/agreement, 3=agreement with minor reservations; 2= unacceptable unless major reservations addressed and 1= unacceptable)*

1) A mapping of CIPs similar to the NIST 800-53 mapping will help quantify and assess the gaps, if any. *(3.9 of 4)*
2) Protection of the communication devices outside to the electronic security perimeters, are out of scope. *(3.75 of 4)*
3) Create non-proscriptive standards and employ a technical exception/compensating documentation process and guidance process to accommodate variations. *(Resist creating exception based standards to accommodate every possible business and operations scenario) (3.7 of 4).*
4) Strive to preserve existing security investments and build upon the existing CIP requirements. *(3.7 of 4)*
5) It is imperative to protect the integrity of data throughout its transit. *(3.7 of 4)*
6) CIP requirements should consider the unique locational characteristics (e.g. substations, data centers, generation plant) and functional capabilities of the cyber assets to be protected. *(3.7 of 4)*
7) Use a consistent risk-based model to classify cyber assets (as critical/high impact, moderate impact, low impact. This will allow for expansion of standards beyond Critical. *(3.7 of 4)*
8) Consider the minimum security controls for high, moderate, low within NIST 800-53 to help model the CIP requirements for each level. *(3.6 of 4)*

NOTE: The SDT acknowledges that currently an entity's cyber asset classification is subject to scrutiny by the compliance enforcement authority and applicable regulators.

Bill Winters followed up on his white paper presentations at the previous two meetings and provided a power point on a possible approach to integration. He suggested the following in his presentation:

- Leverage work begun by NIST and MITRE- overlay CIP and NIST
- Heavy integration- CIP 002 with NERC versions of FISPS 199, 200. Etc.
- Moderate Integration- update CIP 002 to include categorization standard (FIPS 199 analog). Update CIP 003-009 with 800 53 elements to address gaps in 706. (10-21 MITRE/NIST e.g. CIP 005 augmentation.
- Light integration- 003-009 requirements to align with 800-53 controls. Draw on 800-53 controls to fill in gaps id in 706. Use NIST docs as guidance references throughout CIP.
- Start with light and migrate overtime to moderate and heavy.

Kevin Perry distributed a concept paper titled, "Risk Management Framework and Protected Cyber Asset Identification" a day prior to the meeting. *(See Appendix #)* He introduced it at the end of day one with the following comments. The discussion started on day one and continued onto day two.

Jackie Collett presented the approach developed by a team with John Lim, Scott Rosenberger and John Varnell, that suggested the SDT should revise existing CIP –002 to include the functional and systems approach including some levels of protection. She noted that the reliability of the BES was the basis for the proposed approach to Phase II with a clear link between cyber assets and their function in the BES. A Functional risk assessment methodology could define critical vs. non-critical operating functions and define which cyber assets are involved. The approach would include addressing significant gaps in CIP (they identified 5) She acknowledged that there are benefits in providing some gradations in protection of assets. E.g. control centers need protection. Finally she cautioned against the CIP being too tightly coupled to a standard developed and maintained by another group that when changed would affect the CIP. The discussion highlighted that: a systems approach is missing from CIP 002; a link should be made with NERC Principles of Reliability; and the standards should address enforcement of requirements.

Scott Mix presented his strawman on FISMA asset selection first presented in Phoenix. The Team discussed the implications of his strawman for the SDT workplan and the connection with other approaches under discussion.

In the morning and afternoon of day-two the members discussed the implications of the various approaches to Phase II. They agreed there were evolutionary and revolutionary gradations in the approaches discussed and suggested that their focus should initially be on CIP 002 even thought there may be other issues that need to be addressed in the other standards. The challenge from NERC's Mike Assante was to try to produce an outcome-based standard vs. a prescriptive-based standards. We should be focusing on what is it we want as a desired outcome and less initially on how to get there. Their comments ranging over a number of issues including: how to address un-trusted connections; demarcation of transmission and distribution; building on and tailor controls to

BES; addressing changes in accelerating data rates; addressing industry expectations; and addressing computer vs. physical Standards.
In the afternoon of day two, Michael Winters with assistance from the facilitators presented the following for SDT consideration and further discussion based on the review of the different concept papers. Consistent with SAR and FERC Order 706, Mr. Winters presented potential SDT Approaches to Phase II:

1) Take Bill Winter's proposed low to mid-level approach using the framework outlined by Scott Mix but going beyond status quo by addressing gaps as outlined in 706 as part of the NIST-CIP mapping and gap analysis.
   (How: Perform the mapping analysis of CIP to NIST using 706 view of where gaps exist in the CIPs)
   Consistent with Principle 1, 4, 5, 7 & 8
2) Address a consistent cyber asset selection and categorization method by leveraging Kevin's and Jackie's (and others) thoughts on where gaps exist. Use FIPS 199 as another input or even the starting point but produce a BES version.
   (How: Build a prototype, highlight the differences from existing CIP002 and let's test it.)
   Consistent with Principle 4, 7

Guiding Considerations *(taken from the SDT discussion)* could include:

- Start with the NERC/BES assigned mission
- Take a functional approach CIP 002
- Take a systems approach in CIP 002
- We need to address gradations of risk (e.g. high medium low)
- A deficiency in the current NIST/FISMA regarding measurement and enforcement needs to be addressed in the SDT process.
- Address key challenges identified with current CIP: (e.g. piecemeal approach, not protecting assets needing protection; gaming; all or nothing; loss of asset, integrity/misuse, etc.)
- Address both the physical protection issues and the cyber protection issues, separately or not.
- Assume all outside an entity's direct control should be treated as a un-trusted connection.
- Seek to develop more guidance and less modification of standards as an approach.
- Address CIP 2 R2 so that it doesn't drive people towards the physical assets.
- Taking a cyber view should not preclude a physical view.
- Where possible, build on the existing work and research, models etc. E.g. Build upon MITREs cross walk to the control families.
- Focus on a shared view of the outcome that can capture all the attack vectors to make sure they have been assessed and have minimum security controls that we have not addressed in CIP.

The SDT members agreed they were not yet prepared to proceed with the approaches suggested by Michael Winters. Some suggested further clarification of what was meant by "functional" or

"systems" approaches to 002. After further discussion, the SDT agreed that a helpful next step would be to produce two strawman drafts of a revised CIP 002 based on the work to date. One would be prepared by Jackie Collett & John Lim and another would be prepared by Bill Winters and Kevin Perry with assistance from interested SDT members. These would be distributed in advance of the March meeting and form the basis for the agenda in Orlando.

At the end of day two the SDT took stock of its progress and reviewed the schedule for both an cyber expert and stakeholder workshop and presentation to the NERC Members Representative Committee in early May, 2009. The SDT agreed it needed to have sorted out and developed a clearer understanding and agreement on the Phase II approach prior to presenting a substantive briefing to the MRC. As as a result the SDT agreed to seek to provide a short "progress report" to the MRC in May and seek to present a substantive briefing at their August, 2009 meeting. The SDT suggested scheduling the expert/stakeholder workshop in the early Summer.

The Team then evaluated the meeting in terms of what worked and what could be improved. The meeting adjourned at 3:30 p.m.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Cyber Security Order 706 Standard Drafting Team

DRAFT SEVENTH MEETING SUMMARY, FEBRUARY 18-19, 2009 FAIRFAX, VA

I. INTRODUCTIONS, AGENDA REVIEW AND REVIEW OF SDT WORKPLAN

The Vice Chair, Kevin Perry, welcomed the members. Joe Bucierro conducted a roll call of members and participants in the room and on the conference call *(See appendix #2*). Mr. Perry reviewed the meeting objectives and Bob Jones, facilitator, reviewed with the Team and participants the proposed meeting agenda *(See appendix #1*). Mr. Perry noted that at lunch on both days Harry Tom, NERC, would be seeking informal feedback from SDT team members on

Mr. Bucierro reviewed with the Team the need to comply with NERC's Antitrust Guidelines *(See, Appendix #3).* He urged the Team and other participants in the process to carefully review the guidelines as they would cover all participants and observers. He urged all to avoid behaviors or appearance that would be anti-competitive nature and also reminded the group of the sensitive nature of the information under discussion.

The Team reviewed and unanimously adopted the SDT February 2-4, 2009 meeting summary with corrections suggested by David and Michael Winter. The Team adopted unanimously the revised January 7-9, 2009 SDT summary.

Stuart Langton, SDT facilitator, reviewed the current workplan and meeting schedule for both Phase I and Phase II development. (*See Appendix #4)* In particular he noted the proposed "expert workshop" that was currently scheduled for its April, 2009 meeting in Charlotte which Scott Mix was to help organize with the SDT members assistance, the opportunity to present a progress report to the MRC in early May and the possibility of a white paper for industry comment on the SDT's conceptual approach to Phase II.

SDT Comments on Workplan

- Industry expert workshop planning- Is Duke aware of workshop plans? Facilities to support the workshop? Workshop plus? Sharon Edwards has indicated she has reserved a big room. The plan is to run it on Wednesday morning for four hours
- Mike Assante expressed a desire that the workshop take place in D.C. List of industry experts. Invitations will need to be made quickly.
- Where is the Orlando Utility Commission meeting location in Orlando? It is near the airport and NERC will issue a meeting announcement with nearby hotels.

- Mike Winters- what is the white paper product on Phase II? CIP 002? By July 2009? Can we get there faster? Phase II items. Can we hasten the pace.?
- The SDT has been seeking to develop more understanding and possibly consensus for basic concepts and approach to Phase II from industry. This should make it easier to turn into requirements in standard development review cycles and get quicker into the refinement stage. If we can get the concept agreed to, then we can debate the particulars. Issues with pace.
- White paper for industry comment? What are procedural implications. Nothing in guidelines about a white paper as a tool. The purpose is to gauge the level of industry support for direction and help to brief and educate early on. Need to clarify what the intent of the paper will be and what will be in it.

II. TECHNICAL FEASIBILITY EXCEPTION UPDATE AND SDT DISCUSSION

Scott Mix, NERC staff provided the Team with an update on the status of the Technical Feasibility Exception white paper that the SDT last reviewed in December, 2008 and the effort to convert it into a compliance document under NERC Rules of Procedure. He noted that NERC attorneys have been reviewing and that there are no "show stoppers" as of this point. Prior to posting, NERC will share with the SDT. They anticipate posting for NERC industry wide input in the coming weeks for a 45-day posting period. He noted the default language in Appendix 4C includes a self reporting non compliance procedure being proposed with a similar record keeping model. Since the SDT 706 most knowledgeable on issues, NERC wants to coordinate and consult with members. However the SDT is not responsible for the TFE.

The SDT discussion stressed the importance linking the posting of the TFE along with the Phase I ballot issues in terms of the industry's response to Phase I standards/requirements proposals. Following a broad discussion of issues and concerns, the SDT took a straw poll (11 in favor, 1 opposed) on the proposition to move forward as planned and agreed to on February 4, 2009. **On Thursday morning the SDT unanimously (18-0) adopted a motion to proceed forward on the agreed upon Phase 1 timeline and all related documents.**

Member Discussion Comments

- Need to make sure this is at least static by the time we put out phase I for vote.
- SDT intent in passing Phase I products is that NERC Rules of Procedures will posted for industry comment for at least 14 days prior to initial ballot on Phase I. Pre- ballot period is normally 30 days but will be extended connected with the TFE posting.
- 45 day comment will be followed by response to "significant" comments by NERC. Updating, as necessary and then submitted to BOT for approval. Then to FERC for approval with an opportunity for public comment.

- SDT role? FERC said SDT could apply at TFE in other areas that support operations and safety to insert TFE into a requirement. What about a removal of business judgment and acceptance of risk? TFE doesn't address.
- No drafting teams involved in ROP. Mike Assante will present for industry comment. SDT can have input to NERC staff but no control over ROP language.
- Does the current TFF draft say what language must be in a requirement? Requirements say do if technically feasible. Does it say TFE anywhere? Does that language appear in every standard?
- Appears in 4 areas in Phase I requirements: 3 areas in CIP 7 and 1 area in CIP 6 alternative measures of protection.
- May be other places where a TFE might be applicable.
- Requirements are the only thing that is enforceable. Operational and safety concerns included as order provides. FERC would be open to accepting TFE into requirements.
- Requirement by requirement. Sub requirement by sub requirement.
- Do we need to put in Phase I document?
- Timing issues. If SDT pulls back Phase I. Given language proposing, are we going to have to do emergency phase 1A on heels of it that clarifies TFE? In the form of an interpretation?
- Current draft of TFE says, as "specifically identified in standard."
- Problem is the July 1, 2009 audit date from the FERC order. TFE will go through NERC ROP process. The posting and comment process won't be nailed down until later in the year. It is apparent that concern is TFE is applicable to "Version 1 CIP Standards." Working on Version 2. Draft TFE identifies version 1. Then going forward Version 2 applicable as designated within requirement itself.
- Modify version 2 (phase 1) figure out which requirements are applicable to use a TFE. 30 days in the current schedule is provided for Board review. Pre-ballot review period.
- It will be difficult to still meet schedule if we modified requirements to include TFE language. Posting for comments for modifying language again. "Comment response and resolution"
- Practically speaking, we received a number of comments on the Phase I TFE language, and we should expect the same amount of comments if not more for the TFE process.
- Worried about CIP 002-009 review- SDT never had a safety and operations review. What is harm in submitting TFE on any standards?
- It is a potential resource issue in terms of NERC processing, investigating, and reviewing requests.
- If you want to take a TFE, you will have to provide justification. People are going to be aware of need for justification and won't try to abuse the system. We can try to guess where TFE is applicable. But that will not be a valuable effort. E.g. what are all the emergency conditions are requiring a TFE. If we miss it we harm somebody. Entity can choose to file TFE if they can justify and get approved, if not they will be in jeopardy.

- Compliance philosophy- may be seen as shooting holes in standards if you can request TFE for anything.
- ROP: "Comment resolution process"- NERC must incorporate the "well founded" comments and respond to the others.
- Problem is not the TFE process. We took things out of Phase I that people think were covered by TFE. If we don't do something about this the industry will vote this down.
- Need a review and cover "heavy hitters" that would cause industry to vote down Phase I.
- This doesn't address reasonable business judgment piece. FERC take it out. If it looks like this it will be rejected.
- TFE can be a valuable tool to better protect the BES. Industry shouldn't hide, but call it out. By calling it out, it allows peers in industry to share strategies. Allows for another set of eyes to say we figure it out. Is there another mechanism to allow for peer review? Not as part of ROP. If we limit it, it will take away from what we are trying to do.
- The current compliance process calls this out at the regional and NERC levels. Regional entity and ERO allowed to say we've run across this in other audits etc. have you thought of this?
- FERC requires report each year on which requirements are having TFEs being requested for? Yes but redacted at a high level, not on an entity or regional basis. But there should be enough to allow industry to see what the actual technical problem is. Can we leverage this to improving our overall security posture?
- Regions have other venues to discuss how to do something, such as work groups.
- If we go back and address TFEs we will have to hear from industry. Version 2 standards will address this, and the Phase I language that is there now may be sufficient.
- SDT should be responsive to industry once TFE settles. May need to put out Version 3 quickly to address any industry issues.
- Let's go forward and respond as needed.
- Concerned about SDT standard response to comments regarding reasonable business judgment and TFE process. Is this true "should" as part of the response? E.g. page 188, Removal of reasonable business judgment comment and response: "The expansion of TFE should address."
- FERC 158- should not be allowed to use TFE on basis of reasonable business judgment"
- "Address concerns," not replace TFE. We can acknowledge concerns regarding removal of reasonable business judgment. Inserted some flexibility back with TFE. Enough flexibility in all the right places? It is in all places we think it needs to be.
- SDT should go with what we have in terms of Phase I with the risk it industry voting it down. Don't have a good solution. Need to pick the best of a set of bad solutions.
- Team has gone through responses. Documents are consistent with comments.
- If we change TFE language, would we have to change responses? Possibly yes.
- SDT should move forward with track we are on. Post for pre-ballot review. Industry can vote no with negative comment. If ballot is no, NERC will file something by June, 2009 to

FERC. Let the TFE debate take place in that ROP procedure. Phase 2 version 3- include language in those standards.

- If we make even 1 change- fall prey to "hurry up". Let's not let perfection get in the way of adequate here.
- If it goes out for initial ballot and a negative vote recirculation, can we change the standards before re-circulating? No, can't modify at that point.
- If we get 1 negative vote with comments, that will trigger a recirculation ballot. Develop reply comments and post those. Ballot is same unless you change it.
- Test by straw poll going forward:
- Go ahead and proceed with approved Phase I documents including response document to posting for pre-ballot comment period, post for balloting at least 14 days after TFE posted by NERC and see what happens. *(Straw poll: 11 (10/1) for and 1 against)*
- If the industry is opposed, will become apparent after first ballot. If that happens, SDT can withdraw the standards.
- On Thursday morning the SDT unanimously (18-0) adopted a motion to proceed forward on the agreed upon Phase 1 timeline and all related documents.

III. VSL SAR COMMITTEE UPDATE

Dave Taylor talked to standards process manager earlier in the week and it appears that NERC will propose the standards process manager work with subset of SDT and VSL SDT to craft the VSLs for version 2 and be responsible for responding comments. The comments submitted by SDT 706 members urging the VSL SDT address both Version 1 and Version 2 VSLs to the VSL SAR were received but not accepted by the committee. VSL version 1 and Version 2 will for industry comment simultaneously. Kevin Perry suggested that Dave Taylor distribute it to all SDT members and invite their review and comments. Kevin Perry and Jackie Collett agreed to take the lead.

IV. PHASE I RESPONSE DOCUMENT

Kevin Perry noted the SDT had provisionally accepted the Response Document at its February 2-4 in Phoenix. Dave Taylor noted that Maureen was reviewing the response document and once completed it would be submitted to the Standards Committee possibly at their February 20 conference call. The SDT members indicated they were happy with the draft that was completed following the meeting that was consistent with the SDT decisions on responses made at the Phoenix meeting. The Response document sent to the SDT members on February 13.

SDT Member comments and suggestions:

- Suggest a sentence as part of the deferral to Phase 2 response: "The Phase 1 revision to the CIP 002 were focused on the high priority issues raised by FERC in its Order 706 and by the

industry. Additional comments provided are better suited for feedback in Phase 2 and subsequent phases of the CIP standards."
- Senior manager his/her role

V. PHASE II CONCEPT DEVELOPMENT

A. Guiding Principles- *Michael Winters*

Michael Winters presented a 2nd draft of guiding principles for SDT consideration that were initially ranked but not discussed by the SDT on February 2. (*See Appendix #5 for rankings and comments)* He reviewed the changes he made and suggested the SDT rank the revised principles. Below are the "clean version" for the principles resulting from the discussion and suggestions on February 18. The SDT agreed that these should be considered by the Team and industry as a work in progress and preliminary and should be prefaced in our summaries in that fashion.

The set of preliminary guiding principles as revised and ranked are:

These SDT draft guiding principles are a **work in progress** and have been reviewed ranked and refined by the SDT. The SDT will use these principles as it develops its approach and strategies for revising the CIP standards. The SDT expects that these principles will continue to be refined going forward in its standards development process. The draft guidelines are listed below in order of greatest average acceptability (*using a 4 point acceptability scale with 4= acceptable/agreement, 3=agreement with minor reservations; 2= unacceptable unless major reservations addressed and 1= unacceptable)*

1. A mapping of CIPs similar to the NIST 800-53 mapping will help quantify and assess the gaps, if any. *(3.9 of 4)*
2. Protection of the communication devices outside to the electronic security perimeters, are out of scope. *(3.75 of 4)*
3. Create non-proscriptive standards and employ a technical exception/compensating documentation process and guidance process to accommodate variations. *(Resist creating exception based standards to accommodate every possible business and operations scenario)*
    a. *(3.7 of 4).*
4. Strive to preserve existing security investments and build upon the existing CIP requirements. *(3.7 of 4)*
5. It is imperative to protect the integrity of data throughout its transit. *(3.7 of 4)*
6. CIP requirements should consider the unique locational characteristics (e.g. substations, data centers, generation plant) and functional capabilities of the cyber assets to be protected. *(3.7 of 4)*

7. Use a consistent risk-based model to classify cyber assets (as critical/high impact, moderate impact, low impact. This will allow for expansion of standards beyond Critical. *(3.7 of 4)*
8. Consider the minimum security controls for high, moderate, low within NIST 800-53 to help model the CIP requirements for each level. *(3.6 of 4)*

NOTE: The SDT acknowledges that currently an entity's cyber asset classification is subject to scrutiny by the compliance enforcement authority and applicable regulators.

B. NIST/CIP Integration- *Bill Winters*

Bill Winters followed up on his white paper presentations at the previous two meetings and provided a power point on a possible approach to integration *(See appendix #6)*. He suggested the following in his presentation:

- Leverage work begun by NIST and MITRE- overlay CIP and NIST
- Heavy integration- CIP 002 with NERC versions of FISPS 199, 200. Etc.
- Moderate Integration- update CIP 002 to include categorization standard (FIPS 199 analog). Update CIP 003-009 with 800 53 elements to address gaps in 706. (10-21 MITRE/NIST e.g. CIP 005 augmentation.
- Light integration- 003-009 requirements to align with 800-53 controls. Draw on 800-53 controls to fill in gaps id in 706. Use NIST docs as guidance references throughout CIP.
- Start with light and migrate overtime to moderate and heavy.

The facilitators asked the SDT members to address what do you like most about the proposal.

Member Comments and Suggestions

- Do you intend a sequential work process? Yes explore this moving into this over some timeline. Assessment of how fast to move. Proposing heavy with a ramp up.
- NIST mapped initially CIP 005. Then looked at gaps with 800-53- harmonized standards by adding into CIP standard 005. This was done as an example and exercise to see how that worked. Full spread sheet- 2nd document is the entire mapping. (*see pp 2 of Bill Winter's ppt.).*
- When this was done, they didn't take into account all the CIP standards other than 005 nor consider the FAQ?
- How to do this and address conceptual differences between two? What are the differences. E.g. CIP 005 doesn't have controls. Tried to keep CIP as existed and tried to do.
- Suggest the SDT continue to explore this going forward.
- What are the limits, if any, in regards to ANSI process?
- I.e. do our own processes hamstring us? Do we need to think further outside our box?

- Ways both around and through- e.g. guidance documents- guidelines in support of a standard. Including supporting docs and supplemental info. Solves issue of "embedded" guidance. Informative vs. normative ? This is non binding and functional.
- NIST/FISMA- extensive supportive reference documents builds a stronger approach to cyber security.
- Not ready to go to heavy integration. Do like the graduated approach. It is essential that we address CIP 002 first. Kevin's paper seems to attempt that. Going from light to heavy doesn't address the CIP 002. Concept is great, but not ready for the whole cup of koolaide.
- Jump to the medium. It will be a long march through "corn starch" of "light." Starting at medium makes sense. We are most interdependent of structures. Chemical, water, transportation, all going towards the NIST standards approach.
- ISA 99- security standards work group. SDT 706 should review how they are approaching it. KS willing to report back.
- Considering more than 3 levels. Requirements are very near to 800-53. Appendix- applied in a control system environment. Making them control system specific.
- 800-82 guidance document- not a standard without requirements. Provides implementation guidance.
- We should be careful not to limit ourselves.
- Light to moderate approach is complementary to our principles.
- Identification of challenges for CIP.
- "How"
- ISA 99- is similar to the moderate integration proposal.

C. Risk Management Framework and Protected Cyber Asset Identification- *Kevin Perry*

Kevin Perry distributed a concept paper a day prior to the meeting. *(See Appendix #7)* He introduced it at the end of day one with the following comments. The discussion started on day one and continued onto day two.

- Set of cyber assets (control systems) directly affecting the BES.
- Identify those systems that have direct control function or direct visability function. Doesn't matter where it is.
- Look at those critical/essential to reliability function.
- Who is feeding data that you must have, keeping going out. You may cross your neighbor's border? KC power and light feeds EMS data to SPP, SPP feeds them data. Essential to SPP. You get cyber assets having some impacts on BES. What is that impact on the BES? High, medium low impacts determined.
- List of cyber assets that have to be protected. Define perimeters. Apply graduated set of controls based on the impact like 800-53.
- Set criteria on regional basis for conformity.

- Consistent with the principle, depending on the cyber asset itself, the controls will vary.
- Address cherry picking approach. --vulnerability
- Ignored cyber assets with similar functions

Initial SDT Comments

- Is this not a big departure? Still have to establish relationship between cyber assets and other BES. BES Critical assets and then cyber assets associated with them. Identify all cyber assets that touch things.
- This turns process upside down.
- Dynamic system- things change.
- Description of functional approach.
- ERCOT annually reassessing what is critical.
- This is consistent with how to develop NERC equivalent with FIPSE documents. Consistent with risk assessment model. Those describe what need to be in NERC version of these documents.
- Today we look at physical facilities. Determine if it is critical to BES if it is lost. Then sub-set of facilities look at cyber assets for that facility. E.g. Entergy has over 100 generating plants. If 5 or 6 or critical, then don't look at the others. IPPs under certain conditions may be in the path.
- Inventory all cyber assets and impacts of each and then protect accordingly. Conditions can change but the cyber assets have the same characteristics.
- Like the idea of giving the primary charge at the reliability coordinator level.
- A lot of issues raised are also discussed in the draft critical asset id guideline. How close will this concept apply? Are we casting the net too wide? Protecting everything that is a computer? Is industry prepared to accept?
- Under today's approach, we wouldn't consider the SM Honda 2.0 generator vulnerability. Proposal has an impact analysis- and as such is loosely related to current method.
- Under this model, how many would be deemed to be "securable"? All 103 minimum on control systems at the plants. Different number of controls on control systems impact.
- Are we expanding this for the industry by a factor of 20?
- Yes, but this should be phased in over time- phased roll out to transition. This causes you to look at everything, but phase in over time.
- Common mode failure is a problem. One system considered critical another may not be. Tied together systems- sending or receiving data- need some way of verifying data validity. Lots of systems in use to keep bad things from happening. Focus should be on checking validity of data to keep common mode failures to a minimum. This scenario is not as bad as portrayed. The SDT can work on standards to improve. Common mode failure should not drive us to say every thing is a critical cyber.
- Concept requires industry to figure out what systems are talking to other systems. I am feeding data to your system and you are relying on my data, my system is a critical asset.

- Shouldn't data validity checks take care of this?
- Conceptually we shouldn't start with an engineering study before identifying cyber assets.

Day Two Discussion

- Desired outcome as stated in the paper is consistent with CIP 2 outcome.
- Get to a list of cyber assets having an impact on BES and an entity has to be able to justify how they got there.
- Rather not tell them how they are going to do this. Problem is R2 of CIP 002. List of facilities that have a high impact on BES. It has meant we don't look at first cyber asset until the facilities list is developed. That is where heartburn exists with existing standard approach.
- Jackie Collett has a good approach. Others took a different approach- engineering analysis if unit went off line or disappeared. Didn't consider cyber systems/assets until they narrowed the list of facilities.
- Could be a "high impact" system of a broader approach.
- Kevin Perry agrees that not every cyber asset has to be protected. If it touches, or open and close breakers needs some minimum set of controls. Look at Aurora vulnerability to understand concern. It wasn't they blew up industrial generator but it was the gaining access and turn from a protective to a damaging device.
- CIP 002 R2 has to go. R3- how we get there- look at and justify the right list. Any approach will work.
- We have to apply NIST experience and Kevin's paper incorporates a functional view as Jackie is describing. FIPS 199 is categorization process. Are we in "violent" agreement but approaching from different ends of perspective?
- NIST- not good guidance on how to do 199- learn by experience. Look at system from a functional perspective.
- If we take a systems perspective we will get too granular or lose broader perspective. Look at from functional perspective, how they map back to systems in terms of impact- that is where the industry needs SDT to head.
- Deficiencies in 002- give industry the guidance it needs. Through the guidance process. Need to agree that we are talking about the right assets.
- Key problem- keep looking at CIP standards and 800-53. Should acknowledge CIP deficiencies. Tools to mitigate identified risk that have impact on mission functions. Process of tailoring and scoping.
- Look at system that has a function, may not apply all controls. Can't do under CIP making it difficult to implement.
- CIPs are black/white, requirements-based approach vs. an objectives-based approach.

D. Revise existing CIP –002 to include the functional and systems approach including some levels of protection. *Jackie Collett, John Lim et al*

Jackie Collett presented the approach developed by a team with John Lim, Scott Rosenberger and John Varnell, that suggested the SDT should revise existing CIP –002 to include the functional and systems approach including some levels of protection. *(See Appendix #8 for White Paper)* She noted that the reliability of the BES was the basis for the proposed approach to Phase II with a clear link between cyber assets and their function in the BES. A Functional risk assessment methodology could define critical vs. non-critical operating functions and define which cyber assets are involved. The approach would include addressing significant gaps in CIP (they identified 5) She acknowledged that there are benefits in providing some gradations in protection of assets. E.g. control centers need protection. Finally she cautioned against the CIP being too tightly coupled to a standard developed and maintained by another group that when changed would affect the CIP. The discussion highlighted that: a systems approach is missing from CIP 002; a link should be made with NERC Principles of Reliability; and the standards should address enforcement of requirements.

Member Discussion Comments

- Key difference with Kevin's approach. Functional risk assessment methodology- define critical vs. non-critical operating function and define which cyber assets are involved.
- Operations functions may be broader. Generation is the function provided not just by the physical unit and is treated as part of the system. Includes plant control and functions and other systems.
- Common modes have to be protected. The Team may need to provide more explanation as they did this before the risk assessment guidelines came out last week.
- Why do we need to look at all cyber assets if they won't have an impact on BES?
- The approach suggests providing more guidance and less change/modification in the CIP standards.
- **Systems Approach Missing from CIP 002.** The SDT seems to agree that 002 is missing a systems approach- is there consensus?
- You can't leave the SCADA system off the list.
- Does a systems approach adjustment or replacement of CIP 002?
- Industry is ready for more specific guidance on what should be included and not included in the assets category.
- R1.2- assets- listed. Systems not mentioned until R1.2.4. Only 2 places where "systems" show up in CIP 002.
- Way the CIP is written today, it drives most to the individual physical asset not to a system approach.
- Is that the intent of CIP 001 critical assets.
- However, SCADA system is not starting with whole world. Identify the systems that open control breakers, etc. Looking only at physical asset approach is the concern with the approach Jackie et al are proposing.
- Industry may not want specificity back in? Needs to be there but they may not want it. Indicated in the guideline- "135% of applicable ratings on line"- comments from industry on

guidelines- we were "being way too specific." Pulled out the detail. Guideline will be missing from the next version.

- **Link with NERC Principles of Reliability.** Observation: important to tie back to the NERC adequate levels of reliability documents- 6 principles of a reliable bulk electric system.
- "One principle #4 is to maintain operations within normal ratings under normal conditions"
- Assigned adequate level assigned. Nothing in control centers about damage to equipment running too much power through.
- What classifications, characteristics, need to be put back in to get at principle #4?
- Disconnect between what industry wants, needs and finds acceptable.
- Remember that when standards passed- NERC was voluntary. Wrote to be innocuous as possible. The world has changed. SDT charged with "husbandry" for the industry.
- Electrical engineering mindset. E.g. no EHV substations are deemed as critical. Some of the largest entities across many states and none are critical. TVA ran modeling- applied the "sniff test" in addition to the electrical engineering. By policy (common sense) include all EHV and all nuclear plants, switchyards and loop stations and provide minimum standards.
- The SDT is charged with doing the right thing. Anything dancing around it won't do. "The terrible swift sword will come down upon us." This is our last, best shot at getting this right.
- NERC has responsibility over BES. Different governing bodies dealing with other standards. CIP standards directed only at things NERC has responsibility for.
- **Address Enforcement of Requirements.** Nothing in current CIP precludes a systems based approach. The requirements approach provides measures for compliance/enforcement and auditing. Guidelines should say here are things to meet the requirement, but Requirements need to be measureable.
- No need to for "engineer- bashing" on the team. Agree with the load flow approach and the planning approach.
- Keep in mind (in response to auditability), that in the NIST world the enforcement structure is a shortcoming and a deficiency in the NIST process. Are security controls in place operating as intended?
- Assumption that if you do those things- requirements- you do those thing you are managing risk. This doesn't necessarily buy security. This is one of the fundamental things we are grappling with. In this and other control frameworks. Is it operating as intended, does it mitigate risk? Fundamental assumption-
- Look at sub-standards that exist to make measureable today. Identify the appropriate series of control.

E. FISMA Asset Selection Strawman, *Scott Mix*

Scott Mix presented his strawman on FISMA asset selection first presented in Phoenix *(See, Appendix #9)*. The Team discussed the implications of his strawman for the SDT workplan and the connection with other approaches under discussion. He provided the following overview comments:

- Step 2- Control categories and catalogues- 3-9 more focused. Control based approach. More than control selection. More agreement on control selections.
- FIPS- mission focused- accomplish the organization's defined, assigned mission. Get agreement on SDT and in industry at large
- What is the impact to mission if confidentiality compromised. (e.g. computer by computer and data_
- Is it systems? It is information system and information. Run through for each piece separately
- Distribution- VPS and aggregated distribution. Where is the demarcation? 100 kv? Law says excluding "distribution" facilities. Marketing/NASBE. Not strictly reliability
- What if these systems are used by those controlling reliability?
- Current CIP- focused on high impact assets and ignored the rest. Have we done a good job at identifying the high impact assets?
- Is there a class of assets that really doesn't matter in terms of mission.
- Within scope, based on some form of analysis. Still have low and medium assets. Consider category of "lower than low assets. Discuss whether there is a lower than low set of assets that don't matter.
- This is a mid level approach to FISMA using Bill Winter's terms- Current 002 modify to classify all transmission assets/functions and set a high, medium, lows. Minimum level for everything that matters. 800-53 may provide a good starting point for categorization.

SDT Member Comments

- How long will that take? Decades probably.
- Factor of 9 to maintain status quo?
- Does this meet requirements of 706?
- Haven't address multi layers defense in depth.
- "Treading water" is not what the SDT should do- there will be the perception of avoidance. Keep in mind Congress is paying attention.
- How best to accomplish and modify standards
- Apply high water impact mark. Not three layers. Vast majority doing low now. There is actually not so much difference from low to high.
- Flaw in logic- bad guys seek to attack a high value asset from a low value asset. Not the same logic process. Cutting edge of the problem. E.g. use substation to attack upstream.
- Probably not a factor of 9. If look at CIP now and do the math- then yes. Look at how NIST framework- changes.
- Comes back to the systems approach earlier
- This is anything but treading water maintaining status quo. We are proposing to bring more into scope. Follow a different framework. Identify gaps and fill them. Achieve a better application of controls to BES reliability.

- Pinecone power- low trusted zone to high trusted zone. Need access control in high zone for protection.
- That is a requirement today. It is Null on list. Entergy protects itself from Pinecone power whether it is on the list or not.
- SDT is converging to same thing- the need for a consistent risk base- whether its functional.

F. SDT Discussion of Phase II Approaches

In the morning and afternoon of day-two the members discussed the implications of the various approaches to Phase II. They agreed there were evolutionary and revolutionary gradations in the approaches discussed and suggested that their focus should initially be on CIP 002 even thought there may be other issues that need to be addressed in the other standards. The challenge from NERC's Mike Assante was to try to produce an outcome-based standard vs. a prescriptive-based standards. We should be focusing on what is it we want as a desired outcome and less initially on how to get there. Their comments ranging over a number of issues are noted below:

- **Untrusted connections.** Remember that we have to take care of our own assets. Anything coming in from another system, we have to verify all that goes over that.
- Is this an isolationist viewpoint that narrows the focus? Don't disagree,
- We agree that entities should assume all outside control should be treated as a un-trusted connection. Need to be in a cooperative mode throughout industry to achieve security protection.
- Under existing law- don't know what they are doing. Either or? Both/and. Take a systems approach without having to know a system next to you or elsewhere vs. everything about every system that connects with him.
- E.g. SPP members- I have an ICCP- we have in out in a DMZ- nothing coming in important to us and our balancing authority. Declared it not in the scope of CIP. Probably spot on right. That node is essential to SPP ability to see what goes even if not essential to their system. SPP has a reliability role.
- You can handle two of those nodes going down under current system. Data down is an application thing. Key problem with the Perry proposal?
- Protect what you need to protect- just because it was not on list doesn't mean it is not being protected.
- Concepts- identify high, med, low- if there is an electronic security perimeter, all assets may have to be treated as most restrictive. Look for policies and procedures.
- **Demarcation – transmission and distribution**. 100kv and above. Where is that generation and control systems. Relates to how big the scope will be.
- Agree line is fuzzy. But from a NERC viewpoint- load shedding happens a lot at less than 100 kv systems with an impact on BES under NERC.
- Does this satisfy 706? Does 800-53 have a control for it?

- **Build on and tailor controls to BES.** We can push back into 800-53 those controls we think we need for our purposes. Wouldn't need to create new controls. Could modify NIST controls to fit BES environment.
- Caution against bringing in FERC 706 terms such as "defense in depth."
- It is more than what we are doing right now. The SDT should ask FERC to describe what it means.
- **Address Changes in Data Rates.** We have to anticipate for the future. NASPEE- net being designed. Sustained data rates of 6 megabits among data centers- Agree to protect your boundaries. Difficult challenge ahead: latency performance and security. In future real time high speed sharing
- Practical concern about "lower than low"
- **Industry expectations.** "Acceptability"- haven't sold the need for cyber security to the industry. Tell me what I have to do if it is regulatory.
- Our current CIP is not an approach that can serve the industry well. We want an outcome- list of cyber assets- to be protected commensurate with impact.
- **Computer vs. Physical Standards.**
- Possibility of ending up with 2 different methods one for computer one for physical systems.
- Correct- offer that the threat vectors for physical attacks are far different from a vector for a cyber attack. Threat and opportunity is different. Some overlap.
- Point out- if we follow this approach, we are creating a default position eliminating an analysis of physical assets and electronic asset.
- Assume physical asset standards may be used. Make a conscious decision.
- We will end up not having intermediate product. Critical electrical needing physical approach. ignore physical protection of physical assets. Jackie's approach what's critical to BES reliability- drive to cyber.
- Fan of the idea of a separate set physical standards. Systems based approach doesn't preclude that. Every NIST effort includes physical standards.
- Critical asset id methodology would not go away? Still a systems view bottom up approach. Take work already been done and use to determine impact level.
- Let's not assume that that is the case.
- good research going on now on intertwined nature of cyber and physical system. OakRidge National Lab- simulation and modeling on front.
- Relation between 2 is subtle and complicated than we have understood in the past. Research bear this out. Why you shouldn't start with physical in the CIP standard. Electronic security perimeter- treated as critical assets. Attacker isn't going for critical stuff, start from a print server and hop scotch from there.
- What happens when entire system overwhelmed by 3 million bites. Good sound reasons for disconnecting physical analysis and cyber analysis.
- Anything that opens or closes breaker, open generator unit, etc

- Connectivity- are they and in what manner, they become in scope for assessment. May not be essential but assessment will be instructive.
- Impact not just on the function but also whether the path can be used. How explicit in functionality in terms of interconnectedness, determining where you need to implement control.

In the afternoon of day two, Michael Winters with assistance from the facilitators presented the following for SDT consideration and further discussion based on the review of the different concept papers. Consistent with SAR and FERC Order 706, Mr. Winters presented potential SDT Approaches to Phase II:

1) Take Bill Winter's proposed low to mid-level approach using the framework outlined by Scott Mix but going beyond status quo by addressing gaps as outlined in 706 as part of the NIST-CIP mapping and gap analysis.

(How: Perform the mapping analysis of CIP to NIST using 706 view of where gaps exist in the CIPs)
Consistent with Principle 1, 4, 5, 7 & 8

SDT Comments on approach

- Happen in parallel.?#1 is 03-09. #2 is more about 002.
- Includes every approach we discussed.
- Bill Winters and Keven Perry's in line. Scott is along same lines.
- 7 goes with one as well
- Are we going into the how?
- Can't separate categorization from selection. FIPS 199 process most important and least understood. Can they stand alone?
- Need to be able to see where approaches align and where there are gaps. Jackie vs. Kevin or Bill's approach drives to selection and applying controls

2) Address a consistent cyber asset selection and categorization method by leveraging Kevin's and Jackie's (and others) thoughts on where gaps exist. Use FIPS 199 as another input or even the starting point but produce a BES version.
(How: Build a prototype, highlight the differences from existing CIP002 and let's test it.)
Consistent with Principle 4, 7,

Comments:

- Split between controls and 002 piece? Yes
- How to select and categorize.
- How to address gaming etc. how you select cyber assets.
- Bill Winters and Scott Mix covered both.

- If starting with FIPS 099-
- Kevin Perry discussed controls-how you are applying them.
- Try to get a small team together to do some drafting?

Guiding Considerations *(taken from the SDT discussion)* **could include:**

- Start with the NERC/BES assigned mission
- Take a functional approach CIP 002
- Take a systems approach in CIP 002
- We need to address gradations of risk (e.g. high medium low)
- A deficiency in the current NIST/FISMA regarding measurement and enforcement needs to be addressed in the SDT process.
- Address key challenges identified with current CIP: (e.g. piecemeal approach, not protecting assets needing protection; gaming; all or nothing; loss of asset, integrity/misuse, etc.)
- Address both the physical protection issues and the cyber protection issues, separately or not.
- Assume all outside an entity's direct control should be treated as a un-trusted connection.
- Seek to develop more guidance and less modification of standards as an approach.
- Address CIP 2 R2 so that it doesn't drive people towards the physical assets.
- Taking a cyber view should not preclude a physical view.
- Where possible, build on the existing work and research, models etc. E.g. Build upon MITREs cross walk to the control families.
- Focus on a shared view of the outcome that can capture all the attack vectors to make sure they have been assessed and have minimum security controls that we have not addressed in CIP.

Comments on Considerations

- First consideration bullet is a given? Yes, but may help to restate.

The SDT members agreed they were not yet prepared to proceed with the approaches suggested by Michael Winters. Some suggested further clarification of what was meant by "functional" or "systems" approaches to 002. After further discussion, the SDT agreed that a helpful next step would be to produce two strawman drafts of a revised CIP 002 based on the work to date. One would be prepared by Jackie Collett & John Lim and another would be prepared by Bill Winters and Kevin Perry with assistance from interested SDT members. These would be distributed in advance of the March meeting and form the basis for the agenda in Orlando.

Jay Cribbs proposed that the SDT ask the two teams to each produce a strawman CIP 002 in order to ground the discussion and move it forward. The members comments are set out below:

- Could we produce a current single strawman CIP- bring back a CIP 002?
- Fundamental question? Are we going to produce a set of documents codified as standards that are risk-based or traditional requirements based approach?
- Risk based approach deals with asset selection and how to apply controls to mitigate the risks. Depends on the organization's appetite for risk
- CIP 002 is risk-based is to identify assets then apply requirements. No risk-based decision making after that, just comply with requirements.
- Application of security measures takes a risk based vs. requirements approach. How do we merge those two.
- How to apply requirements to a risk based model to security controls?
- Going forward, continue the requirement-based approach or head in another direction.
- Unless the SDT develops a performance-based/requirement-based standard, it is not a NERC standard- would violate FERC order.
- "Risk based requirements?" Focus session on CIP 002. And a focus session on approaches to integrate the 2 models.
- Is it possible? Mandated that the SDT explore this.
- Audit process- subjective process. Deficiency of model.
- If we are going to produce requirements without a risk assessment.
- CIP 002 is risk based but requirements verified for
- Words say risk based but in practice it is not a risk assessment.
- Is there SDT consensus on a risk based approach?
- We should be taking a risk-based controls approach to the development of requirements. How can we craft requirements that include a risk basis?
- Opposite of one size fits all. Require you use a risk-based approach.
- We have a set of requirements that map to risk levels. For a given asset at a given location assigned a level of risk, we know the expectations are, focus in on that requirement at that location.
- Comes out of our catalogue of requirements vs. controls
- Allows for gradations.
- Create a document that contains a control.
- Requirement that they select their own controls.
- In FISMA process you have the base line-
- Nothing to stop SDT- NERC 800-53. Then have requirement that you will select based on risk level, controls appropriate to the device.
- Is the key issue, how can we craft requirements that include a risk based approach?
- Looking a how to apply controls. May timeframe- how to identify systems. Can we get to the Workshop?
- That plus our approach to risk based controlled model integrates into requirements.
- Closing in nicely but not there yet.

- Don't get into constraints of the standards development process. Whether or not to embrace NIST standards. Try not to burden with procedural discussions.
- The current constraints may take things off the table. Whatever we proposed should be within the constraints.
- Catalogue- will have to be run through the ANSI process.
- Basic disagreement between 2 camps revolving around order in which things are done. Get rid of CIP 2 R2. Do this as part of the impact assessment. Jackie/John/John. Have to do the critical asset identification first even though we have talked about systems approach. If correct, need to resolve before.
- Need to test an approach. Do we want to test employ a risk based categorization methodology to assets and apply to levels?
- May need to gut CIP 2 R2 and replace with FIPS 199 categorization vs. selection process to figure out high, medium low based on something.
- Not just on identification of critical assets. Categorization of cyber assets based on function. Proposing that take the functions for the operation and reliability BES and based on functions, id assets providing those functions, categorize and identify connections with external systems.
- To move forward, SDT needs an education/briefing on what is a "systems approach"? Straw documents to drill down on that.
- Need another NIST briefing: little deeper than 101. 200 class on NIST 800-53. Lack of complete understanding of how those would apply.
- We are both talking systems and functions. Each team should identify and define what is meant by a systems based approach and identification of essential functions.
- What kind of documentation should be clearly described.
- Let's look at high-level requirements for CIP 002 that would support each approach.
- What are the functions that are essential to retaining the reliability of the BES?
- Some out there So.Cal Edison. NERC documents- 5 elements:, Supervisor Control of BES assets…… Critical Asset Identification Draft Posted.
- FISP 199 document- list all of the key considerations, run through categorization process. Look at the impact to the function that supports your mission. Not easy. Put together a strawman doc to illustrate this. Somewhat subjective. In control area easier than in the admin area. Specific functions that support reliability. That would lead us to new set or modified set of requirements.
- Proposals- map them over, or a new requirement, adopt the NERC 800-53. Simple in concept with the difficulty evaluating.
- "Defining the system"? may be more difficult than discussions suggest. Consider what the possible gaps in that process.
- 2 documents with strawman CIP 002- 1 based on bill/Kevin method other by John Lim et al. When we look at them both.

- Work with whoever is interested to respond to John Stanford's categorization process clarification.
- Address the mission of BES not just the entity.
- Control function- industry has a good idea. Some structure.
- List of asset types that have to be considered.
- Scott's list of 5- could spread across a number of entities. Comes down to functional entity. Formulaic language at the functional entity level.
- CIP 002 - tell an entity what to assess, here is how to assess and here is what comes out of the process.

VI. NEXT STEPS AND ASSIGNMENTS

A. Expert/Stakeholder SDT Workshop and MRC.

At the end of day two the SDT took stock of its progress and reviewed the schedule for both an cyber expert and stakeholder workshop and presentation to the NERC Members Representative Committee in early May, 2009. *(See Appendix # 4)* The SDT agreed it needed to have sorted out and developed a clearer understanding and agreement on the Phase II approach prior to presenting a substantive briefing to the MRC. As as a result the SDT agreed to seek to provide a short "progress report" to the MRC in May and seek to present a substantive briefing at their August, 2009 meeting. The SDT suggested scheduling the expert/stakeholder workshop in the early Summer.

SDT Comments

- Workshop- both inside and outside the industry. Bringing in peers at level of people from companies didn't make the cut. People consulting vendor, national lab, government, agencies, congress DHS. Community at large consider in the large direction.
- MRC- Maybe in August vs. May?
- When we get up in front of people, have to be ready to present.
- Provide a modest progress report.
- Concern about a mid April workshop and a May 1 MRC. May not be enough time to reflect on the workshop input and prepare a presentation for the MRC a couple weeks later.
- Do we tell the MRC there will be significant potential change in the standards? We will be applying the CIP standards to more assets than included now. Modify existing protections to provide less.
- Given the number of things that need to be protected- net will be cast wider.
- We need to consider before MRC, a concept of how this would be rolled out (timeline and transition plan) so as not to cripple the industry.
- Must be prepared to answer why additional provisions or tougher on some standards. Need to have something focusing on our mission that says why we are doing it.

- Mike Assante and Rick Sergel- high level responses to those kinds of questions.
- Workshop in May and get the August. Workshop right after MRC meeting. BOT meeting. In D.C.
- Know what the questions are. Difficulty closing the deal.

B. Drafting Assignments

The SDT agreed that a helpful next step would be to produce two strawman drafts of a revised CIP 002 based on the work to date. One would be prepared by Jackie Collett & John Lim and another would be prepared by Bill Winters and Kevin Perry, each with assistance from interested SDT members. These would be distributed in advance of the March meeting (by March 6) and form the basis for the agenda in Orlando.

C. Meeting Evaluation

The Team then evaluated the meeting:

What worked or were helpful?

- All of it - staff assistance. Productive session.
- Quality of discussion
- Things went incredibly well kept out of the weeds.
- Heartfelt kudos to the group. The Chair and Vice Chair are exceptionally pleased. Good discussions, not getting into fisticuffs. Respective working with each other trying to understand each other's point of view.
- SDT is coming together, during the last few hours light bulbs were coming on. Bounds checking introduced.
- Kudos to the good work of drafters--Jackie- John John, kudos- engineering angle. Good work.
- All can be used in a NIST like process. All selected for perspectives, no right /wrong answer.

What things to improve/ correct

- Going forward reconnect on SDT objectives

The SDT adjourned at 3:30 a.m.

Appendix # 1
Cyber Security Order 706 SDT — Project 2008-06
Draft Meeting Agenda
February 18, 2009 - 8 AM to 5 PM EST
February 19, 2009 - 8 AM to 5 PM EST
ICF, Fairfax VA

Proposed Meeting Objectives/Outcomes

- Receive updates on Phase I actions, TFE and VSL processes;
- Receive White Paper updates;
- Presentation of a Case Study on a FISMA Application;
- Review and refinement of Phase II principles;
- Develop a series of principles, propositions and approaches that can serve as a foundation for a strawman Phase II concept and guidance document; and
- Agree on next steps in the Workplan and assignments.

Draft Agenda

Wednesday	**February 18, 2009**
8:00 p.m.	Welcome and Opening Remarks- *Jeri Domingo-Brewer/Kevin Perry* a. Roll Call b. NERC Antitrust Compliance Guidelines c. Facilitator Review of January meeting and adoption of February 2-4, 2009 Meeting Summary and Revised January 7-9, 2009 Meeting Summary
8:10	Review of Meeting Objectives, Agenda and Meeting Guidelines- *Jeri Domingo and Bob Jones*
8:15	Organizational Issues and Review of Phase 1 and early Phase II Schedule- Stuart Langton ▪ Update on Phase 1 Workplan, February 2009 ▪ Overview of Phase 2 Workplan- February-June, 2009
8:30	Update on Technical Feasibility Exception (TFE) NERC Rules of Procedure Posting- *Scott Mix*
8:40	Update on VSL SAR for SDT and Implications for SDT 706
8:50	Overview of FERC Order and Steps to Date in the SDT Phase II Development Process- *Stu Langton*
9:00	Discuss and Clarify February 2 SDT Ranking and Refinement of Phase II Principles (Michael Winters)
10:30	*Break*
10:30	2nd Presentation and Discussion of the Phase II White Paper- Potential Applicability of NIST to CIP- *John Lim (with Jackie Collett, Scot Rosenberg, John Varnel)*
12:00	*Working Lunch (Return to plenary meeting at 12:45)*
12:45	2nd Presentation and Discussion of the Phase II White Paper- Potential Applicability of CIP to NIST, Bill Winters
2:15	Applying FISMA – Asset Categorization--A Case Study- *Jeri Domingo Brewer*
3:00	*Break*
3:15	2nd Review of Revised FISMA/CIP Strawman- Scott Mix
4:50	Summary of Day Two Outcomes and Review of Day Three Agenda
5:00	*Recess*
Thursday	**February 19, 2009**
8:00	Welcome and Agenda Review
8:10	Integration and NIST/FISMA Potential Applicability Discussion- Assumption and Principles
10:00	*Break*
10:15	Remaining "Tough Issues" Discussion *(to be identified)*

12:00	*Working Lunch*
12:45	Building a Phase 2 Strawman Concept and Guidance Document
2:45	*Break*
3:00	Building a Phase 2 Strawman Concept and Guidance Document- Continued
4:30	Assignments, Next Steps and Review of Work-plan
4:40	Meeting Evaluation--What Worked. What Needs Improvement
4:50	Review of SDT March meeting objectives
5:00	*Adjourn*

Appendix # 2
Cyber Security for Order 706 Standard Drafting Team and Attendees List
Project 2008-06 — CS 706 SDT
Fairfax, Virginia

Attending in Person – SDT Members

1. Jay S. Cribb	Information Security Analyst, Southern Company Services, Inc.
2. Scott Fixmer	Senior Security Analyst Exelon Corporate Security, Exelon Corp.
3. Gerald S. Freese	Director, Enterprise Information Security America Electric Power
4. Phillip Huff	Arkansas Electric Coop Corporation
5. John Lim	CISSP, Department Manager, Consolidated Edison Co.NY
6. David Norton	Policy Consultant, CIPEnergy Coporation
7. **Kevin B. Perry, Vice Ch.**	Director, IT-Infrastructure, Southwest Power Pool
8. Christopher A. Peters	ICF International
9. David S. Revill	Georgia Transmission Corporation
10.Keith Stouffer	National Institute of Standards & Technology
11.Michael Winters	Hydro One
12.William Winters	Arizona Public Service, Inc.
1. Roger Lampilla	*NERC*
2. David Taylor	*NERC*
3. Harry Tom	*NERC*
4. Scott R. Mix	*NERC*
5. Joe Bucciero	*NERC/Bucciero Assoc.*
6. Robert Jones	*FSU/FCRC Consensus Center*
7. Stuart Langton	*FSU/FCRC Consensus Center*

SDT Members Attending via Webex/Phone

1. Rob Antonishen	Ontario Power Generation
2. Jackie Collett	Manitoba Hydro
3. Tom Hoffstetter	Midwest ISO, Inc
4. Kevin Sherlin	Sacramento Municipal Utility District
5. Jonathan Stanford	Bonneville Power Administration
6. John D. Varnell	Technology Director, Tenaska Power Services Co.

SDT Members Unable to Attend

1 Jeri Domingo-Brewer	U.S. Bureau of Reclamation
3. Joe Doetzl	Manager, Information Security, Kansas City Power & Light Co.
3. Sharon Edwards	Duke Energy
4. Richard Kinas	Orlando Utilities Commission
5. Scott Rosenberger	Luminant Energy
6. Bryan Singer	Kenexis Consulting Corp.

Others Attending in Person

Jim Breton	ERCOT

Roger Fradenburgh	Netsecctech
Judy Fry	ICFI
Darren Highfill	ENERNEX
Sam Morrell	CERT
Farzaneh Tafreshi	ICFI

Others Attending via Webex/Phone

Chris Wright	
Dan Mishra	
David Batz	
Monica Coflin	
Karen Yoder	

Appendix # 3
NERC Antitrust Compliance Guidelines

I. General

It is NERC's policy and practice to obey the antitrust laws and to avoid all conduct that unreasonably restrains competition. This policy requires the avoidance of any conduct that violates, or that might appear to violate, the antitrust laws. Among other things, the antitrust laws forbid any agreement between or among competitors regarding prices, availability of service, product design, terms of sale, division of markets, allocation of customers or any other activity that unreasonably restrains competition.

It is the responsibility of every NERC participant and employee who may in any way affect NERC's compliance with the antitrust laws to carry out this commitment.

Antitrust laws are complex and subject to court interpretation that can vary over time and from one court to another. The purpose of these guidelines is to alert NERC participants and employees to potential antitrust problems and to set forth policies to be followed with respect to activities that may involve antitrust considerations. In some instances, the NERC policy contained in these guidelines is stricter than the applicable antitrust laws. Any NERC participant or employee who is uncertain about the legal ramifications of a particular course of conduct or who has doubts or concerns about whether NERC's antitrust compliance policy is implicated in any situation should consult NERC's General Counsel immediately.

II. Prohibited Activities

Participants in NERC activities (including those of its committees and subgroups) should refrain from the following when acting in their capacity as participants in NERC activities (e.g., at NERC meetings, conference calls and in informal discussions):

- Discussions involving pricing information, especially margin (profit) and internal cost information and participants' expectations as to their future prices or internal costs.
- Discussions of a participant's marketing strategies.
- Discussions regarding how customers and geographical areas are to be divided among competitors.
- Discussions concerning the exclusion of competitors from markets.
- Discussions concerning boycotting or group refusals to deal with competitors, vendors or suppliers.

III. Activities That Are Permitted

From time to time decisions or actions of NERC (including those of its committees and

subgroups) may have a negative impact on particular entities and thus in that sense adversely impact competition. Decisions and actions by NERC (including its committees and subgroups) should only be undertaken for the purpose of promoting and maintaining the reliability and adequacy of the bulk power system. If you do not have a legitimate purpose consistent with this objective for discussing a matter, please refrain from discussing the matter during NERC meetings and in other NERC-related communications.

You should also ensure that NERC procedures, including those set forth in NERC's Certificate of Incorporation and Bylaws are followed in conducting NERC business. Other NERC procedures that may be applicable to a particular NERC activity include the following:

- Reliability Standards Process Manual
- Organization and Procedures Manual for the NERC Standing Committees
- System Operator Certification Program

In addition, all discussions in NERC meetings and other NERC-related communications should be within the scope of the mandate for or assignment to the particular NERC committee or subgroup, as well as within the scope of the published agenda for the meeting.

No decisions should be made nor any actions taken in NERC activities for the purpose of giving an industry participant or group of participants a competitive advantage over other participants. In particular, decisions with respect to setting, revising, or assessing compliance with NERC reliability standards should not be influenced by anti-competitive motivations.

Subject to the foregoing restrictions, participants in NERC activities may discuss:

- Reliability matters relating to the bulk power system, including operation and planning matters such as establishing or revising reliability standards, special operating procedures, operating transfer capabilities, and plans for new facilities.
- Matters relating to the impact of reliability standards for the bulk power system on electricity markets, and the impact of electricity market operations on the reliability of the bulk power system.
- Proposed filings or other communications with state or federal regulatory authorities or other governmental entities.
- Matters relating to the internal governance, management and operation of NERC, such as nominations for vacant committee positions, budgeting and assessments, and employment matters; and procedural matters such as planning and scheduling meetings.

Any other matters that do not clearly fall within these guidelines should be reviewed with NERC's General Counsel before being discussed.

Appendix # 4

Cyber Security Order 706 SDT —Project 2008-06

JAN.-JUNE 2009 DRAFT SDT SCHEDULE

SHORT TERM 2009 SDT SCHEDULE DRAFT CRITERIA

- Follow the ANSI standard development process but use creative ways to efficiently secure input from the industry on emerging concepts and approaches to the CIP standards.
- Seek creative ways to get advice and input to the SDT from experts in cyber security.
- Seek creative ways to get focused input from industry stakeholders.
- Take advantage of input opportunities from related NERC committees that will be meeting in the first half of 2009 (e.g. working with the NERC Members Representative Committee, CIPC, BOT, and industry committees such as the Electricity Sector Coordinating Council, etc.)
- Seek, as soon as possible but no later than late Spring, 2009, to establish a consensus on the way forward for the SDT in its efforts to revise the CIP standards.
- Track any follow up to the "Securing Cyberspace for the 44th Presidency" report of the Commission on Cybersecurity for the 44th President.

SDT DRAFT SCHEDULE-JANUARY-JUNE, 2009

OVERVIEW

- **7 SDT FACE-TO-FACE MEETINGS**
- **MULTIPLE SDT SUBGROUP AND SUBCOMMITEES WEBEX MEETINGS**
- **1 CYBER EXPERT WORKSHOP (MARCH 10 OR 11, 2009)**
- **1 NERC CIPC PRESENTATION? (FEB. 9, 2009)**
- **INDUSTRY COMMENTS ON CIP 002 WHITE PAPER** (APRIL 17-JUNE 3)
- **1 NERC MEMBERS REPRESENTATIVE COMMITTEE, MAY 1, 2009**
- **OTHER MEETINGS?**

SDT DRAFT SCHEDULE-JANUARY-JUNE, 2009

1. January 7-9 SDT Meeting, Phoenix, AZ ½ / 1/½ day format. Wed-Friday

- Review of Technical Feasibility Exceptions white paper
- Review of Industry Comments on Phase 1 products- Establish and convene small groups
- Review of Phase 2 White papers

January 15 Webex meeting(s)

- Small group draft responses to industry.

- Phase 2 drafting concept group?

January 21 Webex meeting(s)

- Small group draft responses to industry.
- Phase 2 drafting concept group?

2. February 2-4 SDT Meeting, 2009, Phoenix, AZ, ½ / 1/½ day format. Mon-Wed.

- Review of Industry Comments on Phase 1 products and Proposed revisions and adoption of Phase 1 products.
- Review of Phase 2 White papers and Testing of a Phase 2 CIP 002 Concept going forward

February 9, 2009, CIPC Meeting- Update on SDT Progress and Input?

3. February 18-19, SDT Meeting Boulder City, NV

- Review of Phase 2 White papers and Adoption of a Phase 2 CIP 002 Concept for review by experts and stakeholders

February 25, Webex meeting(s)

- Development of Phase 2 CIP 002 Workshop for review by experts and stakeholders

4. March 10-11, SDT Meeting 2009, Tampa, FL, 2-day format

- **Invited Cyber Security Experts join SDT in a workshop** to provide expert feedback to draft CIP 002 concept.
- Further SDT refinement of the CIP 002 proposed concept

March NERC Balloting on Phase 1 Products

March 18, Webex meeting(s)

- Phase 2 drafting concept group?

5. April 14-16, SDT Meeting, Charlotte NC, ½ / 1/½ day format. Wed-Friday

- Continue review and refinement of 002 concept
- Adopt White Paper on CIP 002 concept for Industry Comment

Industry Comment Period on White Paper- 45 days (April 17- June 3)

*May 1, **NERC Member Representative Committee**, Presentation of the Phase 2 CIP 002 Approach for MRC input. (Agenda item, Possible Workshop?)*

6. May 13-14, SDT Meeting, Dallas TX, 2-day format

- Respond to MRC input and further SDT refinement of the CIP 002 proposed concept and SDT CIP roadmap.
- Organize SDT in subcommittees to draft revisions to CIP 003-008 or to address key issue areas.

Early June, Webex meeting(s)

- SDT subcommittee meetings to review and draft responses to Industry comments on the CIP 002 concept.

7. June 17-18, SDT Meeting, Location TBD, 2-day format

- Review Subcommittee responses to Industry comments on 002 approach
- Charge subcommittees and conduct organizational meetings
- Subcommittees meet to draft revisions to CIP 003-008

June, 2009 Webex meeting

- SDT Subcommittee meetings

July-December, 2009- SDT and subcommittees meet and continue CIP drafting

2nd DRAFT PHASE 2 ROADMAP APPROACH ASSESSMENT CRITERIA

(Presented, Revised and Added to by SDT in its review on November 14, 2008)

1. The approach is consistent with the SDT purpose statement and is responsive to the FERC 706 directives and the SAR.
2. The approach is achievable given the SDT schedule and workplan.
3. The approach does most to advance and enhance cyber security in the BES.
4. The approach helps the SDT address the foundational issues with the current standards.
5. The approach is capable of implementation.
6. The approach is capable of improving compliance.
7. The approach helps protect the current investments and wherever possible builds on what has already been done.
8. The approach helps to identify and mitigate risk on an ongoing basis.
9. The approach balances a "systems" orientation with a "facilities" orientation to asset protection.
10. The approach is capable of being extended into related interests by others (distribution, AMI, Smart Grid, etc.).
11. The approach enables the industry to provide the appropriate level of security (i.e. not over securing nor under securing the BES cyber assets).
12. The approach allows for discrimination among and targeting the various types of infrastructure that support the BES

Appendix #5 Guiding Principles Ranking and Comments

1. **~~(8)~~ A mapping ~~similar~~ to NIST 800-53 ~~Appendix G~~ to CIPs will help quantify and assess the gap, if any.**

Acceptability Ranking Scale	*4 = acceptable, I agree*	*3 = acceptable, I agree with minor reservations*	*2 = not acceptable unless major reservations addressed*	*1 = not acceptable*	*Avg.*
2-2-09 rank	**11**(10/1)	**2**	**2**	**0**	**3.6 of 4**
2-18- rank	**13(**11/2)	**1**	**0**	**0**	**3.9 of 4**

SDT Comments 2-18 before ranking

- "Similar" = almost the same as? Matrix with other standards. Mapping of 53 to other standards not including mapping to NERC CIP standards. See the MITRE document.
- We do have some "mappings" 53 and NERC CIPs, not in same format as appendix G. DOE has done one as well.
- Michael Winters suggested the principle is to build on work already done, to highlight possible gaps in the CIP standards.
- 800-53 part of a guideline. CIP is a standard. Needs to be a high level piece.
- Quantify the gap is the essence of the principle. Not suggesting adopting 900-53. It can be a tool to identify the size of the problems/gaps.
- Clarification for those thinking 800-53 isn't a standard vs. guidelines. FIPS 200 is the standard. Meet the 800-53 guideline.
- Separate guidelines changes are easier than changing standards.
- There isn't a mapping in the Version 3 IPP document.
- Need to analyze the gaps first. We may find there is not be a gap after all.

2. **~~(2)Resist creating exception-based standards to accommodate every possible business and operations scenario. Instead~~, Create ~~clear~~ non-proscriptive standards and employ a technical exception/compensating ~~controls reporting~~ documentation and guidance process to ~~that~~ accommodates ~~deviations~~ variations.** (Resist creating exception based standards to accommodate every possible business and operations scenario)

Acceptability Ranking Scale	*4 = acceptable, I agree*	*3 = acceptable, I agree with minor reservations*	*2 = not acceptable unless major reservations addressed*	*1 = not acceptable*	*Avg.*
2-2-09 rank	**11**(10/1)	5	1	0	3.6 of 4
2-18- rank	**10** (7/3)	**5** (4/1)	**0**	**0**	**3.7 of 4**

Michael Winters introduction comments

- TFE has a guidance peer process. Feedback loop for mitigate at the regional or other levels. Not just a reporting requirement.
- First sentence is the intent- can delete but remember.
- This principle suggests we write requirements/controls at a higher level so we don't get into

all the details? Bottom line? Make sure you have something at the end. Not just a reporting but a mitigating process.

- In terms of "What vs. how." This principle suggests we avoid the how in our standards.

SDT Member Comments and suggestions before ranking

- Does "clear"= prescriptive? Should avoid the how. Use "Non-prescriptive."
- What is the "guidance" process? Reporting all of our compensating controls?
- SDT could write standards that provide for something like a TFE when you can't do what the standards require you to do. From a compliance standpoint- must do what is in the standards. TFE, meet intent of standard, doing something and explain how you are handling it to meet e.g. 75% level and then address the 25% mitigation measures.
- "Create non prescriptive standards and utilize a defined TFE … to accommodate deviations or variations.
- What is a guidance process? Another guideline? This is the feedback loop.
- Puts compliance into a role of consultants/education. Is this allowed by current procedure or acceptable to industry?
- Audits- make recommendations- entity respond to it. NERC compliance- possible violation goes to region to enforcement component- look at evidence, and make a final decision. Then an alleged violation and a discussion about what can be done. Registered entity can post alongside the violation their position.
- Federal agencies use an inspector generals- process? GAO letter of management.
- "Variance" vs. deviation.

~~3.~~ ~~(3)~~Use a consistent risk-based model to classify ~~all~~ cyber assets ~~(i.e. facilities, sites, physical perimeters) (i.e. not cyber assets at this point)~~ as critical/high impact, moderate impact, low impact. ~~This will allow for expansion of standards beyond Critical(i.e below 100 kV – accommodates AMI, Dx automation, etc). Classifying at the physical perimeter level~~ This would allow for expansion of the standards beyond critical. ~~different classifications to exist within a building or at a site (e.g. control room, computer rooms, dev and testing rooms, and back-office at a control centre).~~

Acceptability Ranking Scale	*4 = acceptable, I agree*	*3 = acceptable, I agree with minor reservations*	*2 = not acceptable unless major reservations addressed*	*1 = not acceptable*	*Avg.*
2-2-09 rank	**9**(8/1)	6	2	0	3.4 of 4
2-18- rank	**11** (9/2)	**5** (3/2)	**0**	**0**	**3.7 of 4**

Michael Winters introduction comments

- Consistency of application is intent and also levels of graduation- high medium and low.

SDT Member Comments and suggestions before ranking

- Strike the classifying sentence? Yes.

- May be headed down the same problematic path. This is an "engineering frame of reference." "Consistent risk based model"? "Holy grail" Any out there? What is important is the function in terms of reliability. Function needs to be preserved. What do we need to know to run the system in reliable fashion. Looked at applications. From SCADA to EMS to generation dispatch. They run on these boxes and use this data on a storage area network. E.g. hurricanes.
- Working group of CIPSE identifying critical asset guidelines. Many came to same conclusion. Functional and impact analysis based on loss or compromise not just of machines but of functions is key. Its draft will be out next Tuesday.
- They identify functional analysis in 4 classes of systems: transmission, generation, control centers and special systems dealing with load shedding etc. (most important at last 2). Criticism- guideline doesn't support the language in the standard? OK, but it is just a non-binding guideline. NERC has told FERC, that document will be made available to this drafting team. Are there things in guideline that should be in the standards in version 3?
- Functional analysis is a good candidate for that. CIPSE agenda packet released March 3. Will send a link to the SDT.
- Functional analysis- important for ERCOT. Identify systems that were critical for situation awareness for BES in Texas. Have control systems but 4000 centers, control systems. Don't own assets. We can't declare it critical unless we are the asset owner. Provide guidance. No authority to do this. We need help.
- We didn't call it a functional model. We didn't get at application side. They are the key to maintaining both reliability and security. Need to address in Phase II.
- Function vs. application: If focus on function vs. assuming a computer involved. Apply first step where there are not computers. E.g. control centers provided this before computers involved. Computers became important because they have performed critical functions. There are still non-computer systems in place.
- Intent is to close gap on the systems we leave out. Everything having to do with controlling the BES. Everything gets a classification and a set of controls and is consistent from entity to entity.
- Aren't these cyber security standards to protect computer systems?
- Classify "all"
- Applications-
- Needing feeds from other places, e.g. ERCOT's comment. Reliability coordinators role?
- Transmission, congestion studies each year. Growth expected. Critical today may not be tomorrow. Each year CA determination may be different. Will be very dynamic. Like more authority to get things done. FERC order 706- reliability coordinator role.
- Focusing on applications has been a challenge. What are mission critical systems? E.g. Weather systems are critical with wind power. What systems required to functionality.
- Identifying cyber assets high medium low. Related to threat profile in FISPE 200- mission focused. Not individual assets. Mission high.

- Placing at end. These principles are driven by the following:……
- Violation risk factors- single risk factor. May have to assign a high? That may depend on how draft the standards.
- Risk factor- what impact will failure to comply have on the reliability of the BES- high impact- e.g. cascading failures. Impact cyber security if asset is compromised. Different assessment. Will there be confusion about the similarity.
- High medium low threat profile organization

~~4.~~ ~~(4)~~An entity's cyber asset classification is ~~would be open~~ subject to scrutiny by the compliance enforcement authority and ~~ERO~~ and applicable regulator(s). ~~The extent of scrutiny to be defined and tightly controlled.~~

Acceptability Ranking Scale	*4 = acceptable, I agree*	*3 = acceptable, I agree with minor reservations*	*2 = not acceptable unless major reservations addressed*	*1 = not acceptable*	*Avg.*
2-2-09 rank	**4**(3/1)	11	2	0	3.1 of 4
2-18- rank	*No rank*	*Agreed to list as a*	*fact or assumption*	-	-

Michael Winter's introduction comments

- Intent is to have a review to make sure interpretation is not incorrect. Regional entities are the front line for compliance today.
- When auditors show up an entity can show a risk-based assessment.
- Reliability coordinator review is by implication in principle #3 in terms of consistent application.

SDT Member Comments and suggestions before ranking

- Roger Lampilla noted what has been learned in compliance through five CIP training classes. First 13 requirements. 8 regions manager of compliance. On CIP 002, if you say you will id high medium low. They will ask the auditor to suggest what category it is. If they don't see an asset that is not on the list you will be asked to run through methodology to explain not on the list. Hearing from the regional audit staff.
- Balance to check in the first one. Demonstrate you have applied the method consistently.
- Regional entity- "compliance enforcement authority"
- Regional entity- sounds like an audit? This is on the back end in #4.
- Asset classification is a requirement? Is this different than what we have today in the audit process?
- Principle #3 is the requirement while principle #4 is the application. Intent is external review component.
- Add cyber asset? Do away with physical basis. Stop thinking of existing CIP standards and approach. Danger we will lock in by default.
- Is this part of compliance process or part of identifying assets? Which is it?
- "Authority" may be giving some heartburn? Broaden to external review?
- "auditable"? Is this the intent? Then "sanctionable". Scope of statement extends to that.

- That is an extreme. Intended to suggest a more collaborative peer review process
- Scope of SDT is to write requirements. We need to write standards that can be audited.
- The scrutiny this draft principle calls for already exists. Authority to challenge and refute
- Take this out. It is a given. It is awkward at part of #3
- Include as a statement of fact or assumption at the bottom or to introduce the principles.

5. ~~(7)Use~~ Consider **the minimum security controls for high, moderate and low within NIST 800-53 to help model the CIP** ~~controls~~ requirements **for each level.** ~~**Address any gaps at the same time but keep the same CIP002 to CIP0XX general format. Re-arrange existing CIPs as previously discussed within SDT to make them flow more effectively. Industry knows this format, is building policies and programs around it, has commented on it and has voted on it.**~~

Acceptability Ranking Scale	*4 = acceptable, I agree*	*3 = acceptable, I agree with minor reservations*	*2 = not acceptable unless major reservations addressed*	*1 = not acceptable*	*Avg.*
2-2-09 rank	**5**(4/1)	8	4	0	3.0 of 4
2-18- rank	**9**	**6** (3/3)	**0**	**0**	**3.7 of 4**

Michael Winter's introduction comments

- Looking at principle not adopting the FIPS/NIST framework.
- High medium low= impact to operation and reliability of BES. That is how you would view cyber security.

SDT Member Comments and suggestions before ranking

- High, moderate, low? Affected how we talk about functions, asset by asset vs. utility by a whole? What about multi-site contingency. Breaking down requirements based on facility.
- OK if doing an organizational threat profile. These are cyber controls which assume the systems have been.
- More risk there is the BES, higher level of protection on the asset.
- Show me the metric--this will be difficult.
- Risk assessment methodology consultants. As you develop your priorities. Impact evaluation criteria- here is what is most, less and least important. What does the high mean? Based on everyone's priorities for the BES. Will reveal how to grade and evaluate,. What are some of those factors. Security categorization is the first step of the risk management assessment- risk in terms of mission. Shared mission re BES: system wide services that need to be assured. Keep in mind thresholds. What is high? Fundamental piece missing from the puzzle.
- Fits in terms of the functional discussion.
- Bring in people to test the nature of the functions- systematically, data flows and end to end.

6. ~~**(6) Any cyber devices that are not within or on the perimeters, including telecom, are not part of the CIPs – the CIPs remain perimeter-based where devices on and within the perimeter are protected and everything beyond is considered untrusted.**~~

Protection of the communication devices outside to the electronic security perimeters, are out of scope.

Acceptability Ranking Scale	*4 = acceptable, I agree*	*3 = acceptable, I agree with minor reservations*	*2 = not acceptable unless major reservations addressed*	*1 = not acceptable*	*Avg.*
2-2-09 rank	**4**(3/1)	6	6	0	2.9 of 4
2-18- rank	**10**	**3** (1/2)	**3** (1/2)	**0**	**3.7 of 4**

Michael Winter's introduction comments

- Intent was to exclude- what is not in.

SDT Member Comments and suggestions before ranking

- JL: Establish zones of trust and treat cyber communication devices and data accordingly.
- Worry about serial lines? Routable protocols. It is a hole we have to close. FERC 706 doesn't talk about serial lines. If not.
- General principle? Zones -Define by governing bodies.
- We have 2 zones. Direct control and stuff you don't. E.g. ATT wire circuit. Data in motion is the asset to protect.
- Sheet- need to protect the BES.
- What is the basis of "trust"? Must define this. Info system perimeter that is not technology specific is better?
- What are the zones and levels of trust- and how to treat them accordingly. Certain devices we trust and treat differently. Principle is one of different level of trust.
  After ranking
- Split into two principles: Communication devices out of scope; and Transit data as a core principle.

7. It is imperative to protect the integrity of data throughout its transit.

Acceptability Ranking Scale	*4 = acceptable, I agree*	*3 = acceptable, I agree with minor reservations*	*2 = not acceptable unless major reservations addressed*	*1 = not acceptable*	*Avg.*
2-18- rank	**13** (12/1)	**1**	**2**	**0**	**3.7 of 4**

Comments following ranking

- 2: "imperative" vs. "important"
- 2. Don't like "integrity"

David Revill proposed the following principle for SDT consideration:

8. **CIP requirements should consider the unique locational characteristics (e.g. substations, data centers, generation plant) and functional capabilities of the cyber assets to be protected.**

Acceptability Ranking Scale	*4 = acceptable, I agree*	*3 = acceptable, I agree with minor reservations*	*2 = not acceptable unless major reservations addressed*	*1 = not acceptable*	*Avg.*
2-18- rank	**11** (8/3)	**5(**4/1)	**0**	**0**	**3.7 of 4**

SDT Comments before ranking

- Consider the application of asset-class specific requirements.
- The requirements need to consider the environment and class of the cyber asset
- Suggest- standards to "guidance"?
- Focus on functionality of the system. E.g. fire wall and a server.
- System functionality?
- Different assets
- Highlights different between an asset vs. computer focused approaches.
- Asset classes envisioned by current CIP.
- Are these mutually exclusive? Physical security requirements of different when
- Asset specific functionality- device. The characteristics of the cyber asset.
- Protection on devices- various ways to place anti viruses to protect on router itself or in front of it.

Delete Old #7 ~~(5)As part of a power system (non-corporate IT) inventory of cyber assets, add an attribute to each device that associates the high/moderate/low classification of the physical perimeter/facility/site within which it resides. Apply security controls based on the classification.~~

~~*Acceptability Ranking Scale*~~	~~*4 = acceptable, I agree*~~	~~*3 = acceptable, I agree with minor reservations*~~	~~*2 = not acceptable unless major reservations addressed*~~	~~*1 = not acceptable*~~	~~*Avg.*~~
~~2-2-09 rank~~	~~**4**(3/1)~~	~~6~~	~~7~~	~~0~~	~~2.8 of 4~~

Michael Winters comment:

- Deleted as this is already covered in Principles#3 and Principles#5.

9. ~~**(1)Protect critical/high, moderate, low cyber assets that are within scope of NERC CIPs – not just the Critical Cyber Assets – but to different degrees of controls depending on their classification.** [NTD: this is the natural progression of #5. The minimum security controls have been defined by level. This principle now states that those controls should also be implemented. Note that 'low' impact may stop at taking the CIP-002 inventory with no other controls required – if that is what the SDT decides.]~~

~~*Acceptability Ranking Scale*~~	~~*4 = acceptable, I agree*~~	~~*3 = acceptable, I agree with minor reservations*~~	~~*2 = not acceptable unless major reservations addressed*~~	~~*1 = not acceptable*~~	~~*Avg.*~~

~~2-2-09 rank~~	~~**3**(2/1)~~	~~8~~	~~6~~	~~0~~	~~2.8 of 4~~

Michael Winter's introduction comments

- Intent of principle: protect all of your assets #5 defined levels and controls.
- This is an implementation principle and should be deleted as a guiding principle.

Appendix # 6

Risk Management Framework and Protected Cyber Asset Identification A Concept

Kevin Perry, February 17, 2009

Desired Outcome

The Responsible Entity shall produce at least annually through an applied risk assessment methodology, a categorized list of Cyber Assets that are to be protected per the requirements of the CIP stan dards. The categorized list shall reflect the importance of the Cyber Asset and the potential risk to the reliability of the Bulk Electric System in the event the Cyber Asset is lost or compromised.

Background

The current risk management approach requires a Responsible Entity to first identify its physical assets (typic ally control centers, generation plants, and transmission substations) that are essential to the reliability of the Bulk Electric System. Once the Critical Assets are identified, the Responsible Entity then identifies the Cyber Assets essential to the operation of the Critical Asset. There has been confusion throughout the industry as to what constitutes a Critical Asset and the FER C has required additional guidance to be provided in this regard. The FERC has also expressed concern that N-1 redundancy is not a valid criterion for Critical Asset selection.

While not all Cyber Assets pose the same level of risk, it is reasonable to assume that any Cyber Asset capable of performing a supervisory control action against the Bulk Electric System or providing visibility of the Bulk Electric System conditions should be protected to some degree. Likewise, any Cyber Asset providing essential functions or data to the control system should alsobe protected based upon the potential risk. It is reasonable to assume that while the loss or compromise of a single Cyber Asset may have no meaningful impact on the Bulk Electric System, the loss or compromise of some number of these Cyber Assets with common points of vulnerability could rise to become a significant impact to the Bulk Electric System. It is also important to remember that the Bulk Electric System is dynamic and that system conditions change constantly. What is not critical today may well be critical tomorrow due to such factors as outages an d extreme weather.

By relying on an engineering approach and focusing on the physical facilities that make up the Bulk Electric System, there is a real chance that potentially risky Cyber Assets will be overlooked or ignored. A systems approach that focuses on the functions and interaction of Cyber Assets and not the physical facility would better serve the reliability of the Bulk Electric System.

A Concept

This concept proposes that a systems approach to identifying and categorizing Cyber Assets thatmust be prot ected per the CIP standards can be used that does not rely upon initially determining the criticality of the physical asset where the Cyber Asset happens to reside. While not focusing on the physical asset as a discriminator, this concept recognizes the levels of risk

posed by individual Cyber Assets and recognizes the interconnection, interdependency, and commonality of Cyber Assets. This concept builds upon the NIST risk management framework by categorizing Cyber Assets as low, moderate, or high risk and applying security controls appropriate to the Cyber Asset and its categorization.

An Approach

This concept proposes an iterative approach to identifying and categorizing Cyber Assets that perform or support supervisory control and/or visibility of the Bulk Electric System. The approach starts out identifying the Cyber Assets and later applies the risk analysis to categorize the systems.

The first step is to identify the Responsible Entity's Cyber Assets that either perform a supervisory control function or provide operational visibility of the Bulk Electric System. This should result in a list of the SCADA/EMS systems (including operator consoles) in the control centers along with plant control systems, substation RTUs, and digital protective control devices;basically any thing that can open or close breakers, move generation, or present information necessary for the operational control of the Bulk Electric System.

The next step is to identify the adjacent connected Cyber Assets and determine which either provide a support function (such as database management) or provide data (such as an ICCP node) essential to the operation (reliability functions only) of the control system. In this scenario, a Cyber Asset that receives data from the control system (such as a Pi Historian) would not be identi fied as an essential system unless it also provided essential data to the control system.

The iterative process is continued until the rest of the Cyber Assets that are ultimately essential to the reliabilit y functions of the control system have been identified. In the iterative process, the Responsible Entity may find a Cyber Asset owned or operated by another Responsible Entity as essential. An example would be an ICCP node at a Balancing Authority providing SCADA data to the Reliability Coor dinator. In this example, the Reliability Coordinator SCADA/EMS relies upon the data provided by the Bala ncing Authority ICCP node to perform its own reliability functions. The Balancing Authority might not rely upon any data received by its own ICCP node and therefo re might not have identified the Cyber Asset as essential. The Balancing Authority would be obligated nonetheless to accept the declaration of essential system from the Reliability Coordinator and continue the iterative process, eventually working its way back to its own SCADA /EMS system.

Once all essential Cyber Assets have been identified through the iterative process, the Responsible Entity would complete the identification process by establishing the Electronic Security Perimeters and identifying any additional Cyber Assets within. The Responsible Entity would then c ategorize each Cyber Asset based upon its potential impact to the reliability of the Bulk Electric System shoul d it be lost or compromised. In the instance of example where the Reliability Coordinator identified a Cyber Asset belonging to the Balancing Authority as essential, the two par ties would need to coordinate the categorization of that Cyber Asset.

Assuming the NIST framework is used as the categorization model, each asset would be categorized as low, moderate, or high impact, depending upon its potential risk to the reliability of the Bulk Electric System. In an ideal world, all entities would have identified similar categorization criteria. In reality, it may be necessary to define or at least review and approve the categorization thresholds based upon NERC-wide or Regional criteria.

Protection Levels

Under the NIST framework concept, the Responsible Entity would apply a minimum set of cyber security controls to all Cyber Assets identified in the discovery process. The minimum control set would be tailored to the type of Cyber Asset. In other words, a firewall or other layer three communication device would have a different set of security controls, appropriate to its configuration and function, than a conventional server or workstation. Likewise, the security controls for a plant control system would necessarily be different from those applied to an RTU.

Moderate risk Cyber Assets would apply additional security controls on top of the minimum set applied to all systems. High risk Cyber Assets would apply yet more security controls in recognition of the potential risk.

Impact to the Responsible Entity

If the Responsible Entity's existing Critical Cyber Asset identification program was properly designed, the Responsible Entity should identify few if any additional High Risk Cyber Assets. Therefore, the sunk costs of protecting the Critical Cyber Assets would not be expected to be lost.

The implementation plan could be designed in such a manner to allow a phased implementation of the security controls for the newly identified essential systems taking into consideration the desire to protect the higher risk systems more quickly.

The minimum set of security controls that apply to all identified systems would be expected to be the normal good security practice controls appropriate for the Cyber Asset, such as patch and password management. Whether additional controls, such as personnel risk assessments, detailed training, and offline test systems are necessary is still to be determined.

Summary

In the end, this concept recognizes that system protection should take risk into consideration while approaching the subject from a systems perspective, not an engineering perspective. The concept helps ensure that all Cyber Assets with a potential risk to the Bulk Electric System are protected commensurate with the level of risk by identifying a uniform approach to Cyber Asset identification. It eliminates the confusion introduced by a lack of transmission system information, especially on the part of the merchant generators and protects the investment already made by the Responsible Entities.

Appendix #7 NIST/CIP Integration Overview- Bill Winters

NIST/CIP Integration Overview

Moving toward public/private adoption

William Winters
Arizona Public Service

Leverage work begun by NIST and MITRE

- **Significant effort has already been done to map CIP and NIST and provide the overlay groundwork**
  - **Applying NIST SP 800-53 to Industrial Control Systems** http://csrc.nist.gov/groups/SMA/fisma/ics/documents/papers/Apply-SP-800-53-ICS-final-22Aug06.pdf
  - **Addressing Industrial Control Systems in NIST Special Publication 800-53** **http://csrc.nist.gov/groups/SMA/fisma/ics/documents/papers/ICS-in-SP800-53_final_21Mar07.pdf**
- SDT team work with these organizations to further refine NIST 800-53 ICS related BES controls

Heavy Integration

- Replace CIP 002 with NERC versions of FIPS 200 and FIPS 199
  - FIPS 199 **Standards for Security Categorization of Federal Information and Information Systems**
  - FIPS 200 **Minimum Security Requirements for Federal Information and Information Systems**
- Replace CIP 003-009 with 800-53 and 800-53a
  - Modify 800-53 controls with ICS Utility BES operation elements
  - Modify 800-53A accordingly
- Common categorization process will provide risk assessment methodology that is consistent across industry.
- Establish low medium and high level controls that correspond to component impact on BES operation
  - Regardless of level of impact on BES, systems used in operation and control of BES will have minimum CIP cyber security standards

Moderate Integration

- Update CIP 002 to include a Categorization Standard (FIPS 199 analog)
- Update CIP 003-009 with 800-53 elements to address gaps identified in 706
- Example: MITRE_NIST_Example_Augmentation_CIP-005.pdf
  - Presented by Keith Stouffer at SDT Meeting 10/21

Light Integration

- Update CIP 003-009 requirements to align more explicitly with 800-53 controls
- Draw on 800-53 controls to fill in gaps identified in 706
- Use NIST documents as guidance references throughout CIP

Migrating towards heavy

- SDT Team Work with NIST (and MITRE?)
  - update and refine 800-53 (eg. 800-53-rev3) with ICS Utility BES operation focus
    - Use NIST/MITRE comparison overlay as starting point
  - Refine related guidance documents
  - Develop new guidance documents as necessary
- Start with light integration
  - Begin to develop direct linkage from CIP to NIST
    - Utilize NIST documents for guidance, particularly 800-53 controls that directly map to existing CIP standard
  - Break out in to CIP standard subgroups
    - Iterative process
    - NIST provide guidance on approach
  - Possibly implement categorization standard in CIP 002 at this stage
- Move to medium integration
  - Implement categorization standard in CIP 002
  - CIP standards previously mapped to 800-53 for guidance updated to specify 800-53 as standard
  - Continue to work with NIST in refining 800-53 and guidance documents
- Finish with full adoption of NIST standard 800-53
  - Industry collaboration refinement of 800-53 complete
  - Guidance documents complete
  - CIP 002 specifies requirement to use 800-53

DRAFT 01/29/09

INDEPENDENT ASSESSMENT OF FISMA AND RELATED NIST DOCUMENTS FOR ADOPTION FOR ELECTRIC SECTOR CRITICAL INFRASTRUCTURE PROTECTION.

William Winters, Arizona Public Service
*(Distributed before the Meeting)_*

What

First, I have to commend the NIST staff responsible for the development of the guidelines and standards documents that form the FISMA framework. This body of work provides an incredibly comprehensive background and framework for information security.

To a limited degree, the current version of CIP standards at least attempted to capture the essence of fundamental cyber security implementation and management however, as is evidenced by the creation of the SDT 706 team, the full extent of what is required was missed. In the years since the CIP standards were conceived, NIST expanded and refined the cyber security framework and standards documents required for FISMA. These documents embody the essence and the detail required for Information Security Management. In fact, the NIST FISMA documents go beyond a framework by providing the narrative background at a fundamental level necessary to develop a clear understanding of the framework, intent and method of implementation to non-cyber security professionals. A clarity that is largely lacking in the CIP standards.

To date the SDT 706 Phase II discussions have largely centered on NIST 800-53 and integration with the CIP standards. To a lesser degree, FIPS-199, NIST 800-53A and FISMA have been discussed.

I feel at this time expanding the discussion to FISMA and the full body of associated NIST standards and guidelines is warranted. Not simply should or how NIST 800-53 can be integrated but to what degree should or can CIP integrate or parallel FISMA.

After review of FISMA as documented and the supporting NIST documents, I count myself an advocate of integration and, to a significant degree, adoption of the FISMA/NIST approach to Information Security Management for electric sector CIP standard.

Why

The FISMA/NIST framework provides a consistent methodology to install a set of security protections appropriate to the criticality of an information system and the associated information.

It is well thought out, documented and based on the fundamentals of cyber security and SDLC. The guidelines provide the fundamental security background as well as the guidance for application.

It is a body of work that is easily accessible by all industries and sectors and all sizes of entities, service providers, vendors, auditors, etc. It is a requirement for federal agencies including those in the electric sector. As such, it represents a common framework. Ambiguity is minimized. Knowledge sharing is maximized.

The use of a common framework will provide the greatest opportunity for uniform application of cyber security controls to protect our Critical Infrastructure. Fundamentally, it provides a common basis for assessment, implementation and audit regardless of sector or service entity.

As much as the existing CIP standards may get most entities to the point of implementing appropriate cyber security controls, it will not have been done in a consistent manner with clear mutual understanding of the objectives.

Though the body of NIST documents is of significant volume, the effort required to understand and apply is in no way more difficult than the effort that has been expended to understand and apply the CIP standards. The most significant difference is that after the NIST process is assimilated, security controls may be implemented consistently, monitored consistently, changed consistently and, assessed consistently.

Protecting our cyber managed supply of electricity in a consistent manner across all entities is the best thing to do.

It's paid for.

How

Integration approaches can range from drawing on individual elements in the NIST documents to fill in the CIP gaps requirement by requirement to wholesale adoption of FISMA.

My recommendation is that we take an approach that establishes a strong parallel to FISMA, utilizing the NIST standards and guidelines as much as possible.

In it's most pervasive manifestation, this would entail a combination of adopting the FISMA/NIST documents directly and/or creating parallel documents/supplements tailored to the electric sector. This would likely result in an overhaul of the current CIP requirement layout and require transition education.

At a minimum, this would entail developing a set of controls (800-53), related assessment procedures (800-53A) and FIPS 200 Minimum Security Requirements equivalent specific to BES

entities, creation of FIPS 199 Security Categorization equivalent that integrates to CIP 002 and other CIP requirements to relevant NIST documents.

The degree to which the FISMA/NIST framework should be adopted will need to be discussed and debated.

A couple of fundamental questions:

- Does FERC feel that adoption of FISMA/NIST framework will meet all the concerns in Order 706?
- What were the concerns with adopting the FISMA/NIST framework as the basis for the existing CIP standards and do those concerns still exist?

W Winters 02/02/09

THOUGHTS FOR DISCUSSION OF CIP/NIST OPPORTUNITIES

(Handed out at the meeting)

- Develop set of controls for each area/entity which could be done regionally
- Entities can create control extensions. This is currently allowed in the NIST method
- Allow option for federal entities currently subject to FISMA and CIP to use FISMA/NIST to satisfy CIP
- Encourage use of FISMA/NIST today. Entities have the option today to use FISMA/NIST as a basis for meeting CIP requirements.

- Develop a process for application of FISMA/NIST (e.g. Develop as an overlay of CIP or Develop as standalone)

Controls Development Approach

- SDT sub-Team(s) could develop initial minimum controls (they could be entity tailored controls and/or "exception" based controls)
- Create clearinghouse for sharing of controls amongst entities as different organizations develop control extensions
- Develop controls using working group model at the regional level. This could be extended to development of educational framework and more effective open information sharing.
- Lifecycle management of controls for improvement/refinement and adoption
- Regional controls could feed to national and periodic update with regional, national and NIST representation.

- NIST and/or SDT team create initial draft of documents for "CIP" (e.g. appendices to existing or separate set of docs,)

- Build transition education program based on mapping of CIP to NIST.

- As body of controls are refined and standardized, auditors, developers of compliance programs (internal, consultant/vendor), developers of applications, support personnel, etc. have common reference and interpretation of the standards

Heavy alignment:

1. Expand/replace CIP 002 to require assessment of:

a) Systems used in control and monitoring of BES/BPS
b) Systems directly connected and/or exchange data with
c) Systems which transport data used in control and monitoring
d) ….

2. Develop equivalent FIPS 199, FIPS 200

3. Develop Risk Assessment process (800-37 equivalent/appendix) tailored to industry.

Integration light (in the beginning):

1. Develop set of controls (can use existing NIST controls as starting point) for each of the CIP requirements. Some of these exist within the CIP standards today but not consistently.

2. Systems that are determined in CIP 002 to be CCA are classified as high, as are all systems within the same ESP and form the ESP. Monitoring systems get medium?

3. Map CIP requirements to NIST docs as guidelines particularly for Risk Assessment

Appendix # 8

CIP-002-1 DISCUSSION DOCUMENT, 1-29-09

Jackie Collett, John Lim, Scott Rosenberger, and John Varnell

I. ORIGINAL INTENT OF THE CIP-002 VERSION 1 STANDARD

- **Starting Point**: A "reasonable" initial attempt to applying cyber security to the electric infrastructure.
  - Initial Baseline – starting from zero
- High Impact Focus: Reduces the scope of implementation to the transmission and generation assets which have the highest impact on the reliability and operability of the BES.
- Cyber Assets: directly linked to the BES elements *FAQ Q2*
- Cyber Asset Scope: limited to control centres, remote access and "jumping-off" points, which may not be evident in the standard *FAQ 2*
- What to Do: Not How to Do
- Non-prescriptive: Allows flexibility for a wide range of scenarios

- **Key Decisions**:
  - Create "trusted zones"
  - Exclude communications outside of "trusted zones": often external carriers and indeterminate paths

- **Assumptions**: Not explicit in the standard, but required for good security
  - **Redundancy**: Critical Asset / Cyber Asset redundancy does not eliminate the requirement for cyber protection. *FAQ Q5*
    - Need to protect common modes of failure.
    - Multiple attacks / compromises are possible electronically.
  - **"Systems approach"**: A systems approach to identifying Critical Assets / Critical Cyber Assets can and should be used. CIP-002 does not preclude a systems approach, but does not explicitly require it.
  - **"Consider**": Consider means include if at all applicable.
  - **"Essential to operation":** Critical Assets and Critical Cyber Assets should be identified and protected to ensure sustainable and reliable operation indefinitely. Loss or compromise of the Control Centre or other critical functions is not sustainable.
  - **Critical Assets**: Critical Assets may include sites, elements and systems.
  - **CCA Compromise**: In addition to the BES impact due to loss of the Critical Asset or Critical Cyber Asset, compromise of the Critical Cyber Asset must be included in the risk assessment (Integrity).

- FERC conditionally approved the Version 1 standards, and directed changes for a "final" version
  - The "gap" is what is currently under discussion

II. IMPORTANT ASPECTS OF CIP-002-1

1. **Relationship to BES**: There is a very clear relationship between the BES assets required for reliability and the cyber assets essential for their operation. The reliability and operations segments of the electric industry are structured upon BES assets. This includes processes, procedures, inventories and terminology.
2. **High Impact Focus**: CIP-002-1 focuses the efforts and resources for protection to the most important BES assets and associated cyber assets, recognizing that resources are not unlimited. Assets which do not affect the reliability and operability of the BES are not considered. As a result, the majority of the BES assets are not included for protection under the CIP standards.
3. **Industry Acceptance**: The electric industry has invested thousands of hours and millions of dollars to meet CIP-003-1 through CIP-009-1 based on CIP-002-1. The industry would not favour a significant or radical change to the asset identification method, and could reject it.

III. ISSUES IDENTIFIED WITH THE CURRENT CIP-002 + STANDARDS

A	PIECEMEAL APPROACH
Description	By identifying individual Critical Cyber Assets, security gaps exist when the CCAs operate in a system. (Eg. data integrity impact for a cyber asset outside of the ESP)
Comment	• The identification of Critical Cyber Assets does not preclude a systems approach, but does not explicitly require it. • A Critical Cyber Asset may be part of a system or network, including other cyber assets, which is currently addressed somewhat by the ESP. • The standards do not address interdependent functions across ESP boundaries, which may be essential to the Critical Cyber Asset and/or the BES.
Options	1. Need to include both Critical Cyber Assets and critical functions. 2. Need to include an impact assessment of the components required for the critical function. 3. Need to include consideration and protection for interfaces into the Critical Cyber Assets – may be at a different risk level. Protection may be required outside of the ESP.

B		**NOT PROTECTING ASSETS NEEDING PROTECTION**
	Description	Assets which may have an impact on the BES, either singly or in conjunction with other assets, are not being identified under CIP-002.
	Comment	• Compliance with the NERC cyber security standards is onerous. • There are large penalties for non-compliance. • Criticality based on BES system planning models (eg. PSSE) are not adequate. BES interconnectivity and interdependencies are very different from cyber connectivity and interdependencies. • Area requirements or impacts may not be available or considered in the identification of Critical Assets and Critical Cyber Assets (eg. generation units' impact on the reliability and operability of the BES in a geographical area). • Perception of "missing Critical Assets" creates a lack of confidence in the industry to self-manage.
	Options	1. Include some responsibility for the BA in determining Critical Assets based on area impact (area overview). 2. Single largest contingency must be included in the impact / Critical Asset identification. 3. The Identifying Critical Assets Guideline[1] provides detailed guidance for Critical Asset evaluation. 4. Targeting specific risks / impacts can help focus the protection requirements.
C		**GAMING**
	Description	Entities are striving to create minimal or null Critical Asset Lists to avoid the effort and expense of complying with the standards.
	Comment	• Some entities are taking a very literal interpretation of the standards, and some oppose guidance that is not explicitly included in the standards. • Asset identification by some entities has been perceived as "unreasonable" and generated criticism of the industry.

[1] The NERC Guideline "Identifying Critical Assets" is presently under development by the Critical Infrastructure Protection Committee Risk Assessment Working Group. The development of this guidance document was directed by FERC in its NOPR, and reconfirmed in FERC Order 706 p253.

	• All compliance avoidance (gaming) cannot be completely anticipated or eliminated. • Gaming will occur regardless of the methodology or framework applied. These issues can be addressed over time through the audit and compliance enforcement process. • "Zero tolerance" for non-compliance: sef-report a violation and possibly be fined (compliance culture vs. good security practice)
Options	1. Improve clarification of the intent of the standards and the requirements.
D	**ALL OR NOTHING**
Description	Assets or cyber assets are either critical and require protection, or not critical and do not require any protection.
Comment	• Conducted diligently, including the interdependencies of systems required for essential functions, the asset identification can provide an adequate level of security for the BES. • NERC's mandate is to protect the BES. This does not include distribution and the related assets. • There are no graduations or levels of assets, and no levels of protection for cyber assets.
Options	1. The fundamental tenet of the NERC reliability standards is to protect the reliable operation of the BES; therefore the focus of cyber protection, for both BES assets and cyber assets, should be on their impact to the reliable operation of the BES. 2. The Identifying Critical Assets Guideline[1] provides some criteria to help define impact to the BES. 3. There may be a need to define what systems beyond the current Critical Assets need protection. 4. Required protection of cyber assets may be related to some characteristics (contains an operating system / purpose-written software / no software). 5. Multiple levels of protection do exist in the standards: critical cyber asset vs. non-critical cyber asset in an ESP vs. cyber asset outside an ESP. May want to provide a different granularity. 6. Define the breadth and depth of protection.
5	**LOSS OF ASSET - INTEGRITY / MISUSE**

Description	Determining the criticality of BES assets tends to focus on a loss (outage) of the asset. Loss of data integrity or misuse of the cyber assets may not be considered.
Comment	– Loss of an asset is a traditional risk analysis approach which may be incomplete for cyber impacts. – Can be combined with other system or cyber events, increasing the impact – Need to include the analysis of intentional and unintentional misuse.
Options	1. Consider magnitude of impact of loss of data integrity / misuse: o Generation or Transmission Control Centre – possible impact. o Transmission Substation or Generation Assets – little or no impact depending upon the size or function of the facility. May be related to the single largest contingency. o ISO – possible impact. 2. Need to educate industry to consider intentional and unintentional misuse

Appendix # 9

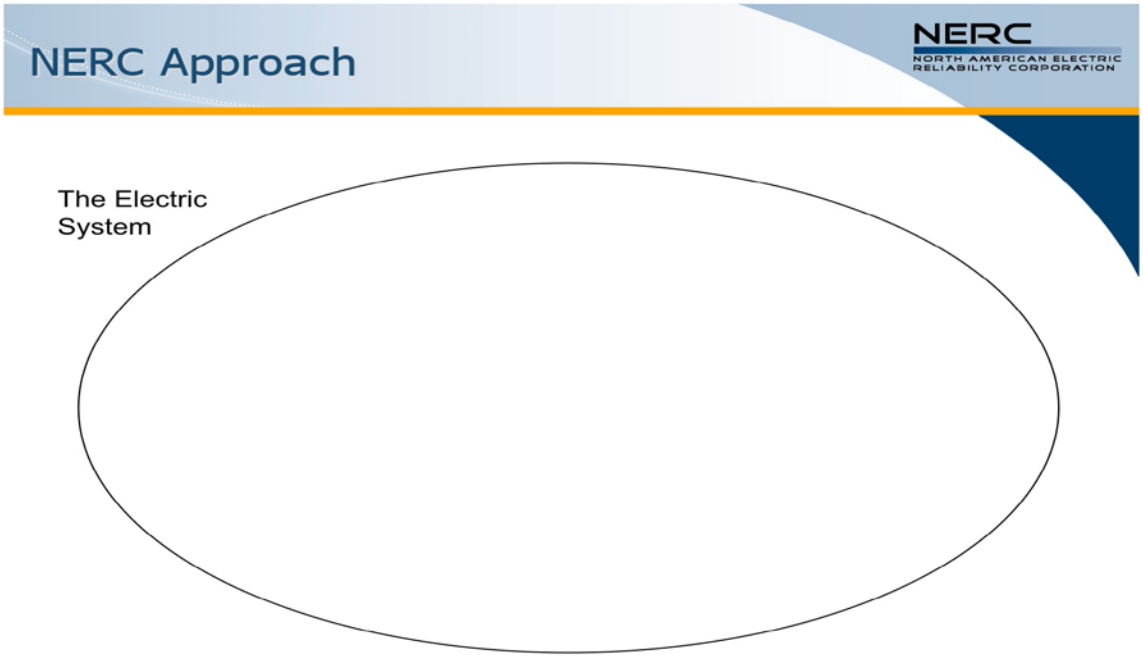
SCOTT MIX, STRAWMAN-FISMA ASSET SELECTION

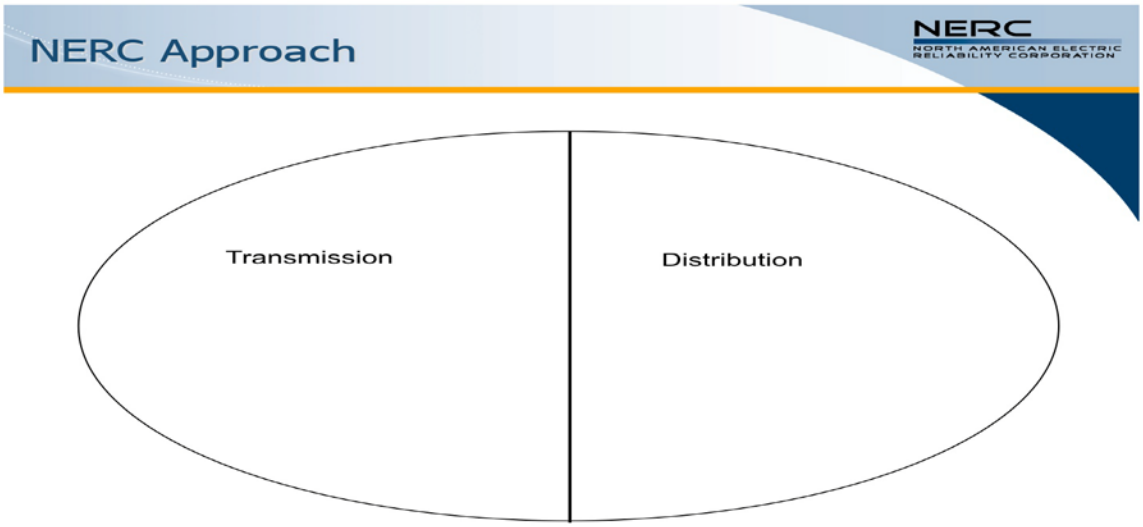
Categorization of Assets

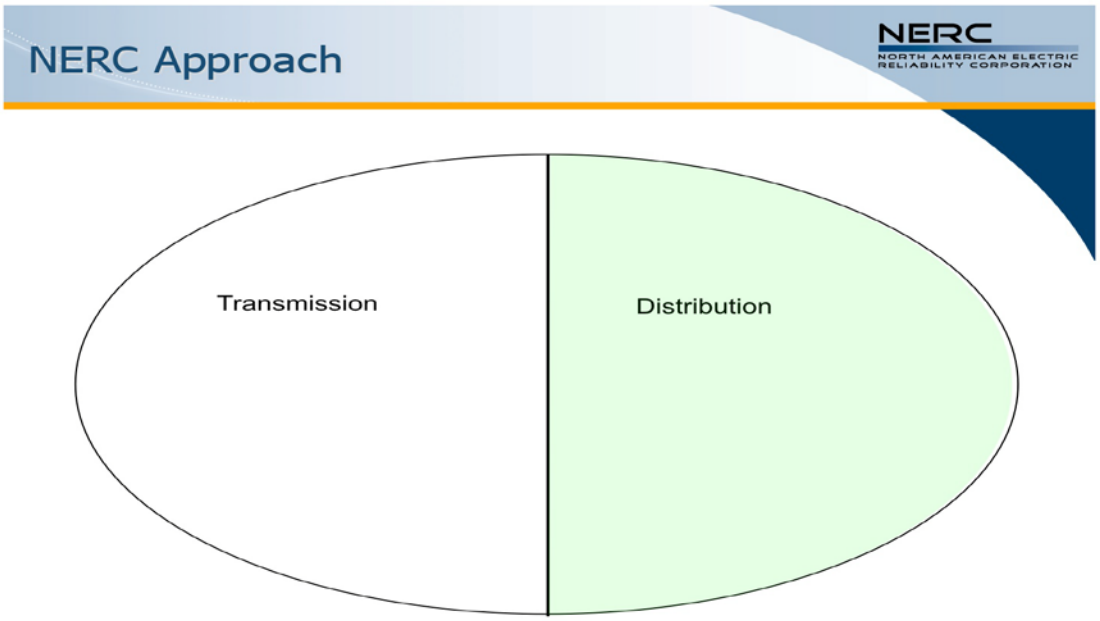
- FIPS-199:
  - Mission Focus:
    - "The security categories are based on the potential impact on an organization should certain events occur which jeopardize the information and information systems needed by the organization to accomplish its assigned mission, protect its assets, fulfill its legal responsibilities, maintain its day-to-day functions, and protect individuals." (emphasis added)
    - "Security categories are to be used in conjunction with vulnerability and threat information in assessing the risk to an organization."

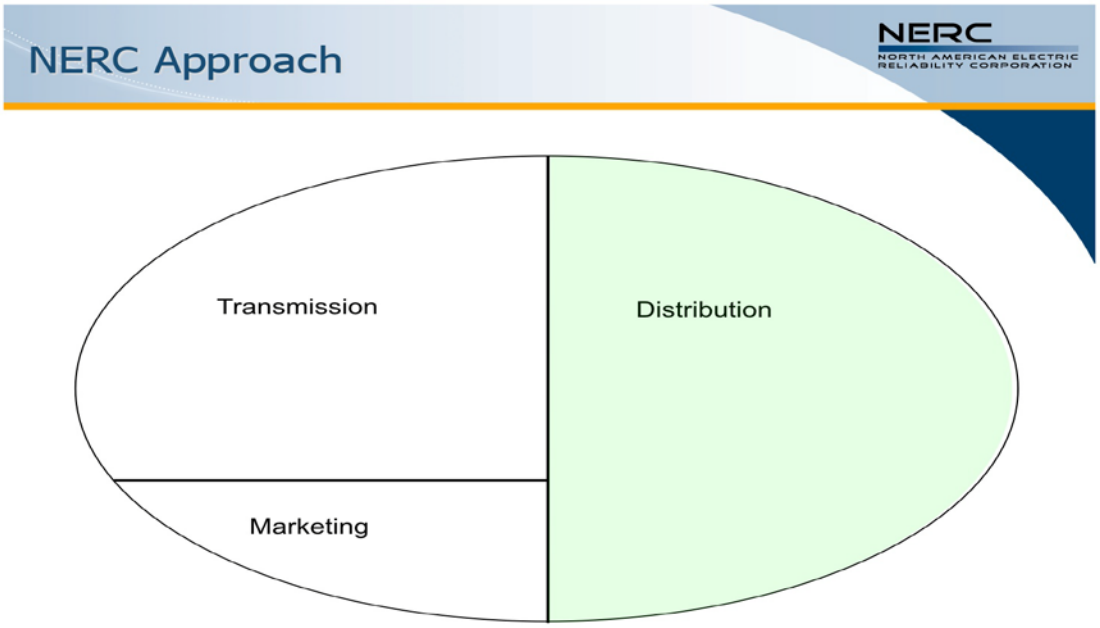
Categorization of Assets

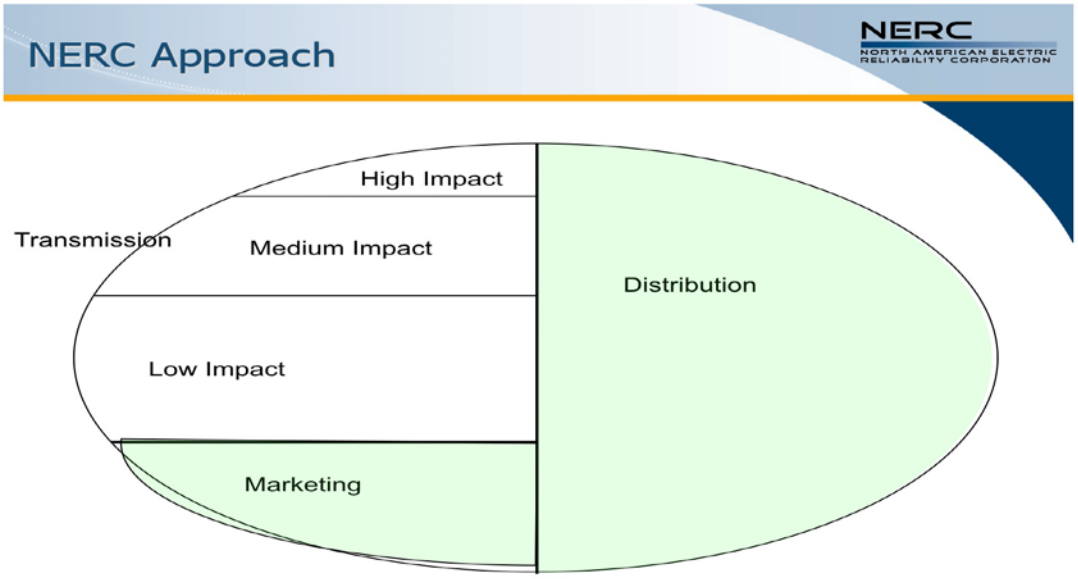
- FIPS-199:
  - Characterize in 3 categories:
    - Confidentiality
    - Integrity
    - Availability
  - Assign level to each category:
    - Low
    - Medium
    - High
  - High Water Mark
  - Customize controls (later)

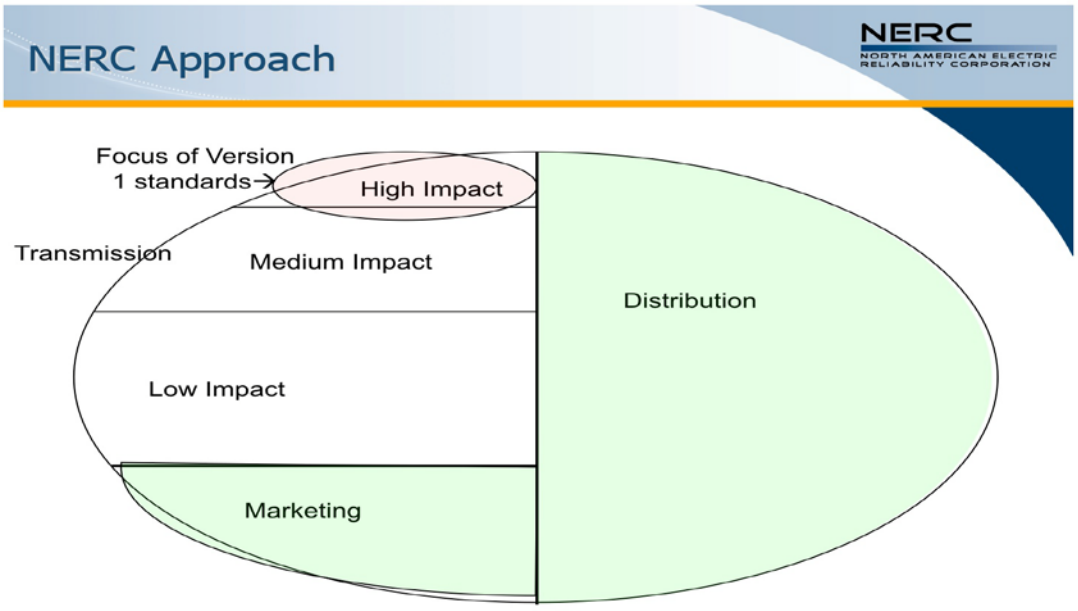

NERC Approach
NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION
The Electric System


NERC Approach
NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION
Transmission
Distribution

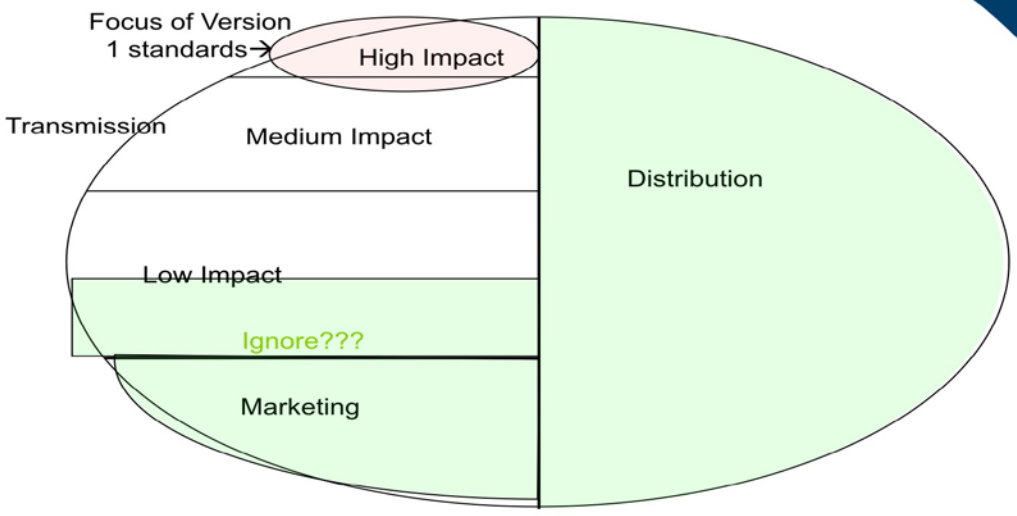

NERC Approach
NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION
Transmission
Distribution


NERC Approach
NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION
Transmission
Distribution
Marketing


NERC Approach
NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION
High Impact
Transmission
Medium Impact
Distribution
Low Impact
Marketing


NERC Approach
NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION
Focus of Version 1 standards
High Impact
Transmission
Medium Impact
Distribution
Low Impact
Marketing

NERC Approach



NERC Approach

- This would require changes:
  - CIP-002 to classify ALL transmission assets by impact category
  - CIP-003 to CIP-009 – requirement-by-requirement specificity for obligations at each impact category level
    - SP800-53 Catalog as an example

NERC Approach

- Separate set of standards for:
  - Control Centers
  - Transmission Facilities
  - Generation Facilities
- Each with 3 levels of requirements
  - Not every requirement would expand – but most would
  - Essentially expanding current requirement set by practically a factor of 9 just to maintain *status quo* with requirement scope

NERC Approach

- Would this meet all the mandated (ordered) changes from FERC Order 706???
  - Probably not by itself
  - Would require significant additional work on top of what was just described.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Draft Meeting Agenda

Cyber Security Order 706 SDT — Project 2008-06

March 10, 2009 | 1–5 p.m. EDT
March 11, 2009 | 8 a.m.–5 PM EDT
March 12, 2009 | 8 a.m.–noon EDT
Orlando Utilities Commission- Pershing Facility
6003 & 6113 Pershing Avenue
Orlando, FL (407-423-9100)

Proposed 706 SDT Meeting Objectives and Outcomes:

- Receive updates on Phase I actions, TFE and VSL processes;
- Review Phase II guiding principles;
- Review, clarify, assess alignment with principles of two CIP 002 strawman proposals;
- Test integration of CIP 002 strawman proposals;
- Agree on 2009 meeting schedule, next steps in the SDT Work plan and assignments.

Tuesday March 10, 2009

1:00 p.m. **Welcome and Opening Remarks — Jeri Domingo-Brewer and Kevin Perry**

a. Roll Call
b. NERC Antitrust Compliance Guidelines
c. Review and adoption of February 18-19, 2009 Meeting Summary
d. Review of Team membership changes

1:15 **Review of Meeting Objectives, Agenda and Meeting Guidelines — Jeri Domingo and Bob Jones**

1:20 **Organizational Issues and Review of Phase 1 and early Phase II Schedule — Stuart Langton**

a. Update on Phase 1 Workplan, March 2009
b. Overview of Phase 2 Workplan — March–June 2009
c. Schedule for July–December 2009, Calendar Forms
d. Update on SDT Membership

1:40 **Update on Technical Feasibility Exception (TFE) NERC Rules of Procedure Posting — Scott Mix**

1:50 **Update on VSL SAR for SDT and Implications for SDT 706 — David Taylor**

2:00 **Review of Phase 1 Timeline — David Taylor**

2:10	**Overview of SDT Phase II Development Process Steps and CIP 002 Review — Stu Langton**
2:20	**CIP 002 Strawman #A — Concept Proposal Presentation Overview — Bill Winters and Kevin Perry — Q & A and Discussion**
3:20	**Break**
3:35	**CIP 002 Strawman #B — Concept Proposal Presentation Overview — Jackie Collett and John Lim — Q & A and Discussion**
4:35	**Complete and Pick up Calendar Forms and Summary of Day One Outcomes and Review of Day Two Agenda**
5:00	**Recess**

Wednesday March 11, 2009

8:00	**Welcome, Agenda Review and Roll Call**
8:15	**CIP-002 Strawman #B Review of Positives/Negatives; Gauge Alignment with Guiding Principles and Acceptability Testing — Jackie Collett and John Lim**
10:15	**Break**
10:30	**CIP-002 Strawman #A Review of Positives and Negatives; Gauge Alignment with Guiding Principles and Acceptability Testing — Bill Winters and Kevin Perry**
12:30	**Working Lunch**
1:15	**Exploration of Potential Integration of Positive Elements of CIP 002 Strawman #A and #B**
3:00	**Break**
3:15	**Building a Phase II Strawman Concept and Guidance Document — Continued**
4:45	**Review of Work-plan and Meeting Schedule through 2009**
5:00	**Adjourn**

Thursday March 12, 2009

8:00	**Welcome, Agenda Review and Roll Call**
8:10	**Review and Refinement of a Strawman Phase II Concept Document — Continued**
10:00	**Break**
10:15	**Refine Strawman Phase II Concept Document**
11:15	**Initial Discussion of SDT Organizational models for Phase II**
11:45	**Review of April SDT agenda and objectives**
11:50	**Meeting Evaluation — What Worked, What Could be Improved**
12:00	**Adjourn**

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

CYBER SECURITY ORDER 706 SDT JANUARY–DECEMBER DRAFT PROJECT SCHEDULE *(REVISED MARCH 2009)*

Short Term 2009 Schedule Draft Criteria

- Follow the ANSI standard development process but use creative ways to efficiently secure input from the industry on emerging concepts and approaches to the CIP standards.
- Seek creative ways to get advice and input to the SDT from experts in cyber security.
- Seek creative ways to get focused input from industry stakeholders.
- Take advantage of input opportunities from related NERC committees that will be meeting in the first half of 2009 (e.g. working with the NERC Members Representative Committee, CIPC, BOT, and industry committees such as the Electricity Sector Coordinating Council, etc.)
- Seek, as soon as possible but no later than late Spring, 2009, to establish a consensus on the way forward for the SDT in its efforts to revise the CIP standards.
- Track any follow up to the "Securing Cyberspace for the 44th Presidency" report of the Commission on Cyber security for the 44th President.

SDT Draft Schedule — January–December 2009

Overview

- 12 SDT Face-to-Face Meetings
- Multiple SDT subgroup and subcommittees WebEx Meetings
- 1 Cyber Expert/Stakeholder Workshop (August, 2009)
- Industry Comments on CIP 002 SDT White Paper (June–July, 2009)
- 2 NERC Members Representative Committee, (May and August, 2009)

SDT Draft Schedule — January–June, 2009

1. **January 7–9, 2009 SDT Meeting, Phoenix, AZ ½, 1, ½ day format. Wednesday–Friday**
   - Review of Technical Feasibility Exceptions white paper
   - Review of Industry Comments on Phase 1 products- Establish and convene small groups to draft responses
   - Review of Phase 2 White papers

   January 15 — WebEx meeting(s)
   - Small group draft responses to industry.

January 21 — WebEx meeting(s)
- Small group draft responses to industry.

2. **February 2–4, 2009 SDT Meeting Phoenix, AZ,** ½, 1, ½ day format. Monday–Wednesday
   - Update on NERC Technical Feasibility Exceptions process
   - Review of VSL process and SDT role
   - Review of Phase 2 White papers, strawman and principles
   - Review and Adoption of SDT Responses to Industry Comments on Phase I and Phase I Product Revisions.

3. **February 18–19, 2009 SDT Meeting, Fairfax, VA**
   - Update on Phase I process
   - Update on NERC TFE process
   - Update on VSL Team process
   - Review, discussion and refinement of Phase II/CIP 002 White papers, strawman and principles

4. **March 10–11, 2009 SDT Meeting Orlando, FL,** ½ , 1, 1 day format
   - Update on NERC TFE process
   - Update on VSL Team process
   - Review and Refinement of Phase II CIP 002 Strawman Proposals

March 2–April 1 — 30-day Pre Ballot
Mid-March — NERC posts TFE draft Rules of Procedure for industry comment

April, 2009 NERC Balloting on Phase 1 Products

March 18 — WebEx meeting(s)
- As needed

March 25— WebEx meeting(s)
- As needed

5. **April 14–16, 2009 SDT Meeting, Charlotte NC, ½, 1/½ day format. Wednesday–Friday**
   - Update on NERC TFE process
   - Update on VSL Team process
   - Review, Refinement and Adoption of Phase II Strawman Proposal

April, 2009 Phase I Ballot Results

May 4, 2009, Member Representative Committee Meeting, Arlington, VA, SDT progress report.

6. **May 13-14, SDT Meeting, Boulder NV, 2-day format**
   - Review and respond to Phase I Ballot Results.
   - Review MRC presentation and any input to SDT on Phase II Concept
   - Further SDT refinement of the Strawman Phase II White Paper
   - Adopt a Phase II White Paper for Industry Comment
   - Review potential SDT subcommittee structure for Phase II

   Industry Comment Period on SDT Phase II White Paper- 45 days (June 1-July 15, 2009)

7. **June 17–18, 2009 SDT Meeting, Manitoba, 2-day format**
   - As necessary, review and respond to Phase I Ballot Results.
   - Organize SDT in subcommittees to draft revisions to CIP and/or to address key issue areas.
   - Agree on and Charge subcommittees and conduct organizational meetings
   - Subcommittees meet to begin drafting revisions to CIP and/or addressing assigned issues.
   - Subcommittee Plenary reports to SDT.

   June, 2009 — WebEx meeting
   - SDT Subcommittee meetings.

8. **July, 2009 Date, Location, and Time — TBD**
   - Convene workshop of cyber experts to review Phase II-CIP 002 Strawman White Paper.
   - Continue review and refinement of Strawman White Paper.
   - Adopt Strawman White Paper as refined for MRC Comment and Input.

9. **August, 2009, Date, Washington D.C., Time — TBD**
   - SDT Expert/Stakeholder Workshop, Washington D.C.
   - SDT Plenary Session(s) review of workshop input on key issues and review and revision, as needed of sub committees' charges.
   - SDT Phase II Subcommittee meetings and reports back.
   - August 2009, NERC Member Representative Committee, Presentation of the Phase 2 CIP 002 Approach for MRC input. Winnipeg, Manitoba

10. **September, 2009 Date, Location, and Time — TBD**
    - SDT Plenary Session(s)
    - SDT Subcommittee meetings.

    September WebEx meeting
    - SDT Subcommittee meetings.

11. October, 2009 Date, Location, and Time — TBD

- SDT Plenary Session(s)
- SDT Subcommittee meetings.

October WebEx meeting

- SDT Subcommittee meetings.

November WebEx meeting

- SDT Subcommittee meetings.

12. December, 2009 Date, Location, and Time — TBD

- SDT Plenary Session(s)
- SDT Subcommittee meetings.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Draft Meeting Summary

Cyber Security Order 706 SDT — Project 2008-06

April 14, 2009 | 1–5 p.m. EST
April 15, 2009 | 8 a.m.–5 p.m. EST
April 16, 2009 | 8 a.m.–noon EST
Charlotte, North Carolina

Meeting Summary Contents

116-390 Village Blvd.
Princeton, NJ 08540
609.452.8060 | www.nerc.com

EXECUTIVE SUMMARY

Joe Bucciero conducted a roll call of members and participants, the Chair reviewed the meeting objectives and the facilitator, reviewed with the team and participants the proposed meeting agenda.

Mr. Bucciero reviewed with the team the need to comply with NERC's Antitrust Guidelines. The team reviewed and unanimously adopted on March 12 the SDT February 18–19, 2009 meeting summary. Stuart Langton, SDT facilitator, reviewed the current work plan and meeting schedule for both Phase 1 and Phase 2 development. At the conclusion of the meeting the SDT agreed on a schedule of meetings from July–December, 2009. The team reviewed and unanimously adopted on April 16 the SDT March 10–12, 2009 meeting summary.

Scott Mix, NERC staff, provided an update on the TFE process. He indicated that he is aware that EEI has indicated it will be filing comments. Once the comments are in, NERC's legal staff and leaders will address the comments. He believes the comments will be addressed and the document will be sent to the NERC board for approval in the summer of 2009. After NERC board approval, the modification to the NERC Rules of Procedure for the TFE will be sent to FERC for approval and filed with the appropriate Canadian governmental authorities.

Dave Taylor, NERC staff, provided an update on VSL/VSR process. FERC issued a recent order on two standards. FERC said in their order that it was not sure about the use of a 'roll-up' approach to VSLs. FERC asked that NEC provide further explanation of the approach. The VSLs proposed for CIP-002 through CIP-009 have included some of these roll-up VSLs embedded in them. He noted that the there may to be a future reassessment if FERC doesn't allow for this approach.

During a pre-session on Tuesday morning, a team, lead by Kevin Perry, prepared responses to the comments received in the ballot of CIP Version II. The SDT reviewed each of the draft responses, suggested changes and reached consensus on all of the responses by Thursday morning. Some of the major issues contained in the comments were:

- Comments concerning the constrictive nature of the Technical Feasibility Exception Process;
- Designation of the Senior Manager as overly prescriptive;
- Objections to the inclusion of "continuous" monitoring in CIP-006 for physical security;
- Several commented and expressed concerns on the reduction from 90 days to 30 days for changes to be made in the standards.

The group reviewed Kevin Perry's initial draft, refined and finalized the team responses to the comments made after the posting of CIP Version II to the industry. The team unanimously adopted the Response Document (16-0) as revised on Thursday morning and asked Kevin Perry with assistance from Joe Bucciero to finalize the document for submission to NERC and to initiate the recirculation ballot.

The team discussed the publicity and media stories last week regarding the vulnerability of the electric grid raising concern with the hyperbole (characterizing as “Pearl Harbor”, “Hiroshima”, “9/11”) and lack of evidence for many of the claims. A letter from Representative Markey, House Homeland Security to FERC and draft legislation filed by Senators Rockefeller and Snow were noted.

Michael Assante, NERC’s Chief Security Officer, provided the team with a briefing on NERC’s response to the media coverage of the last week beginning with the Wall Street Journal article. He noted that NERC has sought to strike the right tone in a complex area of policy and practice. NERC worked behind the scenes with press, congress, FERC and industry associations and issued a press statement noting that the industry is committed to working hard on cyber security and the SDT effort to develop new standards is a leading example of this effort. While acknowledging the reality of continuing vulnerability, NERC challenged the notion that there was evidence of any cyber security compromises that have adversely affected reliability. He noted NERC is working with industry associations. He suggested SDT has a role to play and that it shouldn’t be seeking to defend the industry. NERC will be trying to get the message out as to the progress to date and the SDT role in addressing cyber security and reliability.

Gerry Freese made a proposal made to put together a comprehensive presentation that might be given to Congressional staffers to get out the message that the industry is taking cyber security seriously and has made great efforts. In addition the message would explain some of the inaccuracies contained in the recent publicity concerning vulnerabilities of the electric grid. Facilitators suggested that the briefing for congress might be created in conjunction with the update. In general team members supported a message responding to the recent publicity. The Chair suggested the SDT form a “Key Messages Task Group” and solicited members who would want to participate: Gerry Freese agreed to lead the effort, and John Stanford, Jerry Domingo Brewer, Jay Cribb, Dave Norton, Phil Huff, Rich Kinas and Jim Breton all agreed to participate.

Mr. Langton, SDT facilitator, reviewed the significant progress the team has made together since October 2008. He then set the stage by saying that the point of the Phase II Concept paper presentation is to assure SDT member understanding of the concept and invite ideas for strengthening and clarifying aspects of the concept.

John Lim introduced the white paper noting contributions from Jackie Collett, Bill Winters, Phil Huff and assistance from Scott Mix in refining the white paper since the March SDT meeting in Orlando. He noted the group met two times by phone and WebEx, and convened a SDT WebEx meeting and met this morning. They agreed that they needed additional input and contributions from other SDT members in developing the concept paper. He also noted that the group will need to define terms used in the document. One change in the approach is to move away from a “risk assessment” to an “impact based assessment.” He offered the following overview of the concept:

- Identification and categorization of BES Assets.

- Identification of the cyber systems that support functions or BES assets.
- The idea is to combine the two categorizations to supply the categorization for the asset.
- All applicable cyber assets (EMS, substation, relay, etc.) will need to be identified with a categorization level.
- Total impact on the BES system will need to be determined using the table.
- The categorization will then be utilized for the requirements that follow.

Following a review and discussion of each section of the paper the facilitator asked if any of the SDT members had any fundamental difficulty with the approach and then polled the SDT members as to whether all were comfortable at the conceptual level with the current white paper approach. All members agreed to go forward indicated that they liked the direction the white paper was taking. All acknowledged that they would continue to test this as the details were developed.

On day two, John Lim and Phil Huff agreed to draft some general draft consensus points from the white paper that could be presented by the Chair to the NERC Members Representative Committee on May 4, 2009. They were joined by Jackie Collett, Scott Rosenberg, John Varnell and Rich Kinas. The SDT reviewed and refine these on Thursday morning resulting the following 11 points which received a 3.8 of 4 rank in terms of their acceptability. The chair agreed to base her presentation on the points:

A. The Standards should require a BES impact assessment as an initial approach to categorizing BES Cyber Systems.
B. The impact categorization of Cyber Systems will be based on reliability functions of the BES to achieve Adequate Levels of Reliability.
C. The Standard's BES Impact Assessment will consider a categorization process.
D. The Standards will require oversight of the categorized list of BES assets by entity types which have a more complete wide-area view of the BES.
E. The Standards will categorize Cyber Systems supporting, either directly or indirectly, the reliability functions of the BES and apply security requirements (or controls) that are commensurate and appropriate to their impact on the BES.
F. The final Cyber System categorization will reflect the impact to the BES based on a loss of availability, integrity, or confidentiality of the Cyber System.
G. The Standards will provide Organizations with reasonable flexibility in applying equivalent security controls on the basis of compensating controls and environmental considerations.
H. The Standards will address the complex nature of BES functions and interconnected Cyber Systems, both within and between multiple organizations.
I. The Standards will state explicit criteria for the BES Impact Assessment.
J. The Standards will state explicit criteria for the Cyber Impact Assessment (including use and mis-use of cyber systems).

K. The Standards will include a methodology to merge the BES Impact Assessment and Cyber Impact Assessment into a final Cyber System categorization.

The Chair also agreed to put these points in a narrative format for a letter to Mike Assante as part of the SDT's input to NERC as it develops its input to FERC in response to Rep. Markey's letter.

Bob Jones, SDT facilitator presented the concept of CIP-002- requirements and measures being the work undertaken for the rest of 2009 with the goal of posting for industry comments on a complete CIP-002 standard and go to ballot on it. This might include taking a requirement from CIP-003 through CIP-009 to illustrate how CIP-002 would related to the later development of CIP-003 through CIP-009. The SDT would then develop the entire CIP-003 through CIP-009 package and post for comments and balloting as a complete package. The schedule proposes that the SDT will be into 2012 when a full version of CIP version III is posted for comments.

The Chair reminded people to register for the Boulder City meeting and that the September meeting would take place in Folsom, California near Sacramento and not in Denver:

The CIP-002 sub team will continue working on the parts of the white paper that need development. Categorization of the BES assets still needs refinement and help. The sub team asks for assistance from outside the group. Scott Mix will take the lead to see if additional expertise can be provided to the sub team.

The team offered an evaluation regarding what was accomplished, what helped and what might help for the future.

The Chairman concluded the meeting concluded by thanking the host (Duke Energy) and is looking forward to hosting the meeting in Boulder City. The SDT adjourned at 11:45 a.m. on April 16.

I. Introductions, Agenda Review and Review of SDT Workplan

The Chair, Jeri Domingo-Brewer, welcomed the members. Joe Bucciero conducted a roll call of members and participants in the room and on the conference call for each day *(See appendix #2*). The Chair reviewed the meeting objectives and Bob Jones, facilitator, reviewed with the team and participants the proposed meeting agenda *(See appendix #1*).

Mr. Bucciero reviewed with the team the need to comply with NERC's Antitrust Guidelines *(See, Appendix #3).* He urged the team and other participants in the process to carefully review the guidelines as they would cover all participants and observers. He urged all to avoid behaviors or appearance that would be anti-competitive nature and also reminded the group of the sensitive nature of the information under discussion. The team reviewed and unanimously adopted on April 16th the SDT March 10–12, 2009 meeting summary.

Stuart Langton, SDT facilitator, reviewed the current work plan and meeting schedule for both Phase 1 and Phase 2 development. (*See Appendix #4)* The Chair noted that the meeting location in September would be changed from Denver to Sacramento or Folsom, California. The facilitators noted that the team may want to adjust the work plan so that it is clear that when the Phase II White Paper is ready for release, it will be done so by informally posting on the NERC Web site, inviting industry reactions without triggering the need for a formal ANSI step. This will enable the team to focus in on the development of CIP-002 for potential posting by the end of the calendar year.

Mr. Langton noted that by the conclusion of the meeting, the SDT needed to have the responses to the industry comments completed and sent to NERC for posting and to begin the recirculation ballot and to have made progress on the Phase II white paper and approach.

II. Technical Feasibility Exception Update and SDT Discussion

Scott Mix, NERC staff, provided an update on the TFE process. He indicated that he is aware that EEI has indicated it will be filing comments. Once the comments are in, NERC's legal staff and leaders will address the comments. He believes the comments will be addressed and the document will be sent to the NERC board for approval in the summer of 2009. After NERC board approval, the modification to the NERC Rules of Procedure for the TFE will be sent to FERC for approval and filed with the appropriate Canadian governmental authorities. The modification to the NERC Rules of Procedure becomes effective after regulatory approvals. Scott noted that NERC staff will not be provided individual responses to each comment. See, http://www.nerc.com/filez/standards/Project_2008-06_Cyber_Security.html

III. VSL and VSR Committee Update

Dave Taylor, NERC staff, provided an update on VSL/VSR process. FERC issued a recent order on two standards. FERC said in their order that it was not sure about the use of a 'roll-up' approach to VSLs. FERC asked that NERC provide further explanation of the approach. The VSLs proposed for CIP-002 through CIP-009 have included some of these roll-up VSLs

embedded in them. He noted that the there may to be a future reassessment if FERC doesn't allow for this approach.

Mr. Taylor noted that VRF (violation risk factors) must be assigned to each requirement and any sub requirement. The team that was working on these assigned the VSL's at the requirement level, rather than at each sub requirement level. Therefore, the VSL's for the CIP standards that have been created may have to be un-wound and applied at the sub requirement level. See http://www.nerc.com/filez/standards/Project_2008-06_Cyber_Security.html

IV. Phase I Response Document Review

During a pre-session on Tuesday morning, a team, lead by Kevin Perry, prepared responses to the comments received in the ballot of CIP Version II. The SDT reviewed each of the draft responses, suggested changes and reached consensus on all of the responses by Thursday morning. Some of the major issues contained in the comments were:

- Comments concerning the constrictive nature of the Technical Feasibility Exception Process;
- Designation of the Senior Manager as overly prescriptive;
- Objections to the inclusion of "continuous" monitoring in CIP-006 for physical security; and
- Several commented and expressed concerns on the reduction from 90 days to 30 days for changes to be made in the standards.

The group reviewed Kevin Perry's initial draft, refined and finalized the team responses to the comments made after the posting of CIP Version II to the industry. The team unanimously adopted the Response Document (16-0) as revised on Thursday morning and asked Kevin Perry with assistance from Joe Bucciero to finalize the document for submission to NERC and to initiate the recirculation ballot. For the final response document see: http://www.nerc.com/filez/standards/Project_2008-06_Cyber_Security.html

V. Review of Media and Congressional Treatment of Cyber Security Issues

The team discussed the publicity and media stories last week regarding the vulnerability of the electric grid raising concern with the hyperbole (characterizing as "Pearl Harbor", "Hiroshima", and "9/11") and lack of evidence for many of the claims. A letter from Representative Markey, House Homeland Security to FERC and draft legislation filed by Senators Rockefeller and Snow were noted.

A. NERC's Response

Michael Assante, NERC's Chief Security Officer, provided the team with a briefing on NERC's response to the media coverage of the last week beginning with the Wall Street Journal article. He noted that NERC has sought to strike the right tone in a complex area of policy and practice. NERC worked behind the scenes with press, congress, FERC and industry associations and issued a press statement noting that the industry is committed to working hard on cyber security and the SDT effort to develop new standards is a leading

example of this effort. While acknowledging the reality of continuing vulnerability, NERC challenged the notion that there was evidence of any cyber security compromises that have adversely affected reliability. He noted NERC is working with industry associations.

He suggested the SDT has a role to play and that it shouldn't be seeking to defend the industry. NERC will be trying to get the message out as to the progress to date and the SDT role in addressing cyber security and reliability.

Member Comments:

- Someone needs to set the media straight on the facts.
- Why not securing the whole infrastructure. What about water, etc.
- External communication plan for SDT not for the industry.
- Need to distinguish between securing and complying?
- Better standard does not imply better security. It is not the be-all-end-all.
- NIST as a dismal failure in federal systems?
- As a vendor, 85% of the approach that electric industry clients want to know: how do I get around this?
- If you look at other industries, their public relations efforts are far more effective. Our industry is doing good things and making a valuable contribution but the industry woefully poor in blowing it own horn.
- Standards with a compliance focus give leverage for IT/cyber managers to get things done right. Tool and level for security. Tell our story.
- Need some communication. CIP standards 1 part of puzzle. NERC alerts and Mike Assante. Not necessarily spokesman for cyber security.
- Need to show we are making progress. Need to get on board on Phase III. Need to establish consensus.
- NERC has been relatively quiet. It appears that NERC gets the industry to do things because they are forced to. The standards should be directed towards getting people on the right path to a secure grid.
- If we and industry don't come forward with reforms, Congress will tell us exactly how to do it and we will not like it.
- Impact Assessment= just the consequences. Technical impact- cyber impact- (level of access and results of exploit) BPS impact- impact of effect of denied or compromised
- Concerned that we seemed focused on external threats and system level compromises. Cyber threats much larger. This may reinforce fear and alarmism related to threats to BPS.
- Insider threats, physical threats. E.g. the NIST family of controls- 17 control areas and none have to do with this type of threat.
- What the venue would be to expand the scope- other aspects of security that don't fit cleanly into matrix?
- How to categorize- e.g. technical impact- other forms of attack that may not be categorized. More inclusive in terms of other forms.

- We would do well in our analysis to first assume the worst case scenario- will that result in BPS impact on that cyber assets. Open breakers, etc. What is the worst that can happen?
- If this is for rapid assessment it will be ok. If this is for the longer term it could confuse the industry.
- Breakthrough- work from planning for the worst possible thing- bad or stupid guy from the inside, bad from outside. Later do a care and feeding. Figure out what problem we are solving. Care and feeding and prevention- handled in 03-009. 002 scope, what do I need to do, how much and where.
- NIST standards- like the simplicity. Little more than wording.
- Matrix doesn't take into account the compromise of one leading to stepping up to others and affect the whole system.
- BPS impact side- operating security event level.
- Make sure the likelihood of the impact is reality based. What are components of BES we need to spell out. What are things we have seen that are likely to happen we should focus on. Flushing out BPS impact.
- General sentiment- useful but content may not be appropriate for what we are trying to do.

B. Representative Markey's letter to FERC

On April 9, 2009 Rep. Edward J. Markey (D-Mass.), Chairman of the House Energy and Commerce Committee Subcommittee on Energy and the Environment, sent a letter to FERC regarding the escalating cyber breaches threatening to compromise the electricity grid. NERC is preparing a set of responses to FERC for their consideration in responding to Representative Markey. Mike Assante welcomed the SDT suggestions for NERC's input to FERC.

Member Comments

- Who loaded their gun on this?
- NERC hopes FERC sets the context. The standards piece is just a part of a greater whole in terms of responding to Congress. Minimum standards- uniformly across system because you are interconnected.
- Standards were to provide a "comprehensive…"
- Care taken in addressing the 3rd bullet. "implementing"
- Compliance enforcement piece; spot checks and audits are beginning-
- CERP started audits last fall on the 13 requirements. Midwest ISO.

C. SDT Communication Efforts Going Forward — A "Key Messages Task Group"

Gerry Freese made a proposal made to put together a comprehensive presentation that might be given to Congressional staffers to get out the message that the industry is taking cyber security seriously and has made great efforts. In addition the message would explain some of the inaccuracies contained in the recent publicity concerning vulnerabilities of the electric grid. Facilitators suggested that the briefing for congress might be created in conjunction

with the update. In general team members supported a message responding to the recent publicity.

Member Comments

- Take advantage of some industry presentation opportunities upcoming and coordinate the message: e.g. Jon Stanford is participating on a RSA Panel? Mike Assante on a RSA panel.
- Don't think about the industry as a monolith. Break it up. Deal with different pieces. 3200 organization in NA half with no SCADA system at all.
- Analysis — 160 systems with a profile of interest to terrorists. Spending time and money on security that doesn't work.
- Cannot stop professional hackers — we put up "honey pots" to trip them up. Operational military networked hacked. Gene Spafford testified before Rockefeller until improve quality we will have problems. Until we get the stuff built into the products, its going to be
- We should be getting congressional staffers together organized, structured, where we are, where we have been. Briefing. If materials prepared, Mike Assante offered to gather staffers. Timing is critical, should happen within 1-2 months.
- In terms of the discussion in DC, there is willingness to hear this message. We should strike while the iron is hot.
- Toiling in anonymity — the public and congress only getting 1 side of the picture.
- We should use all approaches (briefings, conference presentations, press coverage) as vehicles. Premier security event. Opportunity.
- Do we need have professionals help us in shaping the message? We can use some our best industry corporate communications. Concern about "misshaping the message." We should guard against not too much outside influence.
- Staff briefings can help dialogue and discussion.

The Chair suggested the SDT form a "Key Messages Task Group" and solicited members who would want to participate: Gerry Freese agreed to lead the effort, and John Stanford, Jerry Domingo Brewer, Jay Cribb, Dave Norton, Phil Huff, Rich Kinas and Jim Breton all agreed to participate.

VI. SDT Phase II CIP 002 White Paper Review and Refinements

Mr. Langton, SDT facilitator, reviewed the significant progress the team has made together since October 2008 including completing Phase I and agreeing conceptually on a thoughtful mix of CIP and NIST approaches to Phase II. He noted that additional SDT members will need to assist and contribute to the development of the Phase II White Paper. He then set the stage by saying that the point of the Phase II Concept paper presentation is to assure SDT member understanding of the concept and invite ideas for strengthening and clarifying aspects of the concept.

A. Phase II White Paper Review

John Lim introduced the white paper noting contributions from Jackie Collett, Bill Winters, Phil Huff and assistance from Scott Mix in refining the white paper since the March SDT meeting in Orlando. He noted the group met two times by phone and WebEx, convened a SDT WebEx meeting and met this morning. They agreed that they needed additional input and contributions from other SDT members in developing the concept paper. He also noted that the group will need to define terms used in the document. One change in the approach is to move away from a "risk assessment" to an "impact based assessment." He offered the following overview of the concept:

- Identification and categorization of BES Assets.
- Identification of the cyber systems that support functions or BES assets.
- The idea is to combine the two categorizations to supply the categorization for the asset.
- All applicable cyber assets (EMS, substation, relay, etc.) will need to be identified with a categorization level.
- Total impact on the BES system will need to be determined using the table.
- The categorization will then be utilized for the requirements that follow.

R1 — Identification of BES Assets

Member comments

- How will this be done?
- The SDT goal should be to create a set of criteria that are specific enough to characterize BES assets.
- Did David Taylor/NERC have a concept paper on this point? Scott Mix noted a paper was prepared but upon review was not sufficiently on point.
- There were several questions for the small group that was putting this paper together. Several in the group had questions around the role of the planning assessments in determining categorization of BES assets.
- The group answered that planning engineers will need to be involved, but those details had not all been worked out. The group asked for volunteers from SDT members who have planning engineering background.
- Need Power system engineers and transmission planners to assist in this part of the concept. Perhaps people like John Sykes who briefed the SDT in Phoenix?
- Jason Marshall, Midwest ISO volunteered to assist in this effort

R2 — Critical Asset Identification Method
R3 — Critical Asset Identification
R4 — Cyber Asset Identification
R5 — Categorization of Cyber Assets

Member comments

- There was much discussion about the use of RTO's and/or RC's for oversight of the categorization.

- The group also questioned the oversight process and whether that would be done by the RC function or by the regions of NERC. A team member explained that RC's, RTO's, etc. may not want to oversee the process and categorization due to liability concerns.

R6 — Annual Approval

Member comments

- What about third party oversight? Third party oversight is provided for in the whitepaper as was specified in FERC Order 706.

Member final comments on the Concept

- Need to acknowledge that the way the SDT is working is different.
- We need to address all sections of the white paper and stay at a fairly high level.
- We know we have agreement. Address shortcomings of the current system.
- Cover all the BES assets not just the critical — categorize all.
- Cover all relevant cyber systems related to BES assets.
- The focus on reliability of functions.
- 5 major points list. Short paragraph on each to enable Jerry fields questions. Enough
- Does this build on principles and on industry investments?
- Flexibility is important

The facilitator asked if any of the SDT members had any fundamental difficulty with the approach and then polled the SDT members as to whether all were comfortable at the conceptual level with the current white paper approach. All members agreed to go forward indicated that liked the direction the white paper was taking. All acknowledged that they would continue to test this as the details were developed.

B. Phase II Consensus Points — Preparing for the Member Representative Committee Presentation

On day two, John Lim and Phil Huff agreed to draft some general draft consensus points from the white paper that could be presented by the Chair to the NERC Members Representative Committee on May 4, 2009. They were jointed by Jackie Collett, Scott Rosenberg, John Varnell and Rich Kinas. The SDT agreed to review and refine these on Thursday morning.

Below is the initial draft and strikethrough/underlined following the SDT discussion.

1. **The Standards should require a BES impact assessment as an initial approach to categorizing BES Cyber Systems. ~~The Standards will require a BES impact assessment as opposed to risk based assessment.~~**

   Member Comments

   - Drafters intended this as a "soft ball."

- Didn't have the criteria to do a risk based assessment.
- "As an approach to Risk based assessment."?
- Standards "will"? The proposed version "will seek to"?
- Concerned about the removal of risk based in #1
- Agree. the standards will incorporate ~~be primarily~~ ~~based solely on~~ a BES impact assessment. Include a BES impact assessment in lieu of a risk based assessment.
- If keep in, consider "instead of a primarily risk based assessment"
- CIA- risk management is also an accepted lexicon.
- Members agreed with changes reflected above.

2. **The impact categorization of Cyber Systems will be based on reliability functions of the BES to achieve Adequate Levels of Reliability.**

   Member Comments
   - None, ok

3. **The Standard's BES Impact Assessment will ~~include categorizing~~ consider a categorization process ~~all BES assets~~**

   Member Comments
   - If you categorize "all", will still come up with equivalences
   - Uncomfortable with "all" Haven't defined at what level we are going to categorize. "More" vs. "all"? Delete "all"
   - Categorize now as critical and non critical. Flag each asset or classes
   - "categorize all BES assets"?
   - "More categories"
   - Will each have some security requirements associated with it?
   - Will consider including more categories than we have today.
   - "risk" or "impact" categories. Impact level categories than previous versions of CIP
   - Will include a categorization process.
   - Members agreed with changes reflected above.

4. **The Standards will require oversight of the categorized list of BES assets by entity types which have a more complete wide-area view of the BES.**

   Member Comments
   - None, ok

5. **The Standards will categorize ~~and apply security requirements (or controls) to all~~ Cyber Systems supporting, either directly or indirectly, the reliability functions of the BES and apply security requirements (or controls) that are commensurate and**

appropriate to their potential impact on the BES. ~~**The standards will require Entities to apply security controls to Cyber Systems commensurate and appropriate to their potential impact on the BES.**~~

Member Comments

- "All"?
- Categorize requirements "to those systems."?
- Members agreed with changes reflected above.

6. **The final Cyber System categorization will reflect the impact to the BES based on a** ~~**security incident i.e.**~~ **loss of availability** ~~**confidentiality,**~~ **integrity,** ~~**and/or**~~ **confidentiality** ~~**availability**~~ **of the Cyber System.**

   Member Comments

   - Shows how we are going to do the categorization.
   - "Loss of confidentiality"?
   - Standard lexicon — remove reference to "incident" CIA standards order
   - Switch confidentiality to last and availability to first?
   - Data confidentiality is a concern.
   - Cyber system — impact of cyber assets if compromised. Doing a translation from power engineering and cyber engineering side of the house. Need to be understood by the multiple disciplines.
   - Military is focused on confidentiality and that was the primary driver of the early models.
   - If take off table, we are presupposing it is not important.
   - "As appropriate?
   - Data and system integrity? Common understanding? Normal understanding includes.
   - The order doesn't matter.
   - Data applied to system only? No. we have background check requirements.
   - Members agreed with changes reflected above.

7. **The Standards will provide Organizations with reasonable flexibility** ~~**should have reasonable flexibility**~~ **in applying equivalent security controls on the basis of compensating controls and environmental considerations.**

   Member Comments

   - Members agreed with changes reflected above.

8. **The Standards will address the complex nature of BES functions and interconnected Cyber Systems, both within and between multiple organizations.**

   Member Comments

- Members agreed with changes reflected above.

9. **The Standards will state explicit criteria for the BES Impact Assessment.**

   Member Comments
   - Missing criteria for the cyber impact assessment? Add an additional point.
   - Use and misuse of cyber assets
   - This is concept not detailed idea.

10. **The Standards will state explicit criteria for the Cyber Impact Assessment (including use and misuse of cyber systems).**

    Member Comments
    - Members agreed with adding the new point reflected above.

11. **The Standards will include a methodology to merge the BES Impact Assessment and Cyber Impact Assessment into a final Cyber System categorization.**

    Member suggestions for the MRC presentation
    - Use the flow chart to present
    - Use diagrams where possible to illustrate the concept.
    - Keep in mind that MRC mostly senior mgrs VP- markets,
    - A participant on the phone suggested the SDT consider the following language as part of the consensus point, "Seek to have more understandable, streamlined with fewer cross references, clearer set of standards." The chair noted these consensus points were to present to the MRC the sense of the SDT on how they agreed to go forward for Phase II standards development. She noted the language suggested may or may not reflect the sense of the SDT at this point. The facilitator suggested that the comment would be included in the meeting summary.

Acceptability Ranking Scale	4 = acceptable, I agree	3 = acceptable, I agree with minor reservations	2 = not acceptable unless major reservations addressed	1 = not acceptable	Avg.
Consensus Points	**10 (5/5)**	**2**	**0**	**0**	**3.8 of 4**

The Chair will base her MRC presentation on these consensus points. She will also put these points in a narrative format for a letter to Mike Assante as part of the SDT's input to NERC as it develops its input to FERC in response to Rep. Markey's letter.

VII. Workplan, White Paper, Meeting Evaluation and Next Steps

A. 2009 SDT Workplan Approach

Bob Jones, SDT facilitator presented the concept of CIP-002- requirements and measures being the work undertaken for the rest of 2009 with the goal of posting for industry comments on a complete CIP-002 standard and go to ballot on it. This might include taking a requirement from CIP-003 through CIP-009 to illustrate how CIP-002 would relate to the later development of CIP-003 through CIP-009. Scott Mix noted that it would be important to get CIP-002 to industry ahead of consideration of the catalogue of controls. The SDT would then develop the entire CIP-003 through CIP-009 package and post for comments and balloting as a complete package. The schedule proposes that the SDT will be into 2012 when a full version of CIP version III is posted for comments.

Phil Huff noted that Bill Winters suggested NIST has done a lot of work on guidelines. The SDT may want to dedicate a future meeting to get input and cooperation from those experts familiar with implementing NIST. John Varnell reminded team members that Keith Stoffer, John Stanford and Jeri Brewer were on the team to bring that perspective.

B. Workplan Schedule

The Chair reminded people to register for the Boulder City meeting and that the September meeting would take place in Folsom, California near Sacramento and not in Denver.

Proposed Dates and Locations for Future Meetings 2009

Dates in 2009	Location
April 14–16	Charlotte
May 13–14	Boulder City, NV
June 17–18	Portland
July 13–14	Toronto
August 20–21	Chicago
September 9–10	Folsom, California
October 20–22	New Orleans
November 17–18	Atlanta
December 15–17	Tampa (FRCC)

C. CIP 002 White Paper Development.

CIP 002 White paper development: The sub team will continue working on the parts of the white paper that need development. Categorization of the BES assets still needs refinement and help. The sub team asks for assistance from outside the group. Scott Mix will take the lead to see if additional expertise can be provided to the sub team.

D. Meeting Evaluation — What worked and what could be improved?

Wireless connectivity has turned out to be an expectation of the group. On the final day of the Charlotte meeting, connectivity was intermittent for some members.

What did the SDT accomplish?

- Got through recommendations and responses to industry comments to enable the recirculation ballot.
- Identified the need for communication within and beyond the industry.
- Made a big step forward in consensus on the principles to be included in the white paper.

What things helped us to accomplish these?

- Strawman documents are very helpful — e.g. Kevin's response document.
- Getting facilitators to the meeting.
- Having a quorum.
- Having the WebEx stay up.
- Continued open engagement and attention of all SDT members.
- Silence is golden consent rule worked well.

What suggestions are there for the future?

- Periodically spend about 30 minutes brainstorming future concepts/ideas that may become topics for future white papers.

The Chairman thanked the host (Duke Energy) and is looking forward to hosting the SDT meeting in Boulder City. The SDT adjourned at 11:45 a.m. on April 16.

Appendix # 1 — Meeting Agenda

April 14, 2009 | 1–7 p.m. EST
April 15, 2009 | 8 a.m.–7 p.m. EST
April 16, 2009 | 8 a.m.–noon EST
Duke Office — Conference room number 2313
400 South Tryon St
Charlotte, NC

Proposed Meeting Objectives and Outcomes

- Receive updates on TFE and VSL processes
- Receive a briefing on the NERC Critical Assets Industry Survey
- Review and Draft Responses to Phase I Industry Comments
- Review and Refine Phase II Framework White Paper
- Agree on assignments and next steps in the SDT Work plan.

Tuesday, April 14, 2009

1. Phase II White Paper Team Drafting Session
2. Welcome and Opening Remarks — Jeri Domingo-Brewer and Kevin Perry
    a. Roll Call
    b. NERC Antitrust Compliance Guidelines
    c. Review and adoption of March 10-12, 2009 Meeting Summary
3. Review of Meeting Objectives, Agenda and Meeting Guidelines — Jeri Domingo and Bob Jones
4. Organizational Issues and Review of Phase 1 and early Phase II Schedule — Stuart Langton
    - Review of April-December 2009 SDT Schedule
5. Update on Technical Feasibility Exception (TFE) NERC Rules of Procedure Posting — Scott Mix
6. Update on VSL/VSR for Version 1 and 2 CIP-002-009 — David Taylor
7. Overview of SDT Phase II Development Process Steps and CIP 002 Review — Stu Langton
8. Critical Assets Industry Survey — Mike Assante
9. CIP-002 White Paper Presentation — Bill Winters and Jackie Collett
10. Q & A and Discussion and Initial Consensus Testing
11. Break
12. Phase I Small Group Proposal for Response Drafting
13. Small Groups Draft Responses to Industry Comments
14. Break — If Needed, Small Groups may continue working until 7:00 p.m.
15. Recess

Wednesday, April 15, 2009

1. Welcome, Agenda Review and Roll Call

2. Phase I Small Group — Draft Responses to Industry Comments
3. Break
4. Phase I Small Group — Draft Responses to Industry Comments
5. Working Lunch
6. Small Group Reports and SDT Review and Consensus Testing of Draft Responses
7. Break
8. Small Group Reports and SDT Review and Consensus Testing of Draft Responses
9. Break — If Needed, Full or Small Groups may continue working until 7:00 p.m.
10. Recess

Thursday, April 16, 2009

1. Welcome, Agenda Review, and Roll Call
2. CIP-002 White Paper Consensus Testing
3. Break
4. CIP-002 White Paper Consensus Testing
5. Review of May SDT Agenda and Objectives
6. Meeting Evaluation — What Worked, What Could be Improved?
7. Adjourn

Appendix #2 — Attendees List for March 10–12, 2009 Meeting in Orlando, Florida

Attending in Person — SDT Members

1. Rob Antonishen	Ontario Power Generation *(Tuesday and Wednesday)*
2 Jeri Domingo-Brewer, Chair	**U.S. Bureau of Reclamation**
3. Jay S. Cribb	Information Security Analyst, Southern Company Services, Inc.
4. Sharon Edwards	Duke Energy
5. Scott Fixmer	Senior Security Analyst Exelon Corporate Security, Exelon Corp.
6. Gerald S. Freese	Director, Enterprise Information Security America Electric Power
7. John Lim	CISSP, Department Manager, Consolidated Edison Co. NY
8. Frank Kim	Ontario Hydro
9. David Norton	Policy Consultant, CIPEnergy Corporation *(Tues & Wed.)*
10. **Kevin B. Perry, Vice Chair**	Director, IT-Infrastructure, Southwest Power Pool
11.Keith Stouffer	National Institute of Standards & Technology
12. John D. Varnell	Technology Director, Tenaska Power Services Co.
1. Roger Lampilla	*NERC*
2. David Taylor	*NERC (Tuesday)*
3. Scott R. Mix	*NERC*
4. Tom Hoffstetter	*NERC (Formerly Midwest ISO, Inc)*
4. Joe Bucciero	*NERC/Bucciero Assoc.*
6. Robert Jones	*FSU/FCRC Consensus Center (Wed. & Thursday)*
7. Stuart Langton	*FSU/FCRC Consensus Center*
Hal Beardall	*FSU/FCRC Consensus Center*

SDT Members Attending via WebEx and Phone

13. Jackie Collett	Manitoba Hydro
14. Joe Doetzl	
15. Phillip Huff	Arkansas Electric Coop Corporation
16. Richard Kinas	Orlando Utilities Commission
17. Scott Rosenberger	Luminant Energy
18. Kevin Sherlin	Sacramento Municipal Utility District
19. Jonathan Stanford	Bonneville Power Administration

SDT Members Unable to Attend

1. Joe Doetzl	Manager, Information Security, Kansas City Power & Light Co.
2. Christopher A. Peters	ICF International
3. David S. Revill	Georgia Transmission Corporation
4.William Winters	Arizona Public Service, Inc.

Others Attending in Person

Jim Breton	ERCOT
Travis Jafray	Subnet Solutions
Jason Marshall	Midwest ISO
Darren Highfill	ENERNEX
Sam Morrell	CERT

Others Attending via WebEx and Phone

Chris Wright	
James Bassett	Lafayette
David Huff	FERC
Bob Tallman	E.ON
Chris Wright	Burns & Mac
Raghu Rayalu	SCE (Wed.)

Appendix # 3
NERC Antitrust Compliance Guidelines

I. General

It is NERC's policy and practice to obey the antitrust laws and to avoid all conduct that unreasonably restrains competition. This policy requires the avoidance of any conduct that violates, or that might appear to violate, the antitrust laws. Among other things, the antitrust laws forbid any agreement between or among competitors regarding prices, availability of service, product design, terms of sale, division of markets, allocation of customers or any other activity that unreasonably restrains competition.

It is the responsibility of every NERC participant and employee who may in any way affect NERC's compliance with the antitrust laws to carry out this commitment.

Antitrust laws are complex and subject to court interpretation that can vary over time and from one court to another. The purpose of these guidelines is to alert NERC participants and employees to potential antitrust problems and to set forth policies to be followed with respect to activities that may involve antitrust considerations. In some instances, the NERC policy contained in these guidelines is stricter than the applicable antitrust laws. Any NERC participant or employee who is uncertain about the legal ramifications of a particular course of conduct or who has doubts or concerns about whether NERC's antitrust compliance policy is implicated in any situation should consult NERC's General Counsel immediately.

II. Prohibited Activities

Participants in NERC activities (including those of its committees and subgroups) should refrain from the following when acting in their capacity as participants in NERC activities (e.g., at NERC meetings, conference calls and in informal discussions):

- Discussions involving pricing information, especially margin (profit) and internal cost information and participants' expectations as to their future prices or internal costs.
- Discussions of a participant's marketing strategies.
- Discussions regarding how customers and geographical areas are to be divided among competitors.
- Discussions concerning the exclusion of competitors from markets.
- Discussions concerning boycotting or group refusals to deal with competitors, vendors or suppliers.

III. Activities That Are Permitted

From time to time decisions or actions of NERC (including those of its committees and subgroups) may have a negative impact on particular entities and thus in that sense adversely

impact competition. Decisions and actions by NERC (including its committees and subgroups) should only be undertaken for the purpose of promoting and maintaining the reliability and adequacy of the bulk power system. If you do not have a legitimate purpose consistent with this objective for discussing a matter, please refrain from discussing the matter during NERC meetings and in other NERC-related communications.

You should also ensure that NERC procedures, including those set forth in NERC's Certificate of Incorporation and Bylaws are followed in conducting NERC business. Other NERC procedures that may be applicable to a particular NERC activity include the following:

- Reliability Standards Process Manual
- Organization and Procedures Manual for the NERC Standing Committees
- System Operator Certification Program

In addition, all discussions in NERC meetings and other NERC-related communications should be within the scope of the mandate for or assignment to the particular NERC committee or subgroup, as well as within the scope of the published agenda for the meeting.

No decisions should be made nor any actions taken in NERC activities for the purpose of giving an industry participant or group of participants a competitive advantage over other participants. In particular, decisions with respect to setting, revising, or assessing compliance with NERC reliability standards should not be influenced by anti-competitive motivations.

Subject to the foregoing restrictions, participants in NERC activities may discuss:

- Reliability matters relating to the bulk power system, including operation and planning matters such as establishing or revising reliability standards, special operating procedures, operating transfer capabilities, and plans for new facilities.
- Matters relating to the impact of reliability standards for the bulk power system on electricity markets, and the impact of electricity market operations on the reliability of the bulk power system.
- Proposed filings or other communications with state or federal regulatory authorities or other governmental entities.
- Matters relating to the internal governance, management and operation of NERC, such as nominations for vacant committee positions, budgeting and assessments, and employment matters; and procedural matters such as planning and scheduling meetings.

Any other matters that do not clearly fall within these guidelines should be reviewed with NERC's General Counsel before being discussed.

Appendix #4
January–December Draft Project Schedule (Revised April 2009)

OVERVIEW

- **13 SDT Face-to-Face Meetings**
- **Multiple SDT subgroup and subcommittees WebEx Meetings**
- **One Cyber Expert and Stakeholder Workshop (**Summer/Fall 2009 — Tentative)
- **Industry Comments on CIP-002 SDT White Paper** (June–July 2009)
- **2 NERC Members Representative Committee Meetings,** (May & August 2009)

SDT Draft Schedule — January-December 2009

1. **January 7–9 Meeting in Phoenix, AZ** (half, full, half day format Wednesday–Friday)
   - Review of Technical Feasibility Exceptions white paper
   - Review of Industry Comments on Phase 1 products — Establish and convene small groups to draft responses
   - Review of Phase 2 White papers

January 15 WebEx meeting(s)
- Small group draft responses to industry.

January 21 WebEx meeting(s)
- Small group draft responses to industry.

2. **February 2–4 Meeting in Phoenix, AZ** (half, full, half day format Monday–Wednesday)
   - Update on NERC Technical Feasibility Exceptions process
   - Review of VSL process and SDT role
   - Review of Phase 2 White papers, strawman and principles
   - Review and Adoption of SDT Responses to Industry Comments on Phase I and Phase I Product Revisions.

3. **February 18–19 Meeting in Fairfax, VA**
   - Update on Phase I process
   - Update on NERC TFE process
   - Update on VSL Team process
   - Review, discussion and refinement of Phase II and CIP-002 White papers, strawman and principles

4. **March 10–11 Meeting in Orlando, FL** (half, full, full day format)
   - Update on NERC TFE process
   - Update on VSL Team process
   - Review and Refinement of Phase II CIP 002 Strawman Proposals

March 2–April 1 — 30-day Pre Ballot
Mid-March — NERC posts TFE draft Rules of Procedure for industry comment
March 30 — WebEx meeting(s) White Paper Drafting Team
April 1–10 — NERC Balloting on Phase 1 Products
April 6 — WebEx meeting — White Paper Drafting Team
April 8 — WebEx meeting(s) — White Paper Preview — Full SDT Conference Call
April 11 — Phase I Ballot Results and Industry Comments

5. **April 14–16 Meeting in Charlotte NC** (half, full, half day format Wednesday–Friday)
   - Update on NERC TFE process
   - Update on VSL Team process
   - Update on the NERC Critical Assets Survey
   - Review in SDT small groups and respond to Phase I Ballot Results and Industry Comments
   - Review and Refinement of Phase II Whitepaper and Progress Report to MRC

May 4 — Member Representative Committee Meeting in Arlington, VA — SDT progress report.

6. **May 13–14 Meeting in Boulder City NV** (2-day format Wednesday–Thursday)
   - Review MRC presentation and any input to SDT on Phase II white paper
   - Further SDT refinement of the strawman Phase II White Paper in plenary and small groups.

7. **June 17–18 Meeting in Portland OR** (2-day format)
   - Further SDT refinement and adoption of the Draft Phase II White Paper for industry comment.
   - Review potential SDT subcommittee structure and work plan for implementation of Phase II.

~~**Industry Comment Period on SDT Phase II White Paper- 45 days** (June 20-August 5, 2009)~~

8. **July 13–14 Meeting in Toronto, ON**
   - Agree on and charge subcommittees and conduct organizational meetings
   - SDT Subcommittees meet to organize and begin drafting revisions to CIP and/or addressing assigned issues.
   - Subcommittee organizational reports to SDT

July–August WebEx meeting(s)
- SDT Subcommittee meetings to review applicable industry input on white paper

9. August 20–21 Meeting in Chicago, IL

- SDT Plenary and Subcommittee meetings to review and respond to industry input on white paper.

August 2009 — NERC Member Representative Committee, Presentation of the Phase 2 White Paper and Summary of Industry Comment and Response for MRC input, Winnipeg, Manitoba

10. September 9–10 Meeting in Denver, CO

- SDT Plenary review industry and MRC input on White paper and consider and agree on refinements
- SDT Subcommittee drafting meetings
- SDT Plenary Session(s)- briefings and subcommittee reports
- Review Workplan through Summer, 2010, as needed

September WebEx meeting

- SDT Subcommittee drafting meetings

11. October 20–22 Meeting in New Orleans, LA

- SDT Subcommittee drafting meetings
- SDT Plenary Session(s)- briefings and subcommittee reports
- Adopt Workplan through Summer, 2010, as needed

October WebEx meeting

- SDT Subcommittee drafting meetings

12. November 17–18 Meeting in Atlanta, GA

- SDT Subcommittee drafting meetings
- SDT Plenary Session(s)- briefings and subcommittee reports

November WebEx meeting

- SDT Subcommittee drafting meetings

13. December 15–17 Meeting in Tampa, FL

- SDT Plenary Session(s)
- SDT Subcommittee drafting meetings

December WebEx meeting

- SDT Subcommittee meetings

Appendix #5 — Rep Markey's Letter to FERC

COMMITTEES
ENERGY AND COMMERCE
SUBCOMMITTEE ON ENERGY AND ENVIRONMENT
CHAIRMAN
SELECT COMMITTEE ON ENERGY INDEPENDENCE AND GLOBAL WARMING
CHAIRMAN
NATURAL RESOURCES

EDWARD J. MARKEY
7TH DISTRICT, MASSACHUSETTS

Congress of the United States
House of Representatives
Washington, DC 20515–2107

2108 RAYBURN HOUSE OFFICE BUILDING
WASHINGTON, DC 20515–2107
(202) 225–2836
DISTRICT OFFICES:
5 HIGH STREET, SUITE 101
MEDFORD, MA 02155
(781) 396–2900
188 CONCORD STREET, SUITE 102
FRAMINGHAM, MA 01702
(508) 875–2900
http://markey.house.gov

April 9, 2009

The Honorable Jon Wellinghoff
Chairman
Federal Energy Regulatory Commission
888 First Street, NE
Washington, DC 20426

Dear Chairman Wellinghoff:

I have long been concerned about threats to our energy infrastructure, from terrorist attacks on LNG facilities to assaults on nuclear power plants from the air or the ground. Recent reports raise concerns about a more modern threat: cyber attack to our nation's electricity generation and transmission infrastructure. This matter warrants serious attention and I ask your assistance as we investigate the nature of the threat and what can be done to repel it.

As you know, the North American Electric Reliability Corporation, which is mandated to ensure the reliability of the nation's electricity supply, recently completed a survey of industry stakeholders to determine compliance with the Critical Cyber Asset Identification Standard. The results of this survey raise two issues of serious concern. First, the survey makes clear that industry has not fully adhered to this Standard, which is only concerned with identifying – not defending – facilities and equipment critical to the reliability of the electrical supply. This lack of adherence by industry to the Standard is disturbing because it indicates the vulnerability of the nation's electrical grid to cyber attack. If we have not yet even identified which assets need to be defended from cyber attack, how can we possibly defend them?

The second, and more disturbing, concern arises from recent news reports that the computer-based infrastructures of the grid have been repeatedly and systematically compromised through the Internet by foreign nations and groups. All Americans are troubled to learn that foreign nations and potentially hostile groups are apparently preparing a detailed "map" of the grid and its vulnerabilities, possibly to be used to facilitate some sort of attack in the future.

In light of these reports on growing threats to our electrical grid, I request additional information on what steps the Federal Energy Regulatory Commission (FERC) is taking to respond to these threats in the near term and prevent such breaches in the future.

In January of 2008, FERC approved eight mandatory critical infrastructure protection (CIP) standards, as developed by the North American Electric Reliability Corporation, to protect the nation's grid from cyber security attacks and other reliability breaches. The mandatory reliability standards required certain users, owners and operators of the bulk power system to

PRINTED ON RECYCLED PAPER

establish policies, plans and procedures to safeguard physical and electronic access to control systems, to train personnel on security matters, to report security incidents, and to be prepared to recover from a cyber incident. These standards were to provide a "comprehensive set of requirements to protect the Bulk-Power System from malicious cyber attacks."

Please answer the following questions regarding FERC's actions in response to these threats and what additional measures may need to be taken by the industry, the Commission, and by Congress.

- What is the Commission's view of the results of the North American Electric Reliability Corporation survey? What percentage of Critical Cyber Assets have been identified? What is the significance of the information backbone of the electric grid being compromised? What immediate steps is the industry taking to stop these breaches?
- If foreign nations or hostile groups already have gathered detailed information to develop a "map" of the electricity grid, what actions can be taken now to prevent this information from being used to attack the grid?
- Have the CIP standards been fully implemented by industry? If not, why not?
- Are the current CIP standards sufficient to prevent cyber-security attacks and to respond to breaches? If not, what additional standards are needed?
- Has FERC developed metrics to measure the efficacy of the CIP standards? If so, what are these metrics? If not, why not?
- What processes are on-going at NERC to identify the need for new cyber-security standards?
- Is too much discretion given to industry participants in creating the cyber-security standards, since two-thirds of the group's members must support a standard before it is adopted or modified?
- What authorities does FERC possess to prevent and respond to cyber-security threats and breaches? Does FERC need additional authorities to protect the electricity grid from these threats?

Thank you for the attention to these matters. If you have any questions regarding this request, please contact Will Huntington of my staff at 202-225-2836.

Sincerely,

Edward J. Markey

Edward J. Markey
Chairman
Subcommittee on Energy and
The Environment

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Appendix #6
Phase 2 White Paper (April 5, 2009)

Categorizing Cyber Systems

An Approach Based on BES Reliability Functions

NERC Cyber Security Standards Drafting Team for Order 706
4/14/2009

CATEGORIZING CYBER SYSTEMS: AN APPROACH BASED ON IMPACT ON BES RELIABILITY FUNCTIONS

EXECUTIVE SUMMARY

Intentionally left blank – to be redacted last

INTRODUCTION

The North American Electric Reliability Corporation (NERC) Reliability Standards are a set of standards aimed at preserving and enhancing the reliability of the Bulk Electric System (BES). The objective of the CIP series of these standards is to protect the critical infrastructure elements necessary for the **reliability and operability** of this system. One must not forget the overarching mission of preserving and enhancing the reliability of this system, which consists of assets engineered to perform functions to achieve this objective. The CIP Cyber Security Standards define cyber security requirements to protect cyber systems used in support of these functions and the reliability and operability of these assets.

CIP-002 – Cyber Security – Critical Cyber Asset Identification requires "the identification and documentation of the Critical Cyber Assets associated with the Critical Assets that support the reliable operation of the Bulk Electric System. These Critical Assets are to be identified through the application of a risk-based assessment." In reviewing the current CIP-002 version, the drafting team considered FERC's comments in its Order 706 approving the Cyber Security Standards and common perceptions and observations from various other commenters. In particular, the Standard Drafting Team considered these characteristics of the current CIP-002 approach which needed to be addressed beyond a first revision standard:

- A piecemeal approach
- Not protecting assets needing protection
- Allows "gaming" in the application of the requirements
- Uses an all or nothing approach
- Concentrates on loss of an asset and requires more explicit consideration of loss of integrity or misuse

This paper describes an approach based on the concepts of NERC's definition of Adequate Level of Reliability (ALR) and the characteristics of the BES described therein that will achieve this ALR, namely:

1. The System is controlled to stay within acceptable limits during normal conditions;
2. The System performs acceptably after credible Contingencies;
3. The System limits the impact and scope of instability and Cascading Outages when they occur;
4. The System's Facilities are protected from unacceptable damage by operating them within Facility Ratings;
5. The System's integrity can be restored promptly if it is lost; and
6. The System has the ability to supply the aggregate electric power and energy requirements of the electricity consumers at all times, taking into account scheduled and reasonably expected unscheduled outages of system components

In particular, the approach relies on the identification of functions which are essential to achieving these characteristics and the BES assets which support these functions. These BES assets may be defined as facilities, equipment or systems performing functions to ensure that the BES achieves an Adequate Level of Reliability.

The methodology proposes to identify all cyber systems essential to the reliable operation of these BES assets: one must note that a cyber system can itself be a BES asset if it directly performs one or more of the identified functions.

Once BES assets and their cyber systems are identified, the methodology proposes a two pronged categorization which results, on one side, in a categorization of BES assets based on their impact on the reliability and operability of the BES, and on the other, a categorization of their associated cyber systems and their elements based on their impact on the BES assets they support. A rigorous merger of the two categorizations for any given cyber system results in a deterministically derived categorization of each cyber system based on its impact on the BES.

One must note that the scope of the CIP Cyber Security standards as defined during the SAR drafting team discussions exclude the elements associated with the market functions UNLESS they also affect the reliable operation of the BES. In addition, these standards explicitly exclude facilities, equipment and systems regulated by US and Canadian nuclear regulatory bodies, since they are regulated outside of NERC. Note that there may be facilities, equipment or systems which may be in a nuclear facility associated with the BES which are outside of the regulatory realm of these nuclear regulatory organizations, and would therefore be regulated under these NERC CIP standards. It is also worth noting is that the CIP Cyber Security Standards do not include those assets associated with BES Planning activities UNLESS they also have a direct effect on the reliable operation of the BES. There will however be cases where these types of BES Planning and market function systems may be required to be protected under the CIP standards if they meet the protection requirements of the Cyber Security Standards (e.g. if they are within an Electronic Security Perimeter which is subject to the standards).

The concepts associated with an impact based approach to determining the criticality of certain facilities, equipment and systems are particularly well covered in the Draft Volume 1 of NERC's Security Guideline for the Electric Sector: Identifying Critical Assets. The development of this guidance document was in direct response to a directive by FERC in Order 706. An additional important concept in this approach is the inclusion of assets based on their functions in the operation of the BES. The group is currently engaged in Part 2 of the series, which addresses the identification of Critical Cyber systems.

The concepts and approach in this paper draw on elements of approaches already defined in several presentations by members of the Cyber Security Standards Drafting Team for Order 706 (CSSDTO706) to the drafting team. The approach on the identification and classification of BES assets also draws heavily on the work done by the NERC Risk

Assessment Working Group on the Draft Security Guideline for the Electric Sector: Identifying Critical Assets and current work being done by this group in the Identification of Critical Cyber Assets. The presentations by CSSDTO706 members to the group include the application of a FIPS199-like approach to classifying Cyber systems, NIST integration, a cyber systems based approach and discussions on Guiding Principles used for development, as well as comments and discussions by other members of the drafting team.

The overall approach includes the consideration of NERC's mission, the essential functions necessary in achieving this mission, an impact based methodology to categorize its BES assets and the associated cyber systems engaged in the process, and finally the deterministic derivation of an overall impact based categorization of the cyber elements, with the anticipated application of cyber security requirements commensurate with that categorization. This is in keeping with general approaches to risk management practices, which focus first on identifying key processes necessary for meeting high level objectives, then drilling down into supporting processes.

BES RELIABILITY FUNCTIONS

A pre-requisite to the start of the identification of BES assets which affect the reliability and the operability of the BES is the identification of functions which support the characteristics of ALR.

These include, at a minimum, support for:

1. Generation for the BES
2. Transmission for the BES
3. Voltage and voltage stability in the BES
4. Frequency and frequency stability in the BES
5. Protection of BES generation and transmission equipment from damage
6. Control and operation of BES assets
7. Wide-area situational awareness for real-time BES reliability and operability
8. Restoration of the BES

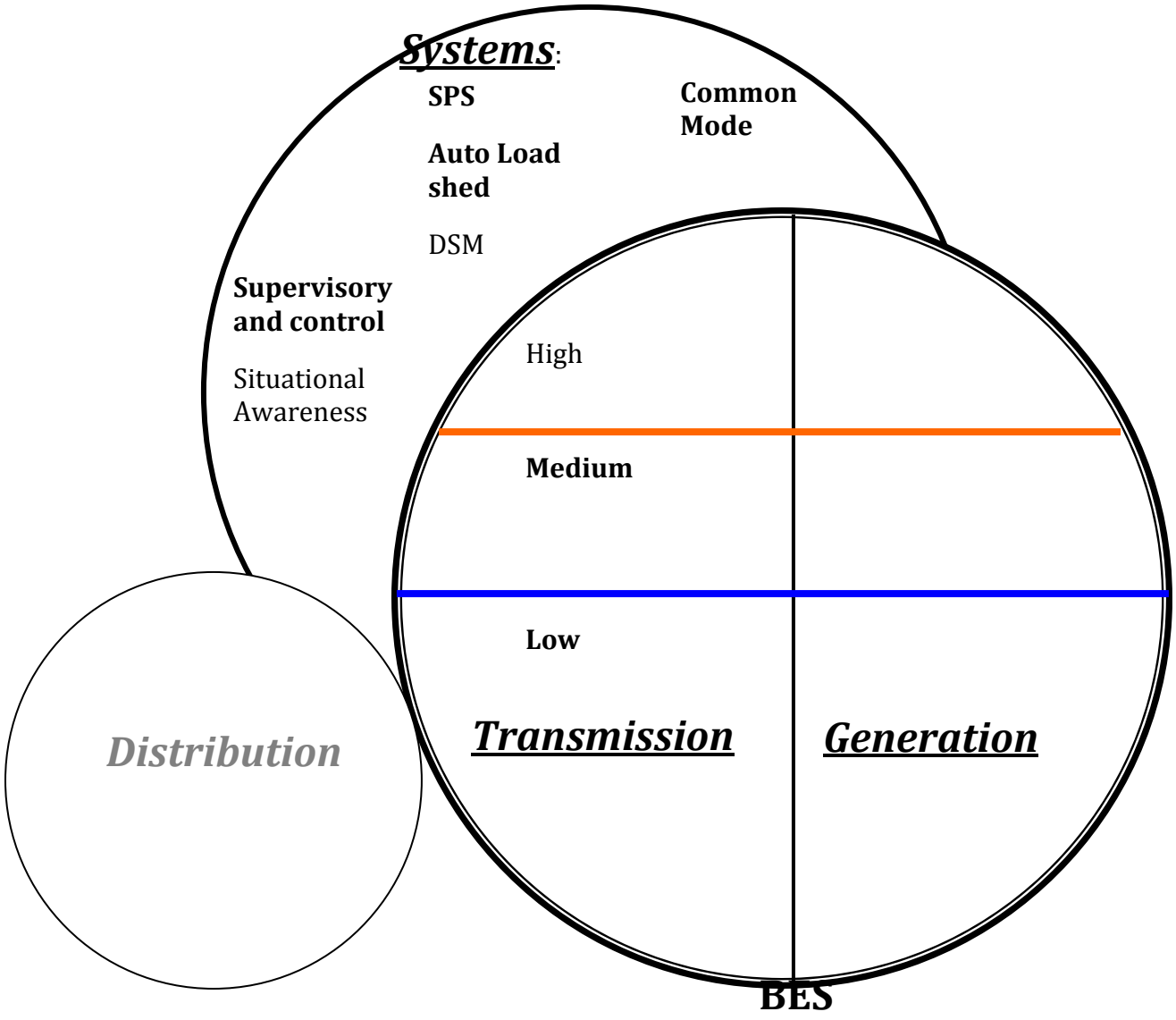
IDENTIFICATION OF BES ASSETS

The functions above are then used to identify all BES assets which support them. The inclusive list of these identified BES assets constitute the overall scope for application of criteria for their categorization based on their impact on the reliability and operability of the BES as defined by the characteristics of an ALR. In addition to facilities and equipment, the included BES assets must include systems which perform the following, at a minimum:

– Situational awareness

- Supervisory and control capability
- Special Protection Systems
- Systems essential to BES restoration
- Systems performing automatic load shedding
- Other systems that may perform a function directly related to the reliability or operability of the BES.

Bulk Power Assets



CATEGORIZATION OF BES ASSETS

(I would propose that we review the criteria defined in the Critical Asset Identification Guideline in the Transmission, Generation, Control Center and Special Systems sections (tables) be used as a minimum set for defining High Impact BES assets. I do not know how practical it is to ask a separate group, as discussed in the last SDT session, to come up with the categorization standards, unless substantial other work which can be translated into a categorization standard has already been done in this area. The guideline uses operating limits as credible criteria for determining criticality: I think the operating folks will be hard pressed further classifying this. Let's see what Dave Taylor provides at the next session. In the absence of adequate prior work, I am strongly tempted to propose using a 2 tier approach (i.e. a 2x3 matrix), High and Low for assets, and H,M,L for Cyber Systems. Anyway, whatever categorization scheme for assets goes here depending on what is determined).

Try for support from operations and planning committees to help define criteria for assigning assets to impact levels of high, medium, low, and none or others.

THIRD PARTY OVERSIGHT OF BES ASSETS AND THEIR CATEGORIZATION

An additional concept introduced in the approach is the inclusion of oversight of the critical asset list by entity types which have a more complete wide-area view of the BES. The approach uses a hierarchical approach to the oversight structure.

- Entities performing the functions of Balancing Authority, Interchange Authority, Transmission Service Provider, Transmission Owner, Transmission Operator, Transmission Operator, Generator Owner, Generator Operator, and/or Load Serving Entity submit their list of Critical Assets to their Reliability Coordinator for review.
- Each Reliability Coordinator submits its list of Critical Assets to its Regional Entity for review.
- Each Regional Entity submits its list of Critical Assets to NERC for review.
- NERC has its list of Critical Assets reviewed by the Regional Entities.

Based on their wider-area view, reviewers may add, but not remove, Critical Assets from lists and will provide justification for the addition of assets. In cases of disputes, there will be an arbitration process adjudicated by the next higher entity type.

The compliance responsibility of the identification and categorization of BES assets and their review and approval ultimately rests with the Responsible Entity owning and operating the assets.

IDENTIFICATION OF CYBER SYSTEMS

Two new terms have been introduced in this approach. The terms Cyber System and Cyber Component are defined in the glossary section of this paper. Cyber System is intended to replace the term Cyber Asset and more accurately represents the intended use of the term. Cyber Components are those discrete elements which make up the Cyber System (e.g. processors, disks, network interfaces, data). In particular, there have been some questions of whether requirements apply individually to the elements or the Cyber System as a whole. The use of these terms will hopefully clarify the intent of the application of these requirements.

Once the list(s) of BES assets have been defined, and all the essential functions performed by the BES Assets have been identified, the Responsible Entity uses this list to define those Cyber Systems which will support:

- The operation and control of these BES assets

  Examples of these are HMI systems in Generating Stations and Transmission Substations, Generating Plant DCS systems, RTUs and PLCs with control and operation functions for BES elements, EMS systems providing control and operate functions for operators *(review examples from CA Guideline)*

- The monitoring and alerting functions for the reliability and operability of these BES assets

  Examples of these are RTUs providing remote metering functions, Dynamic Feeder Rating systems *(review examples from CA Guideline)*

- The data acquisition equipment and systems which support wide-area situation awareness for automated or operator assisted real-time reliable operation of these BES assets

  Examples include Phasor Measurement Units when used in State Estimators for real-time operator assisted actions/alerts. *(review examples from CA Guideline)*

Any BES and non-BES cyber system which directly exchanges data with these cyber systems and elements will be identified for assessment. The judicious design and definition of electronic security perimeters and the application of access controls to these perimeters should be considered by entities to avoid the over-inclusion of cyber systems which do not affect the reliability or operability of the BES. Connectivity considerations will be discussed further in a separate section of this document.

CATEGORIZATION OF CYBER SYSTEMS

The proposed criteria for the classification of these cyber systems are based on the criticality of the function they provide on the BES asset: for each cyber system, an assessment is made on the effect of loss or compromise of the system on the availability, integrity and/or confidentiality of the BES asset it supports. The classification proposed is a 3-tier classification into High, Medium and Low.

(Should we insert here a matrix with A, I, C and H,M,L which would determine how to end up with the categorization of the cyber system based on this assessment? The meaning of what H, M, L in each of the 3 legs of Infosec should also be included. This would be intended to provide some rigor in categorization rather than simply leaving the criteria for the assessment to the entity). Consider the "high-water mark" approach from NIST to determine the impact characteristic of each element. See the FIPS 199 as a reference.

All cyber systems which meet the criteria defined in the Identification of Cyber Systems section above must be within a defined ESP. If there is no communication from inside the ESP to the outside, there is no access point to the ESP.

Cyber systems which perform the functions defined in the Identification of Cyber Systems section above on a set of more than one BES assets will be evaluated based on the impact of the common mode failure or compromise and may be classified a High, Medium or Low impact.

It should be noted that cyber systems which have a common mode impact on a set of BES assets and meet threshold criteria for affecting the reliability and operability of the BES should have been classified as BES assets, and these cyber systems will be assessed based on the common mode impact.

Systems classified as Critical Cyber Assets in versions 1 and 2 of CIP-002 (excepting those non-critical cyber assets that are in the same ESP) would be classified as high impact cyber systems.

Discussion of Cyber System Interconnections Impacts --– Phil

The proposed criterion for the classification of BES Cyber Systems is based on the impact to the function they provide or BES Asset they support: for each Cyber System, an organization determines the impact to the BES of the Cyber System's loss of confidentiality, integrity and availability. Categories of impact are defined as follows:

The potential impact is **High** if the loss of confidentiality, integrity, or availability directly causes or contributes to BES instability, separation, or a cascading sequence of failures, or places the BES at an unacceptable risk of instability, separation, or cascading failures.

The potential impact is **Medium** if the loss of confidentiality, integrity, or availability directly affects the electrical state or the capability of the BES, or the ability to effectively

monitor and control the Bulk-Power System, but is unlikely to lead to BES instability, separation, or cascading failures.

The potential impact is **Low** if the loss of confidentiality, integrity, or availability would not be expected to affect the electrical state or capability of the BES or the ability to effectively monitor and control the BES.

To perform the impact assessment, the organization would assign BES function types and/or BES Assets to each applicable Cyber System. Then for each function type and/or asset, the organization would determine the ~~BES~~ impact on the BES asset/s or function/s based on the loss of confidentiality, integrity, or availability within the Cyber System.

This methodology recognizes that a single Cyber System may support multiple BES function types and/or BES assets as shown in Figure 1. For example, a SCADA system may provide control functionality to a generator with minimal impact on the BES. However, the same SCADA system also provides control for substations on a high impact transmission line. So the organization would assign the final security categorization as *High* for the SCADA system.

This categorization approach makes two important advancements to ensuring a more complete and accurate assessment of Cyber System impact to the BES. First of all, the impact analysis requires a consideration of all BES functions and assets that the Cyber System provides or supports. Secondly, the final categorization ties directly to the security requirements of the Cyber System. As a result, the later security control selection should have its basis in reducing risk to the BES caused by a security breach in Cyber Systems.

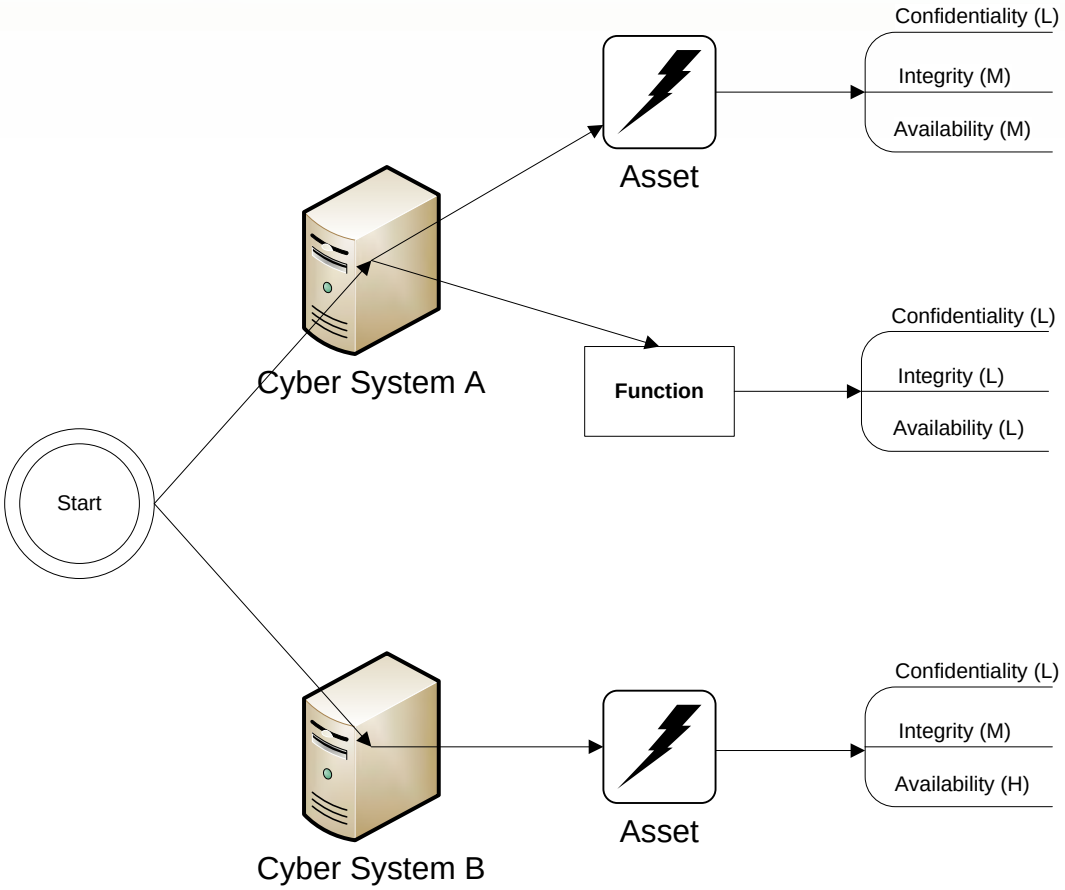


Figure 1: Cyber System Security Impact Analysis

Cyber system interconnections

Many BES Cyber Systems exist within a complex network of interconnected systems and exchange information necessary for the reliable operation of the BES. Just as downstream fault could cause cascading power outages, so a security breach in one Cyber System could utilize a trusted path to affect systems outside of an organization. Consequently, the security assurance of the Cyber System should reflect the level of risk associated with any interconnections.

Since this document only addresses the selection and impact analysis of BES Cyber Systems, the exercise of documenting and protecting interconnections is left as a security control to apply to the target Cyber Systems. However, the identification of essential interconnections into a Cyber System indirectly has a role in identifying BES Cyber Systems. For example, if Utility A classifies one of its Cyber Systems *High* and identifies an essential Cyber System interconnection with Utility B, then Utility B must consider the interconnected system in its BES impact categorization.

The drafting team recognizes the complex nature of interconnected systems and feels the Cyber System connection controls should be non-prescriptive. An organization should define, authorize and monitor connections as part of its secure operation of the Cyber System. An agreement should also be in place between two Responsible Entities to ensure the communication and consideration of Cyber System interconnections.

This approach ensures the standards address the complex nature of Cyber Systems operating the BES and assist organizations operating Cyber Systems downstream to understand the impact these systems have to the BES.

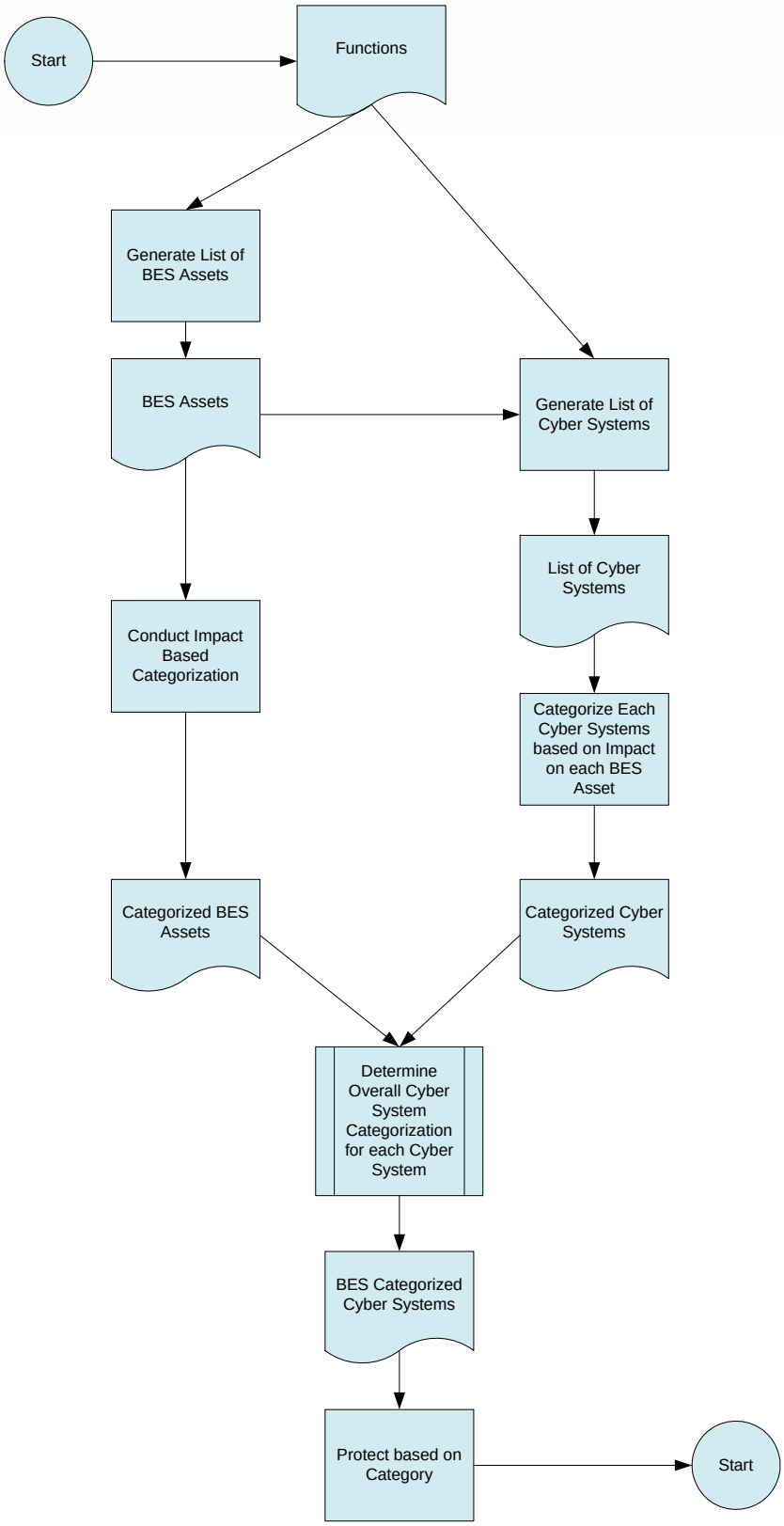
FINAL CATEGORIZATION OF CYBER SYSTEM BASED ON OVERALL IMPACT ON THE BES

The final categorization of each cyber system is determined by the application of a matrix which has predetermined outcomes based on the supported BES asset categorization and the categorization of the cyber system derived from its impact on the BES asset it supports.

This deterministic methodology will provide a more consistent approach than the looser requirement of any risk-based methodology in CIP-002-1 and CIP-002-2. The approach is based on an impact based methodology and will provide for more uniform application of a methodology for categorizing cyber systems.

An example of the application of this approach in an evaluation matrix is shown below:

Asset Impact -->	High	Medium	Low	None
Cyber Impact:				
High	5	4	3	1
Medium	4	3	2	1
Low	3	2	1	0
None	2	1	0	0


Start
Functions
Generate List of BES Assets
BES Assets
Generate List of Cyber Systems
List of Cyber Systems
Conduct Impact Based Categorization
Categorize Each Cyber Systems based on Impact on each BES Asset
Categorized BES Assets
Categorized Cyber Systems
Determine Overall Cyber System Categorization for each Cyber System
BES Categorized Cyber Systems
Protect based on Category
Start

EFFECT OF CYBER SYSTEMS CATEGORIZATION ON REQUIREMENTS

CIP-002 provides for the identification and categorization of BES cyber systems. Once categorized, the definition and applicability of requirements based on the category of the cyber system must be completed throughout the standards. This paper proposes that the current overall control (requirement) grouping in the respective CIP standard be kept wherever possible. The Drafting Team will review, change and augment the requirements in these standards as necessary and appropriate based on an analysis of the catalog of controls in the NIST guidelines when mapped to the CIP requirements. It must be noted that the High, Medium and Low categorization resulting from the proposed CIP approach does not necessarily correspond to the categorization levels defined in the NIST guidelines. This should be resolved during the analysis and mapping of the CIP requirements to the NIST controls by the Drafting Team.

In particular, in the review of these standards, this paper proposes that consideration be made for the different general cyber system types and their capabilities. In particular, the Drafting Team will consider differences in characteristics of cyber systems built on general-purpose platforms from proprietary purpose-built systems. The Drafting Team recognizes that proprietary purpose-built systems may have vulnerabilities similar to general-purpose systems. The Drafting Team will consider the preponderance of purpose-built systems and the implication on exception management, oversight and enforcement.

The Drafting Team will also consider the differences in transmission field and substation, generating plant and control center, equipment types and operating environments, and evaluate an approach to include them without unduly providing exceptions in the standards.

CONCLUSION

The approach proposed in this paper builds on work which the industry has already done in complying with the current standards, the guidance to be available soon in using a risk-based methodology for classifying BES assets, the industry's experience and investments in current compliance programs, and a recognition that the reliability of the BES is based on an engineered system increasingly supported by cyber systems. It is an incremental approach and addresses many areas of the perceived or real deficiencies in the current CIP-002 standard. It certainly ensures that all cyber systems related to the reliable operation of the BES are required to implement a security posture commensurate to the level of criticality of the BES assets they are supporting.

Action Items:

1. John — Will prepare the Introductory paragraph additions
2. Phil — Cyber Security Impact assessment description
3. Jackie — Categorization levels for impacts write-up
4. Scott — List of committees and disciplines for BES analysis support
5. Scott — John Sykes example white paper
6. ALL — send all inputs to John by Friday (4/3/09) for incorporation in to the next version.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Draft Meeting Agenda

Cyber Security Order 706 SDT — Project 2008-06

April 14, 2009 | 1–7 p.m. EST
April 15, 2009 | 8 a.m.–7 p.m. EST
April 16, 2009 | 8 a.m.–noon EST
Duke Office — Conference room number 2313
400 South Tryon St
Charlotte, NC

Dial-in Number: 888-237-9331
Conference Code: 745311
*Note the dial-in information is the same for all three days.

Proposed Meeting Objectives and Outcomes

- Receive updates on TFE and VSL processes
- Receive a briefing on the NERC Critical Assets Industry Survey
- Review and Draft Responses to Phase I Industry Comments
- Review and Refine Phase II Framework White Paper
- Agree on assignments and next steps in the SDT Work plan.

Tuesday, April 14, 2009

9:00 a.m. Phase II White Paper Team Drafting Session

1:00 p.m. Welcome and Opening Remarks — Jeri Domingo-Brewer and Kevin Perry

a. Roll Call
b. NERC Antitrust Compliance Guidelines
c. Review and adoption of March 10-12, 2009 Meeting Summary

1:15 Review of Meeting Objectives, Agenda and Meeting Guidelines — Jeri Domingo and Bob Jones

1:20 Organizational Issues and Review of Phase 1 and early Phase II Schedule — Stuart Langton

- Review of April-December 2009 SDT Schedule

1:40 Update on Technical Feasibility Exception (TFE) NERC Rules of Procedure Posting — Scott Mix

1:50 Update on VSL/VSR for Version 1 and 2 CIP-002-009 — David Taylor

2:00 Overview of SDT Phase II Development Process Steps and CIP 002 Review — Stu Langton

2:10 Critical Assets Industry Survey — Mike Assante

2:40 CIP-002 White Paper Presentation — Bill Winters and Jackie Collett

Q & A and Discussion and Initial Consensus Testing

4:00 Break

4:10 Phase I Small Group Proposal for Response Drafting

4:20 Small Groups Draft Responses to Industry Comments

5:00 Break — If Needed, Small Groups may continue working until 7:00 p.m.

7:00 Recess

Wednesday, April 15, 2009

8:00 Welcome, Agenda Review and Roll Call

8:15 Phase I Small Group — Draft Responses to Industry Comments

10:15 Break

10:30 Phase I Small Group — Draft Responses to Industry Comments

12:30 Working Lunch

1:15 Small Group Reports and SDT Review and Consensus Testing of Draft Responses

3:00 Break

3:15 Small Group Reports and SDT Review and Consensus Testing of Draft Responses

5:00 Break — If Needed, Full or Small Groups may continue working until 7:00 p.m.

7:00 Recess

Thursday, April 16, 2009

8:00 Welcome, Agenda Review, and Roll Call

8:10 CIP-002 White Paper Consensus Testing

10:00 Break

10:15 CIP-002 White Paper Consensus Testing

11:40 Review of May SDT Agenda and Objectives

11:50 Meeting Evaluation — What Worked, What Could be Improved?

12:00 Adjourn

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Cyber Security Order 706 SDT January–December 2009 Draft Project Schedule (Revised April, 2009)

Overview

- **Thirteen SDT Face-to-Face Meetings**
- **Multiple SDT Subgroup and Subcommittees WebEx Meetings**
- **One Cyber Expert/Stakeholder Workshop — Summer or Fall 2009 — Tentative**
- **Industry Comments on CIP-002 SDT White Paper — June–July 2009**
- **Two NERC Members Representative Committee Meetings — May and August, 2009**

Draft Schedule — January–December 2009

1. **January 7–9, 2009 Meeting in Phoenix, AZ (half, full, half day format, Wednesday through Friday)**
   - Review of Technical Feasibility Exceptions white paper
   - Review of Industry Comments on Phase 1 products — Establish and convene small groups to draft responses
   - Review of Phase 2 White papers

   January 15, 2009 WebEx meeting
   - Small group draft responses to industry

   January 21, 2009 WebEx meeting
   - Small group draft responses to industry

2. **February 2–4, 2009 Meeting in Phoenix, AZ (half, full, half day format, Monday through Wednesday)**
   - Update on NERC Technical Feasibility Exceptions process
   - Review of VSL process and SDT role
   - Review of Phase 2 White papers, strawman and principles
   - Review and Adoption of SDT Responses to Industry Comments on Phase I and Phase I Product Revisions.

3. **February 18–19, 2009 Meeting in Fairfax, VA**
   - Update on Phase I process
   - Update on NERC TFE process
   - Update on VSL team process
   - Review, discussion and refinement of Phase II and CIP-002 White papers, strawman, and principles

4. **March 10–11, 2009 Meeting in Orlando, FL (half, full, full day format)**
   - Update on NERC TFE process
   - Update on VSL Team process
   - Review and Refinement of Phase II CIP-002 Strawman Proposals

March 2–April 1 — 30-day Pre Ballot Review
Mid-March — NERC posts TFE draft Rules of Procedure for industry comment
March 30, 2009 — WebEx meeting White Paper Drafting Team
April 1–10, 2009 — NERC Balloting on Phase 1 Product
April 6, 2009 — WebEx meeting — White Paper Drafting Team
April 8, 2009 — WebEx meeting — White Paper Preview — Full SDT Conference Call
April 11, 2009 — Phase I Ballot Results and Industry Comments

5. **April 14–16, 2009 Meeting in Charlotte NC (half, full, half day format, Wednesday through Friday)**
   - Update on NERC TFE process
   - Update on VSL team process
   - Update on the NERC Critical Assets Survey
   - Review in SDT small groups and respond to Phase I Ballot Results and Industry Comments
   - Review and Refinement of Phase II Whitepaper and Progress Report to MRC

May 4, 2009 — Member Representative Committee Meeting in Arlington, VA — SDT progress report.

6. **May 13–14, 2009 Meeting in Boulder City, NV (2-day format, Wednesday through Thursday)**
   - Review MRC presentation and any input to SDT on Phase II white paper
   - Further SDT refinement of the strawman Phase II White Paper in plenary and small groups.

7. **June 17–18, 2009 Meeting in Portland OR (2-day format)**
   - Further SDT refinement and adoption of the Draft Phase II White Paper for industry comment.
   - Review potential SDT subcommittee structure and work plan for implementation of Phase II.

Industry Comment Period on SDT Phase II White Paper — 45 days (June 20–August 5, 2009)

8. **July 13–14, 2009 Meeting in Toronto, ON**
   - Agree on and charge subcommittees and conduct organizational meetings

- SDT Subcommittees meet to organize and begin drafting revisions to CIP and/or addressing assigned issues.
- Subcommittee organizational reports to SDT

July–August 2009 WebEx meeting(s)

- SDT Subcommittee meetings to review applicable industry input on white paper

9. August 20–21, 2009 Meeting in Chicago, IL

- SDT Plenary and Subcommittee meetings to review and respond to industry input on white paper.

August 2009 — **NERC Member Representative Committee**, Presentation of the Phase 2 White Paper and Summary of Industry Comment and Response for MRC input in Winnipeg, Manitoba

10. September 9–10, 2009 Meeting in Denver, CO

- SDT Plenary review industry and MRC input on White paper and consider and agree on refinements
- SDT Subcommittee drafting meetings
- SDT Plenary Session(s)- briefings and subcommittee reports
- Review Work plan through summer 2010, as needed

September 2009 WebEx meeting

- SDT Subcommittee drafting meetings

11. October 20–22, 2009 Meeting in New Orleans, LA

- SDT Subcommittee drafting meetings
- SDT Plenary Session(s)- briefings and subcommittee reports
- Adopt Work plan through Summer, 2010, as needed

October 2009 WebEx meeting

- SDT Subcommittee drafting meetings

12. November 17–18, 2009 Meeting in Atlanta, GA

- SDT Subcommittee drafting meetings
- SDT Plenary Session(s)- briefings and subcommittee reports

November 2009 WebEx meeting

- SDT Subcommittee drafting meetings

13. December 15–17, 2009 Meeting in Tampa, FL

- SDT Plenary Session(s)

- SDT Subcommittee drafting meetings

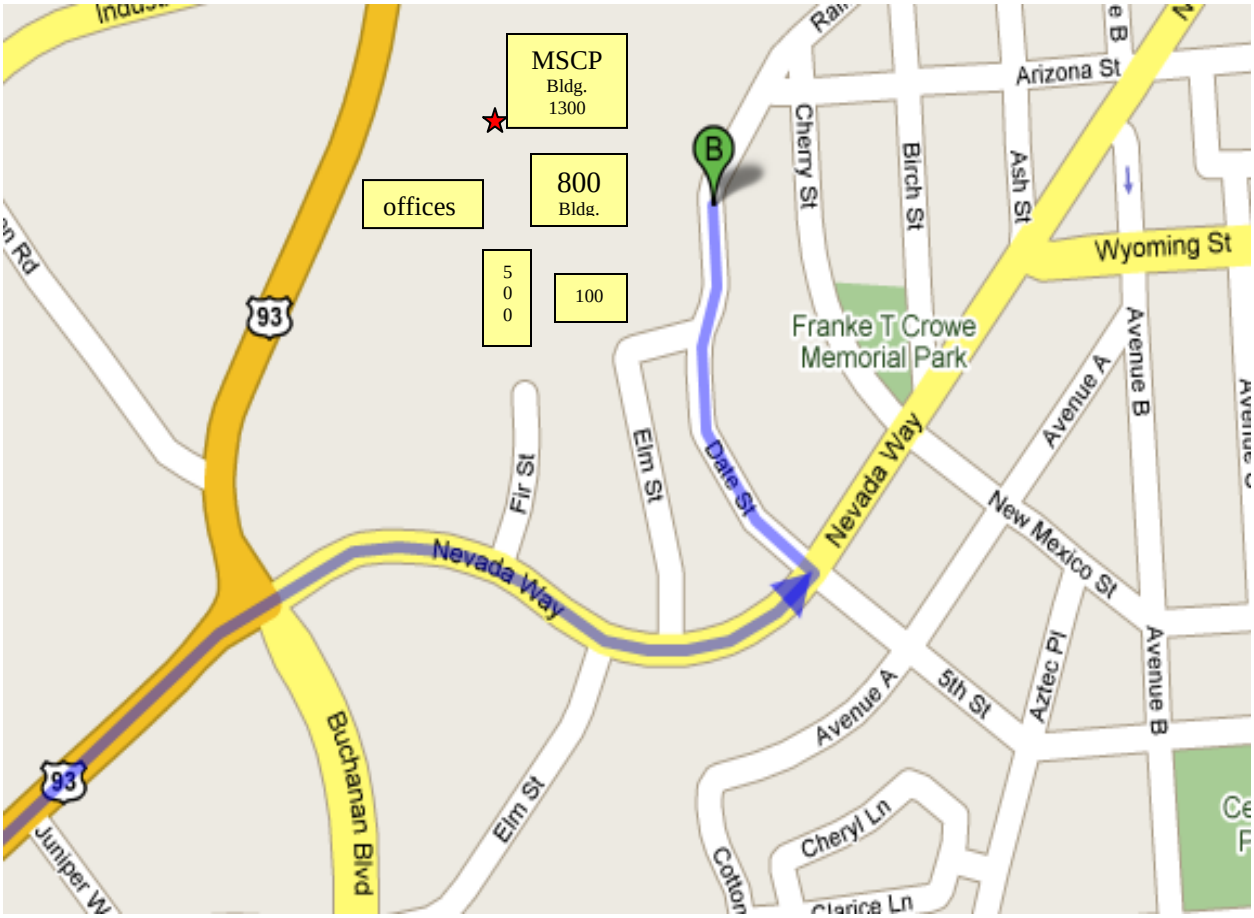
December 2009 WebEx meeting

- SDT Subcommittee meetings

HOTELS IN THE BOULDER CITY/HENDERSON/EAST LAS VEGAS AREA

HOTEL	ADDRESS	PHONE (AREA CODE 702)
Best Western Lighthouse Inn	110 Ville Drive, Boulder City	293-6444
Boulder Dam Hotel	1305 Arizona Street, Boulder City	293-3510
Boulder Manor	4823 Boulder Hwy, Las Vegas	456-2104
Boulder Station	4111 Boulder Hwy, Las Vegas	432-7777
Hacienda Hotel & Casino	US Hwy 93, Boulder City	293-5000
Milo's Inn at Boulder (B&B)	538 Nevada Highway, Boulder City	257-6456
Extended Stay America II	4240 Boulder Hwy, Las Vegas	433-1788
Nevada Inn	1009 Nevada Hwy, Boulder City	293-2044
Railroad Pass	2800 South Boulder Hwy, Boulder City	294-5000
Sam's Town	5111 Boulder Hwy, Las Vegas	456-7777
Sunrise Resort & RV Park	4575 Boulder Hwy, Las Vegas	434-0848
Sunset Station	1301 Sunset Road, Henderson	547-7777
Fiesta (formerly Reserve)	777 West Lake Mead Drive, Henderson	737-0777
Town and Country Manor	4360 Boulder Hwy, Las Vegas	547-9393

Directions to the
Multi-Species Conservation Program
(MSCP BUILDING 1300) 500 Fir Street
Multi-Species Conference Room



Directions: After Railroad Pass Casino, continue on US-93 through the second stoplight (Buchanan Blvd), the road becomes Nevada Highway (Nevada Way). Pass by the restaurant called Casa De Flores on the corner of Fir Street. Do not turn on Fir Street because these gates are usually locked. Stay on Nevada Highway and pass Elm Street then **take a left onto Date Street** and drive past the apartments. The entrance will be on your left. **These gates should be open**. The class will meet in the MSCP Building 1300, Multi-Species Conference Room . If you have any questions feel free to contact the training office at 702-293-8444.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Meeting Summary

Cyber Security Order 706 SDT — Project 2008-06

May 13, 2009 | 8 a.m. – 5 p.m. PST
May 14, 2009 | 8 a.m. – 5 p.m. PST
Boulder City, Nevada

Robert Jones, Hal Beardall and Stuart Langton,
Facilitation and Meeting Design
FCRC Consensus Center, Florida State University

Joe Bucciero, Bucciero Consulting, LLC
http://www.nerc.com/filez/standards/Project_2008-06_Cyber_Security.html

116-390 Village Blvd.
Princeton, NJ 08540
609.452.8060 | www.nerc.com

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Cyber Security Order 706 Standard Drafting Team
Draft 10th Meeting Summary,
May 13-14, 2009
Boulder City, NV

MEETING SUMMARY CONTENTS

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Cyber Security Order 706 Standard Drafting Team
Draft Eighth Meeting Summary,
May 13-14, 2009
Boulder City, NV

EXECUTIVE SUMMARY

The Chair, Jeri Domingo-Brewer, welcomed the members and Joe Bucciero conducted a roll call of members and participants in the room and on the conference call for each day. The Chair reviewed the meeting objectives and Bob Jones, facilitator, reviewed with the Team and participants the proposed meeting agenda.

Mr. Bucciero reviewed with the Team the need to comply with NERCs Antitrust Guidelines including avoiding behaviors or appearance that would be anti-competitive nature and also reminded the group of the sensitive nature of the information under discussion. The Team reviewed and unanimously adopted on the SDT 706 April 14-16, 2009 meeting summary with editorial corrections suggested by the Vice Chair. The Chair and Vice Chair welcomed Jim Breton as a newly appointed member of the SDT representing ISO perspectives. The Chair then congratulated the SDT members on the overwhelming industry approval of the Phase I package of changes to the CIP 002-009 (April 17-27 Recirculation Results: Quorum: 94.37 percent Approval: 88.32 percent). Stuart Langton, SDT facilitator, reviewed the current work plan and meeting schedule Phase 2.

The Chair noted that she was unable to present to the MRC but Jim Brenton noted he was present and that the SDT materials were well received by the MRC.

Scott Mix provided an update briefing to the SDT noting that the posting period closed for the TFE had closed with 52 organizations providing comments over 450 pages. He said that NERC staff is now analyzing the comments. All comments have been posted on NERC web site. Mr. Mix noted there were concerns over the 60-day automatic approval and issues concerning where a TFE can be applied. Members reviewed the history of the TFE process and the SDT's role in their development and clarified the procedural and substantive implications of the TFEs for the CIP 002-009 standards development.

David Taylor, NERC, provided an update on the VSL/VSRs. Since the last meeting they were posted out for industry comment. The comment period is now closed and the 93 pages of comment from 10 entities are being reviewed by the SAR drafting team at their meeting on May 14, 2009.
Version 1 and 2 VSLs must be filed by July 1.

Gerry Freese presented an update from the "Key Messages" discussion at the April SDT meeting in Charlotte. He noted there was perhaps less emphasis than last time given the flood a media attention in April. Members discussed the fact that there were several bills that had been filed in both the Senate and House that focus on different aspects of cyber security policy including the Senators Snow and Rockefeller bill that focuses on Education - R&D, a Senators Bingaman, Lieberman and Thompson bill and a bill Markey is working on in the House.
Michael Assante noted that NERC had been focused on developing key points for Rick Sergel's (President, NERC) testimony in the past weeks. He suggested that there was still value in having good communications and engaging with congressional staff on pending legislation. Gerry agreed to share his draft with the sub team and bring it back on the second day for considerations regarding next steps. On Day Two he agreed to work with the Key Messages Team in refining this and developing a strategy going forward.

Stu Langton reviewed with the SDT the milestones in Phase 1 and Phase 2 of the SDT. The facilitators made a suggestion to consider calling this a "working paper" as the term "white paper" suggested a less dynamic, more static state. The working paper provided a basis for developing the consensus points that were tested and refined in April at the Charlotte meeting.

The Vice Chair proposed the SDT's consideration of a different timeline for CIP 002. The current proposal seeks industry comment on CIP 002 by the end of the year but then develops CIP 003-009 before going out for ballot. Instead consider taking CIP 002 for ballot when ready. In terms of the implementation plan, limit it to those assets considered high and continue to apply the existing CIP 003-009 until they are redrafted. This approach gets improved asset protection out faster. Wouldn't cause anyone to lose under existing standards. The SDT members discussed this option and left it open for further consideration.

The SDT discussed when it would be timely to consider whether to maintain the current CIP structure 002-009 or consider streamlining and addressing overlaps and duplication and possibly creating one set of standards.

The facilitators summarized the discussion of possible directions and next steps**.** First there appeared to be SDT support for getting out the new CIP 002 as early as possible for comment, refinements, and on to ballot. As the SDT develops CIP 002 with measures and requirements, it will need to address how it wants to develop the structure for the present CIP 003-009. The suggestion was made to review all of these issues at the next meeting and to talk about our schedule and strategy.

The Chair thanked John Lim, Phil Huff and their drafting team for working hard since the Charlotte SDT meeting and expressed on behalf of the SDT her gratitude for their leadership and good effort. John Lim, Phil Huff, Jackie Collett and Bill Winters jointly presented the next draft of the Phase 2 Working Paper. They noted the expanded team met twice by phone-WebEx following the Charlotte meeting. They noted they cleaned up the introduction and sought to expand some sections based on the SDT discussion in April. They underscored the fact that there remain significant gaps in the documents, in particular: the critical assets categorization

methodology; and the criteria for categorization of the cyber assets. They have tried to define a couple of additional terms. Overall, the team is not very close to finalizing the document. The members discussed the fact that the evolving document has been made accessible to industry and that it is already being broadly discussed. The SDT needs to be prepared to address inquiries as it continues to refine this document.

The SDT reviewed, discussed and offered suggestions for each section of the working paper including sections addressing: Introduction; the Terms and Definitions; BES Reliability Functions; Identification of BES Subsystems; Categorization of BES Subsystems; Third Party Oversight; Identification of Essential Cyber Systems; Categorization of Cyber Systems; Cyber System Interconnections; Final Categorization of Cyber System Based on Overall Impact on the BES; Risk Based Approach to Security Control Selection; and Effect of Cyber Systems Categorization on Requirements

On Day two the facilitators reviewed the following SDT areas of possible agreement with the Working Paper approach and concepts from the Day One SDT discussion:

- Recognize different audiences: develop Executive Overview (e.g., will have to protect more assets than before; will require identification of more BES assets than did before; will require different levels of protection) that clarifies the intent at a high level regarding methodology;
- Address structured and unstructured threats;
- Develop graphic and tabular depictions of key concepts in white paper;
- Terms and definitions- take a step back and address in content sections;
- Address connectivity as an important concept;
- Seek outside assistance from operating and planning committees for identifying and categorizing BES sub systems and reliability function; and
- Categorize the cyber systems.

The facilitators suggested that the following were outstanding Working Paper issues from the Day One discussion, some of which could be taken up in small group discussions. The SDT reviewed the 3rd Party Review section and ultimately agreed to clarify how much ability each entity has to categorize BES subsystems and what kinds of overview is intended.

The SDT worked in small groups to further explore and refine the issues and options surrounding:

- Identification of Essential Cyber Systems
- Risk Based Approach to Security Control Selection; and
- A third small group participated in a phone conference with FERC staff regarding an issue that was discussed under the Technical Feasibility Exception.

In general, going forward the SDT agreed that the Working Paper focus should be on the overall approach to the CIP-002 issues. The drafting team agreed to continue working on refining the working paper including taking a more conceptual approach while holding the details for

consideration as the SDT begins development of the new CIP 002. Categorization of the BES assets still needs refinement and help from outside experts. Scott Mix and Joe Bucciero will take the lead to see if additional expertise can be provided to the sub team.

Bob Jones, SDT facilitator, noted the proposal to proceed with CIP 002's development in the remaining half of 2009 and refine it after a sequence of comments from the industry before going to the ballot. The Chair reminded people to register for the Portland Bonneville Power meeting and that the July meeting would take place in Vancouver, B.C., Canada.

Hal Beardall reviewed with the SDT the results of the process survey undertaken in March and April. Following the review, Stu Langton led an onsite meeting evaluation discussion and members completed written evaluation forms.

The SDT adjourned at 3:45 p.m. on May 14.

The SDT Order 706 turns a corner in Boulder City

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Cyber Security Order 706 Standard Drafting Team
DRAFT TENTH MEETING SUMMARY,
MAY 13-14, 2009
BOULDER CITY, NEVADA

I. INTRODUCTIONS, AGENDA REVIEW AND REVIEW OF SDT WORKPLAN

The Chair, Jeri Domingo-Brewer, welcomed the members at 8:30 a.m. having been delayed by technical problems with the WebEx and phone. Joe Bucciero conducted a roll call of members and participants in the room and on the conference call for each day (See appendix #2). The Chair reviewed the meeting objectives and Bob Jones, facilitator, reviewed with the Team and participants the proposed meeting agenda (See appendix #1).

Mr. Bucciero reviewed with the Team the need to comply with NERC's Antitrust Guidelines (See, Appendix #3). He urged the Team and other participants in the process to carefully review the guidelines as they would cover all participants and observers. He urged all to avoid behaviors or appearance that would be anti-competitive nature and also reminded the group of the sensitive nature of the information under discussion.

The Team reviewed and unanimously adopted on the SDT 706 April 14-16, 2009 meeting summary with editorial corrections suggested by the Vice Chair. The Chair and Vice Chair then welcomed Jim Brenton as a newly appointed member of the SDT representing ISO perspectives.

The Chair congratulated the SDT members on the overwhelming industry approval of the Phase I package of changes to the CIP 002-009 (April 17-27 Recirculation Results: Quorum: 94.37 percent Approval: 88.32 percent). Stuart Langton, SDT facilitator, reviewed the current work plan and meeting schedule for Phase 2. (See Appendix #4) The Chair noted that the location for the SDT July meeting would be in Vancouver, Canada.

II. UPDATE ON NERC MEMBER REPRESENTATIVE COMMITTEE MAY 5, 2009 PRESENTATION

The Chair noted that she was prepared but unable to present as she was ill. Jim Brenton noted he was present and that the SDT materials were well received by the MRC. At this juncture the MRC did not have feedback for the SDT. SDT Members requested that the written presentation materials including a power point be circulated to them and the Chair agreed to do so.

III. UPDATE ON TECHNICAL FEASIBILITY EXCEPTION (TFE) NERC RULES OF PROCEDURE POSTING

Scott Mix provided an update briefing to the SDT noting that the posting period closed for the TFE had closed with 52 organizations providing comments over 450 pages. He said that NERC staff is now analyzing the comments. All comments have been posted on NERC web site. Mr. Mix agreed to send a link to the members. Some of the common themes in the comments included:

- Concerns over the 60-day automatic approval which no one appeared to like.
- Issues around the requirements where a TFE can be applied.

NERC staff is now reviewing and considering modifications and will try to get this done as quickly as possible. Mike Assante, the NERC CSO is the Corporate Officer in charge of content. Dave Cook, NERC General Counsel is in charge of procedure. Mr.Mix noted that the Edison Electric Institute had submitted both a redline version change to the appendix. The SAR hasn't been submitted as of yet to the standards committee.

Member Discussion Comments on TFE Update

- Version 1 of standards compliance July 1. Version 2 effective date kicks in after FERC approves the standards.
- Canadian entities without regulation (e.g. Manitoba) January 1, 2010 is the effective date for the Version 2 CIP Standards.
- Is there a compliance gap? It is a self report, as before.
- "Version 1 of CIP standards- auditably compliant by July 1, 2009.
- "Reasonable business judgment"- what does it provide entities now?
- Roger Lampila, NERC Compliance, indicated that by taking away reasonable business judgment the auditor will determine if you used reasonable business judgment. Always has the appeal.
- Version 1- "what's the shell game"? TFE draft- could apply to other reliability standards not just CIP? Yet it seems to be all about CIP. Industry will want to see this in the CIP standard.
- If it is in the standard, there needs to be a requirement around a TFE process that compliance could hold you to.
- The TFE has not been approved yet by the NERC BOT nor filed with FERC. This is to get NERC/industry started in the rules of procedure. What do you do now? Self report, the same as before.
- Why are we amending the blanket rules of procedure with language specific to CIP? Why not write this more generically?
- Mike Assante noted that NERC will be responding to the comments.
- No other standard has the triggering language. Don't want a blanket exception in CIP or at large. That is what NERC is trying to prevent. E.g. TFE tree trimming, etc.
- TFE makes more formally recognized process within mitigation plan. Changing the cover page. From a regional entity perspective, today NERC receives, evaluates approves/rejects TFE.

- What should the role be for the regional entity?
- Given TFE says can't ask for TFE unless standard says you can. Do we have to do through a separate SAR or can the group do this under our charter. Limited focus, placement of TFE in the standard?
- SAR should allow the SDT to address TFE where appropriate. David Taylor indicated that he would recommend to the Standards Committee that the SDT have ability to do so in the current SAR. It would take a lot of discussion to determine which requirements this should apply to.
- If the group wanted to do it would be an appropriate thing. Possible consider doing this in a SDT subcommittee - could do this. This will not be a trivial or easy task for the SDT. If it is the right thing to do we should do it even if it will take time to complete.
- Industry is between rock and hard place - if need for TFE and standard doesn't permit.
- TFE has to be approved and in place. Could be part of the SDT's Phase II, (i.e. Version 3) of standards.
- The SDT should come back to this and do some preparation and thinking regarding how to frame and how to organize to get the work done.
- NERC and RE role in evaluation? There are industry comments on that and NERC staff will be responding.
- Mike Assante noted that there has been discussion in the industry on whether there will be modifications where RE's could play a different or bigger role and its budget implications.
- There are some practical issues with the FERC order and the TFE: e.g. the 24 hr removal of access after termination for cause. Proceeded on assumption - remove access. Isn't a TFE designed to take care of this? Puts in non-compliance. 706 said 24 hours was too long. Can't be done practically. Could have addressed some of these issues in version 2 and will need to address this in Version 3. Is there a way we can address, "All assets"?
- Version 1 issue - TFE, document through self report.
- E.g. password - exception against own compliance policy and a TFE against standard. "Where technically feasible" - No process to file at TFE. Have to do self-reported compliance.
- Where requirement allows TFE exception - do I have to file a compliance exception separately. In 007 or e.g. 005 R3.2. Doesn't specify exception. This one tells you what to do in the requirement. Others don't.
- What you have written into a policy.
- You can see the level of TFE contention in the SDT and this is also happening in the industry. Lots of questions around this "can of worms."
- TFE concerns - version 1 and 2 going forward. Time takes to respond when standards have specificity. We could go through with blanket statement - take TFE where applicable. Changes in technology. With reasonable business judgment stripped away. Limit TFEs to a limited number of standards with changing technology will be a losing proposition. Should approach more generally. Shouldn't specify only certain places.
- If you take away physical and network access, you have removed access and fix other policies.

- Compliance auditors only audit to standards and not to policies.
- Version 2 - BOT approved in May, 09. Canadians need to file with regulatory authorities. Effective date - 1st day of 3rd quarter. (i.e. Jan. 1, 2010).
- Communication to industry - let everyone know when things become effective. There is confusion. For any new standards what is the effective date. NERC needs to get info out on TFE's.
- Can't take a TFE until then. Self report of non-compliance with a mitigation plan. E.g. Passwords - 6 characters. CIP 007 R5.3 "as technically feasible". If device supports only 4 characters. Required by standards to do anything? What was the intent? 4 position password. Would have to demonstrate why only using 4- produce industry.
- In the meantime perhaps the SDT can put together an explicit document - here is what you need to do. Focus on what does the industry need to do today. This is what enforceable at what dates.
- Industry and auditors don't know how to handle these.

IV. UPDATE ON VSLS/VSRS -

David Taylor, NERC, provided an update on the VSL/VSRs. Since the last meeting they were posted out for industry comment. The comment period is now closed and the 93 pages of comment from 10 entities are being reviewed by the SAR drafting team at their meeting on May 14, 2009.
Version 1 & 2 VSLs must be filed by July 1. Didn't receive a lot of comments on Version 2. Asked questions about changes in VRS. Didn't receive comments. These will soon get out for ballot/recirculation.

V. UPDATE ON THE "KEY MESSAGES" TASK GROUP

Gerry Freese presented an update from the "Key Messages" discussion at the April SDT meeting in Charlotte. He noted there was perhaps less emphasis than last time given the flood of media attention in April. Members discussed the fact that there were several bills that had been filed in both the Senate and House that focus on different aspects of cyber security policy including the Senators Snow and Rockefeller bill that focuses on Education/R&D, a Senators Bingaman, Lieberman and Thompson bill and a bill Markey is working on in the House. All want cyber security but the question is how to fund this. Concern about the industry being log-rolled with a poorly designed solution. Need to identify who is the driving force and find that out and seek out their staff for the key messages.

Mr. Freese noted that he went on vacation immediately following the Charlotte meeting. He has since put together presentation which he suggested showing to those who agreed to work with him on the "team" which included John Stanford, Jerry Domingo Brewer, Jay Cribb, Dave Norton, Phil Huff, Rich Kinas and Jim Brenton. He asked the Team and Michael Assante if this was still worthwhile going forward with. Michael Assante noted NERC had been focused on key points for Rick Sergel's (President, NERC) testimony in the past weeks. He suggested that there was still value in having good communications and engaging with congressional staff on pending

legislation. Gerry agreed to share his draft with the sub team and bring it back on the second day for considerations regarding next steps. On Day Two Gerry noted he had inadvertently sent the draft out to the SDT plus list. He agreed to work with the Key Messages Team in refining this and developing a strategy going forward.

VI. SDT PHASE II/VERSION 3 DEVELOPMENT PROCESS- THE "WORKING PAPER"

A. Overview of Phase II/Version 3 Work Plan

Stu Langton reviewed with the SDT the milestones in Phase 1 and Phase 2 of the SDT work including the work in Little Rock to begin to frame the challenges, the development of "white papers" following the Washington D.C. meeting in December and further review and refinement of those and other papers and the convergence on an single consensus approach in Orlando that was refined further in Charlotte with John Lim and Phil Huff leading a team to continue to refine the white paper. The facilitators made a suggestion to consider calling this a "working paper" as the term "white paper" suggested a less dynamic, more static state. The paper provided a basis for developing the consensus points that were tested and refined in April and offered to the industry Members Representative Committee.

Member Discussion of Progress To Date

Overall

- Congress - wants to see standards that protect all the control networks.
- What congress will do or not do shouldn't drive the SDT process, rather the SDT should seek to do the "right thing.
- Productivity in working together as a group - confidence in producing a lot and working at a good pace.
- At the end of the day NERC - industry should be in control of the shaping of the CIP standards.

CIP 002 Workplan - Go to Comment and Ballot First with a Complete CIP 002.

- The Vice Chair proposed the SDT's consideration of a different timeline for CIP 002. The current proposal seeks industry comment on 002 by the end of the year but then develops 003-009 before going out for ballot. Instead consider taking CIP 002 for ballot when ready. In terms of the implementation plan, limit it to those assets considered high and continue to apply the existing 3-9 apply until we get they get redone. This gets improved asset protection out faster. Wouldn't cause anyone to lose under existing standards.
- The idea of completing CIP 002 makes sense. Nobody can tell us what CIP 002 should be. Congress could say "secure all." Nobody can do this for us. In following the Smart Grid Task Group - there are many consultants but few industry representatives there.
- CIP 002 is the big ticket item for the industry. The SDT effort to tackle CIP 002 can provide leadership guidance to Smart Grid group. May need to jump in on that? $4.3 billion is

devoted to supporting its development. By getting the scope and methodology in CIP 002 earlier we will help provide leadership for other efforts including NASBEE.

- CIP 002 - angst with Version 1 and 2. Doubts regarding industry's willingness to adopt without 003-009. May need to know about controls and effect on controls.
- CIP 002 - critical asset identification is a challenge but the SDT should make this happen quickly and deliver.
- Got to get past the industry push back. We should be doing the right thing. Won't be an easy process.
- Scott Mix suggested that procedurally it would not be a big issue in going to ballot on CIP 002 first. Would need to make clear on the impacts with other standards. Assuming the first draft is out for comment in December, will probably take multiple times back and forth responding to industry comments before going to the ballot with CIP 002. In the meantime during 2010 the SDT could be working in parallel making headway on CIP 003-009.

Structure of CIP 002-009

- Are we stuck with 002-009 Standards structure? Can we think about 1 set of standards? There are problems with the structure of current standards? Give consideration to putting into one set?
- All NERC standards have a family and sequence number.
- Structure of CIP 002-009. This works together- structure is there is you read the whole thing.
- Renumbering the standards - straighten out. List existing, list by categories. Cross-referencing makes interpretation difficult. Industry willing to spend $ just needs to know what to spend it on.
- There may be more understanding - on structure than is suggested by the discussion. Careful not to throw out the baby with the bathwater.
- Jon Southern noted he was not suggesting that. There are some overlapping and duplicative aspects to the current structure, e.g. audit logging in several sections. 005 and 006 are circular. NIST doesn't have this issue. The movement is to view cyber security assets more holistically as correlating systems.

The facilitators summarized the discussion of two possible directions and next steps**.** First there appeared to be SDT support for getting out the CIP 002 as early as possible for comment, refinements and on to ballot. As the SDT develops CIP 002 with measures and requirements, it will need to address how it wants to develop the structure for the present CIP 003-009. The suggestion was made to review all of these issues at the next meeting and to talk about our schedule and strategy.

B. Phase II Working Paper Presentation and Discussions

The Chair thanked John Lim, Phil and their team for working productively since the Charlotte SDT meeting and expressed on behalf of the SDT her gratitude for their leadership and good effort. John Lim, Phil Huff, Jackie Collett and Bill Winters jointly presented the next draft of the Phase II Working Paper (See Appendix #6) They noted the expanded team met twice by phone-WebEx following the Charlotte meeting. They pointed out that they cleaned up the introduction

and sought to expand some sections based on the SDT discussion in April. They underscored the fact that there remain significant gaps in the documents, in particular, the critical assets categorization methodology and the criteria for categorization of the cyber assets. They have tried to define a couple of additional terms. Overall, they suggested the drafting team was not close to finalizing the document yet and that there were a number of issues the SDT needed to address and resolve. The members discussed the fact that the evolving document is accessible to industry and that it is already being discussed. The SDT needs to be prepared to address inquiries as it continues to refine this document and minimize any confusion that making the evolving draft available might cause.

1. Overall SDT Comments on Working Paper

The Team engaged in an initial discussion of the working paper. A summary of their comments are noted below:

- Industry is interested in what we are doing. Asset identification. Compress the timeline. Sooner the better.
- Consciously stayed away from reviewing the paper until this draft. Through 1st half. Struck by definitions and some more later. Could we create a taxonomy of the terms? E.g. a BES system can be used in different ways. Diagram showing the logical relationship of high order concepts,
- Members should consider this a very early draft that still includes some contradictory statements and inconsistency on terms.
- Scott Mix reported on his discussions with Operating Committee members to help the SDT with the engineering side of the analysis. Big topic last week. Lack of inability to participate in the standards process. Will be well received by the Committee members and hope we will get some who can participate. Won't get names from the Committee until mid June which will be just before Portland. If goal is to have a draft good enough for industry comment. Hold off a month to get the benefit of the Committee members input.

2. Introduction- Section

- The Team cleaned up and accepted changes suggested from the April meeting. Not much new work in the Introduction.

Member Comments and Suggestions

- Reference to the 6 characteristics? Adequacy is the last of the 6? Is that separate and distinct? Problem with implications see it in the table later.
- Reaction of 6 points of the NERC ALR - "reasonably expected " Protect to the normal, vs. protecting for the for unexpected and unplanned in cyber. The focus. Understand focus on ALR - send the wrong message to industry. Emphasize from cyber security.
- Mike Assante noted the same concern - we should think about multiple loss of assets in an abnormal instance.

- Mike Assante's letter of April 6 noted the industry will have to address structured and unstructured threats. The standards will have to be tailored to deal with unstructured. That is how the cyber side works.
- ALR is the granite cornerstone to grow our efforts? If 6 " 2. "Credible contingencies". Leave these as they are? If we play with them everywhere.
- "Everything is credible after it happens" pp 12 5 functions - focus on that - forget about other?
- References to previous presentations to SDT - not helpful in current form, because they need to be understood by the reader who hasn't heard those presentations. Consider our audience.
- Illustration diagram-graphically captures the relationship between the 3.

3. Terms and Definitions Section

John Lim and Phil Huff indicated that the drafting Team was trying to ideally define cyber system vs. asset. Realizing the audience, it will be important to delineate an "essential" cyber system from a cyber system. The Drafting Team decided to look at the essential cyber system first to delineate the target of protection and the essential cyber system and determine what is our target of protection when later developing controls.

Member comments

- Define systems (cyber). What is a BES subsystem? Thought about this in pieces - systems vs. assets on both the power system and cyber side.
- Discussion of cyber systems - pp 8- aggregation and segregation. Embellish all applicable cyber assets that need to be slotted into those systems in a logical and manageable way. Point not well made yet in this paper.
- The drafting team grappled with how much do we want to go into that in the terms and definitions section vs. later in substantive sections. May have gone too far in the terms and definition section in this draft. Address this in a content section.
- We may have gotten too detailed, in trying to get the content down first and then think about whether rearranging. Entity allowed to cherry pick?
- Segregation will take you to controls. We were trying to hit a higher level in first run.
- May have to move some of this further into the paper and consider the effects on requirements.
- Perhaps the new terms and concepts can be defined in this section. There is typically some confusion in a technical paper. Maybe in the introductory section address the high level view-framework of what we are trying to say here. Concept of cyber system introduced, drill down later.
- How does the identification work, when will it become clearer? Is the goal of the paper to let industry know what they need to protect?
- No. This is a rough conceptual draft. This section has continued to get less clear with the introduction of new concepts. There is a need for a new taxonomy. Is there any input on whether we have presented a clear enough concept to get reactions? Tripping over things. How far off base are we with the intent?

- This paper's intent is to give an idea of the methodology we are considering. It will say this at a high level. The takeaway for industry is: 1) You will have to protect more assets than before. 2) You will have to identify more BES assets than did before. 3) There will be different levels of protection but you won't get a list yet as this is not a standard but a concept.
- Overview of the approach is needed - executive summary. Introduction doesn't do it yet. It should include Jackie's points. Jackie agreed to write it up.
- Who is the audience we are addressing in the working paper? Technical people? Higher level Execs? Focused intent of what this is about. Jackie's points are perfect for that audience.
- Tried to focus on full gamut of audiences from executive viewpoints and the technical viewpoints. Should we consider breaking this up into 2 papers one for technical folks, one for executive management?
- Take the highest level approach for discussion of the concept which can set the context for details that follow.
- The diagram shows the departure from critical asset. Cyber isn't limited by electronic security perimeter. Proper network segmentation.
- Protection requirement applies to assets not directly part of the BES. Because of "interconnectedness" and FERC's direction, this may end up in assessment and controls. There may be a minimum set of controls to other systems because of the interconnectedness of cyber systems that are used to control them.
- If generation unit, has no impact on BES is it off the table? It would be brought in if you establish its interconnectedness and vulnerability and implementation of minimum set of controls to mitigate.
- Can be separate electronic security parameters. Maybe we can try to get at that with an additional diagram.
- End point security model is another alternative to the perimeter model. That is where CIP 007 comes in?
- RFI team and WEC - integrated firewalls and routers etc. Some discovery in that discussion?

4. BES Reliability Functions

The Drafting Team shared that the intent was to capture work and discussion on critical asset identification of risk assessment working group translation. They hope to get some help from the operating and planning committees and this is a work in progress not intended as final. They are looking for suggestions.

Member Comments

- Criteria in table - criticality and impact factors concern of their appearance here. Credit to Sam Merrill. He is working on a paper of a services approach to critical infrastructure protection.
- With terminology change - might work. (diagram) Is this what we are trying to get at? Consider this? Phil believes this aligns nicely. Overload the term "systems" It should be clear that BES - cyber can be a sub-system of BES. There is no diagram yet to show it can be both.

- Parallel categorization effort presents a concern: BES on one side, cyber on the other and merge later? BES should feed into cyber categorization. May be problematic to do this independently.
- Drafting Team had the same concerns with cyber impact assessment - on the function not on the BES sub system. You don't know to what degree it has an impact on BES. You need to know to what degree high-medium-low affect the BES.
- Come up with some e.g. a protective relay is a cyber system. Whether it's on a 500 kv line, or 115 kv line in middle of nowhere. Same equipment but the impact on BES is different. Put minimum security on 115 kv.
- I like both the diagram and table. Need to present in different ways for different audiences.
- Two concerns: generation too all encompassing. Avoid "other" catch alls in these standards.
- Contingency reserve = single unit bigger than reserve - not all units together? "Biggest unit"? Combined units.
- Drafting Team's intent to signal that lots of generation not included in current assets. It will be more than your black start units but less than everything. We will need help from the Operating and Planning committees. That is hard work ahead.
- Words - use the same label on both tracks. Use other words (assembly, components, etc.)? NERC glossary is a concern. Some of terms we like to use, such as element, doesn't work.
- Relays as cyber systems and be consistent: is connectivity-risk is missing from the document? Don't see it explicitly here. Vulnerability isn't discussed, but impact is. Look at the section: Risk Based Approach to Security Control Selection)
- We are talking about assets and we don't have enough generation on list? That is not the right question. If there is connectivity then maybe all are there. Don't like the approach - if it doesn't provide security - won't be doing the job.
- The paper is trying to relate assets to functions (services approach) which weren't done before.
- We have fuzzy boundaries, generation, transmission, distribution. Turf state and federal. Cyber security view - if you can get into and move up line on a common controls network this is a problem. Smart grid lumped together Transmission and Distribution.
- Capture even with distribution level system that "connect" to transmission and impact reliability of BES.
- The SDT needs to get more involved with the smart grid security task group.

5. Identification of BES Subsystems

The Working Paper characterizes cyber system as a BES asset.

Member Comments

- Is the diagram in original paper clearer? See the outline of the white circle.
- Labels systems - suggestion to make clearer that h/m/l in each transmission, generation

6. Categorization of BES Subsystems

The Working Paper makes no changes in this section since April. The drafting team will get this fleshed out when help comes for the identification BES assets from the Operations and Planning committees.

7. **Third Party Oversight**

While there were no major changes but a rewrite of the format with some help from Sam Merrill and a clarification of the process for disputes and appeals.

Member Comments

- Focuses approval - oversight on BES engineering side not the cyber side. No oversight provisions on the cyber side.
- What about the Reliability Coordinator role?
- Does this relate to oversight of entities to make up their own rules? Better approach -- the development of regional interconnect wide categorization criteria for BES subsystems. Simplify the process. Map your assets to regional criteria and functions. The categorization is a mapping exercise vs. an oversight exercise.
- Can the paper explore this as an option? Put both options on table making the case for each? Or present to SDT for decision. Does this section currently assume entities will make up own rules?
- Why not be told what the assets are vs. providing the criteria?
- Industry has been involved with this e.g. 100kv. If you go to region to make decision, the entities will be making the criteria. Might be looser criteria if done at the regional level.
- Looking for uniformity around this asset categorization. E.g. Reliance on redundancy, etc.
- Regional criteria for bulk power hasn't worked in other instances.
- This is an idea worth exploring. Weakness in federal model lack of uniformity across federal agencies. This could help industry address CIP 002 process and send a message to congress that the industry is looking at holistic solutions.
- Whoever has responsibility - they should pay the fine if this is not done right. Need to think this through. Don't want to touch this with a 10 ft pool. Policy is no thank you. We determine our critical assets. Lean much towards compliance.
- Categorization is dynamic process. Add and retiring transmission. Continual nightmare keeping a list up-to-date and current.
- Move towards criteria by which multiple entities come to the same conclusion. Three entities with the same equipment should come up with the same solution.
- Why not have the SDT come up with criteria?
- Problem with creating a fill in the blank standard. Dead end. Can we require each region to come up with own independent standard? Have to be able to justify. What would it be?
- Single NERC standard with West, East, ERCOT, nailed at an interconnection level. E.g. criticality of a control center would be same across the three.
- Challenge is you can't audit "reasonability"-- this would bring the entities to the same place. The pass through of the region is to check if something was missed.

- Can we define a criteria that sets minimum expectations. If there are regional differences, there can be a process that will define and justify any differences. Gets away from "reasonableness", but allows for differences between the regions and their infrastructure to be taken into account.
- A regionally specific standard - can be more stringent than a continent wide standard.
- SDT should come up with a base set of minimum criteria.
- Why have a different set of rules for a region to identify BES subsystems?
- We are trying to run through two sets of filters - will we get the same answer? Focus on categorizing cyber assets side first BES. See if we can categorize those. We have similar e.g. control centers, etc.

8. Identification of Essential Cyber Systems

The Drafting Team noted that the change in the introduction of BES subsystems is consistent with the new definitions. This is the introduction of essential cyber systems.

Member Comments

- Focus is BES and generation - on back end, are the other systems managing those part of this? Coal, gas etc.?
- Fuel inventory managing piles, timelines no. Control over pulverizer-conveyor belt. Possibly?
  Does this capture those things?
- Go back to 215 a (1) - doesn't include distribution facilities.
- Essential at this point. Doesn't preclude other systems coming in within the scope of protection.
- "Critical systems"- systems at the control center level are complex. ISO's challenge-zonal vs. nodal markets, market system may be essential to reliability. We have found in working with operations staff that key functions are not always obvious.
- Need to look at this section more closely for its implications.
- Is the market system itself a critical asset? May depend and vary. How you schedule a function may be in or out. Moving towards more integrated systems and this will present a challenge.
- Should we have a list that limits what systems?
- Identifying different levels of protection required. Are we focused too much on BES assets.
- Mindful of as developing the standards, if it is in the standards and there is not fuzziness, then everything is included. Other systems that impact reliability?

9. Categorization of Cyber Systems

The Drafting Team noted that this section was clarified, not substantively added to.

Member Comments

- BES functionality concern - problem regarding lack of clarity is a critical assets. Does it require a wholesale move away?
- With CIP 002 we have learned that one size doesn't fit all. The challenge is in applying good security practices to interrelated assets. This is the cyber security realm.
- The concept proposes a melding of two approaches to meet the security outcomes sought.
- The concept is looking to understand the impacts to the BES functions. Not tying it to BES reliability. That is done however, implicitly, through the matrix.
- Still perform both assessments. BES subsystem assessment feed into.

10. Cyber System Interconnections

Member Comments

- Requirement of standard should be that two parties negotiate an agreement to protect the security device.
- This is in part addressed by the oversight section.
- If utility A has interconnection, then they will address in a service agreement with Utility B.

11. Final Categorization of Cyber System Based on Overall Impact on the BES

Member Comments

- Merging of the categorizations of BES and Cyber to be used for applying of controls appropriate to the level
- Review and clarify the Table- low = no impact and none = consistency. Are low to none the same?
- Start/End.
- BES assets would replace BES sub systems.

12. Risk Based Approach to Security Control Selection

The drafting team asked if they have adequately addressed risk after categorization?

Member Comments

- Provide a framework (similar to NIST) to use to provide your security controls.
- Address what doing with controls - commensurate with the cyber system they will be protecting.
- Overall objective mitigating the risk- high impact system- take what you are trying to protect and reduce the risk commensurate to its impact on the BES.
- Addresses the earlier comment about connectivity.
- Concept of controls - incorporate risk assessment into that construct. Not assuming everyone does their own risk assessment. Perhaps not as extensive as NIST.

- A device that doesn't have impacts but could have. As you change the connectivity. Pick a different control now that you have modified the environment.
- This adds another layer of complications in implementation (3 impact ratings; 5 more)
- 1 size fits all doesn't work. Flexibility should make sense from several perspectives.
- Cyber - less important. Applicable to all BES systems?
- Intent is to significantly address cyber issue.
- Physical security - applicability broad enough to reach beyond cyber. Cyber is a part.
- 1st half of 002 is not a cyber - BES impact method will be
- Security issues - overlaps - categorization exercise sets up for CIP 10 -18 family, physical protection of equipment. Electro mechanical vs. digital.
- Upgrading equipment - don't have to go through the process.
- Unclear section of white paper. Trying to address risk in the writing of the controls addressing different operating environments. Addressing risk in the entity level - applying a vulnerability analysis.
- If we don't know how we are going to do this.
- Trying to write a requirement for this will be very hard.
- Remember Mike Assante's advice to the Team in December: look at what you want to accomplish and then think out of the box on how to get there.
- Focusing on what is our method of identify protections. After feedback, we will move forward flushing out another white paper focusing on the controls and protection.
- Concerned about expectations regarding risk assessments and small entities

13. Effect of Cyber Systems Categorization on Requirements

The Drafting Team did the best we could laying out levels we know today.

Member Comments

- Focus on the importance of connectivity.
- We need to evaluate - the appropriate format, vs. assuming we will keep the same format. This may be an issue to take up further into to the development of the CIP 002 Standard.

C. Phase 2/Version 3 Working Paper Discussion - Day Two

1. Day One Summary

On Day two the facilitators reviewed the following SDT areas of possible agreement with Working Paper approach and concepts from the day one SDT discussion:

- Recognize different audiences: develop Executive Overview (e.g. will have to protect more assets than before; will require identification of more BES assets than did before; will require different levels of protection) that clarify the intent at a high level regarding methodology;

- Address structured and unstructured threats;
- Develop graphic and tabular depictions of key concepts in white paper;
- Terms and definitions - take a step back and address in content sections;
- Address connectivity as an important concept;
- Seek outside assistance from operating and planning committees for identifying and categorizing BES sub systems and reliability function; and
- Categorize the cyber systems.

The facilitators noted there were several outstanding issues raised by the Working Paper issues and the day-one discussion which could be taken up in small group discussions.

2. 3rd Party Review and Risk Based Approach

The facilitators first reviewed the day one discussion on the section, "3rd Party Review of BES Subsystem Categorization Options"and the related point of consensus from the April 2009 SDT meeting upon which the drafting team had drafted this section which stated: "The Standards will require oversight of the categorized list of BES assets by entity types which have a more complete wide-area view of the BES." The facilitators then reviewed several possible oversight options from the day one discussion including:

- White Paper option - hierarchal structure (entities, reliability coordinator, regional entity and ERO) area wide perspective, entities categorize BES subsystems with oversight by RC, RE and ERO and with burden on reviewer to justify adding to the entities list of categorized BES subsystems and an appeals process.
- Regional Entities develop criteria for categorization of BES subsystems through regional standards development process and ERO review and approval.
- BES System Categorization criteria will be established at the Interconnect wide level and SDT drafts the criteria and augment with subject matter expertise with oversight through the normal audit process.
- BES System Categorization minimum criteria established at the continental level and SDT drafts the criteria and augment with subject matter expertise with oversight through the normal audit process with an option for interconnections to argue for variation or additional more stringent criteria.

The SDT discussed the working paper section on Risk Based Approach to Security Control Selection. Members suggested the needs for some level of flexibility given that this is an exercise in reducing the risk.

SDT Comments on the Risk Based Approach

- Give entity some level of flexibility other than just the TFE – propose a move to a performance based security assessment – write controls to address risk to the asset – valuable based assessment

- Rewriting the requirements and decoupling them from the controls – different types of controls to address requirements – look at environment and have options to address
- Changing the requirements to better point to the controls – with different ways to mitigate the risk
- How do we do what we feel needs to be done within the bounds of the NERC requirements – what a properly written requirement or standard is still a question – these standards are different but can not throw out the auditing system – still have to play within those confines
- Categorizing according to risk impact
- Vulnerability is easier to figure out than threat
- Remember that audits will be to the requirement
- Control based audits work in certain contexts to work out conflicts – that is not how NERC audits – need to write requirements to meet NERC audits
- Gaining consensus on a control based audit system – need to get NERC staff (legal, standards development and audit) on board
- Need to write what the objective is into the working paper to open dialogue with NERC staff
- This aligns with the industry – performance based auditing – sets basis for standards to evolve over time, for lessons to fold back into the standards – this is a culture shift
- Don't agree that the audit system can give much back – because of the way the penalties are assessed

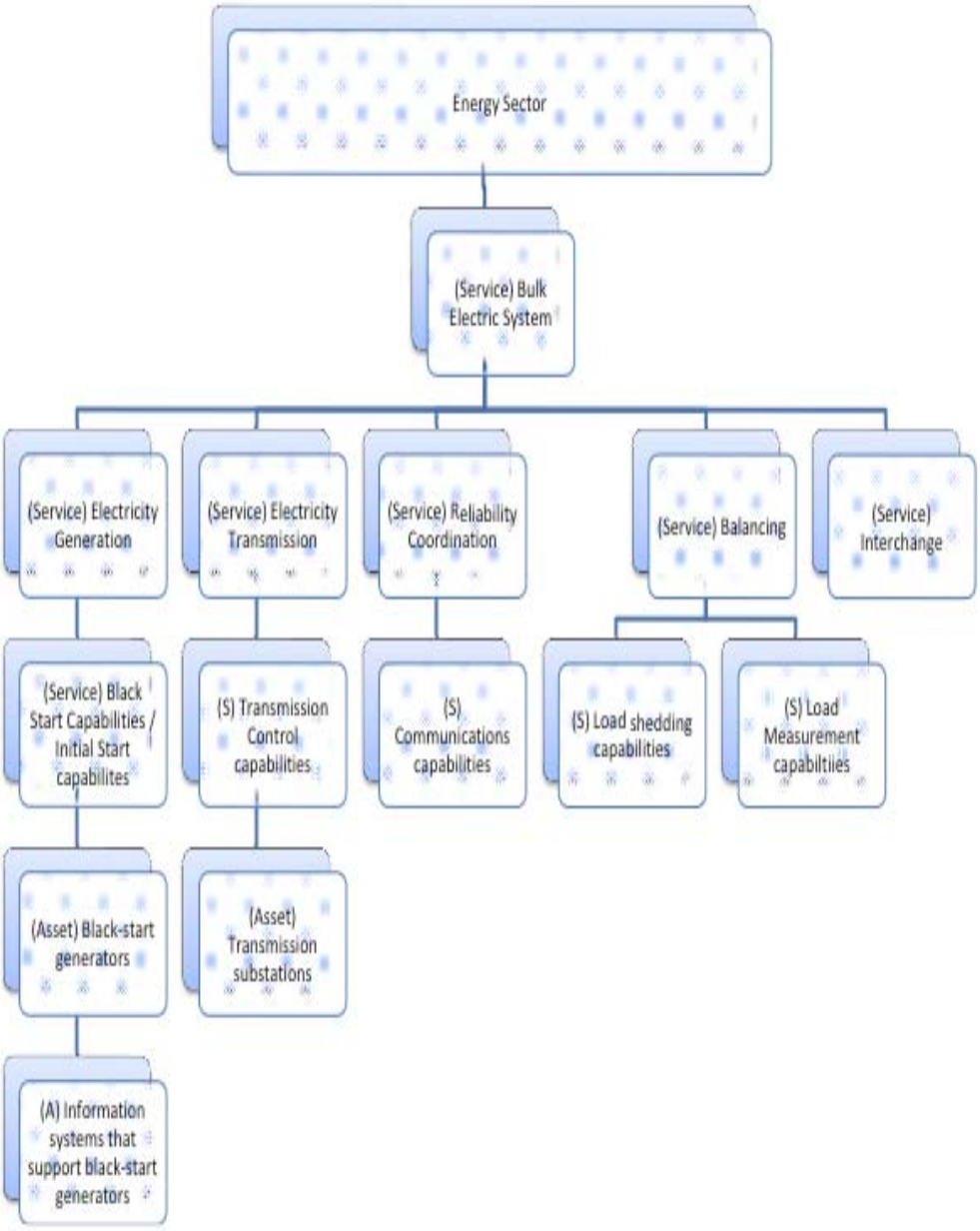
3. Identification of Essential Systems and Categorization of BES Subsystems.

After some clarifying discussion regarding the intent of the white paper, the drafting team agreed to refine the existing section and clarify to what degree the entity should have the discretion to categorize any of the BES subsystems. Of the areas of concern the facilitators identified from day one's discussion, the SDT agreed to work in two small groups to further explore and refine the issues and options.

a. Identification of Essential Systems

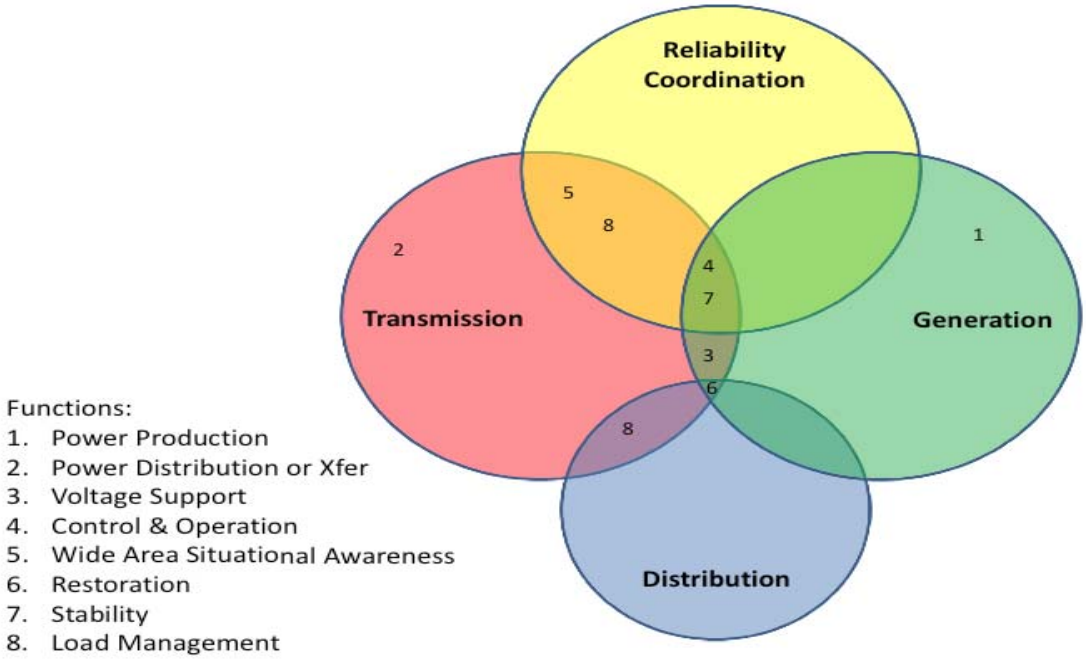
Frank Kim provided a summary of the small group take away points including:

- Reduce ambiguity about what is and is not within the scope;
- Clarify what is meant or included in "other" – list what was meant as examples for the industry; and
- Whether or not integrity of data as to communications is a requirement – integrity of function of the links between systems.


Energy Sector
(Service) Bulk Electric System
(Service) Electricity Generation
(Service) Electricity Transmission
(Service) Reliability Coordination
(Service) Balancing
(Service) Interchange
(Service) Black Start Capabilities / Initial Start capabilites
(S) Transmission Control capabilities
(S) Communications capabilities
(S) Load shedding capabilities
(S) Load Measurement capabiltiies
(Asset) Black-start generators
(Asset) Transmission substations
(A) Information systems that support black-start generators

b. Categorization of BES subsystems

Jackie Collett presented the small group's report using the chart below. She noted they have attempted to graphically relate the eight functions (set out in the working paper) to some of the services – roles. They may try to put in some specific examples for clarity for the industry. Once they flesh this out we can ask committees for their thoughts and reactions**.** They deliberately tried not to use some of the common NERC terms and they are getting away from who owns it. This will be is an iterative process, a series of steps. The current CIP standards are system – based but you may not be protecting what you really need to protect for purposes of reliability – this is a more holistic approach to what you need to protect. While you may have to protect a thing, it is a collection of things that must operate together**.** Assessments help compartmentalize what you need to look at – those who claim to not have anything may actually have assets that need to be protected. We will be trying to identify the set of controls needed to protect an asset. In the end the objective will be to come up with categorized list – categorized by level of risk. How can we quantify the impact without knowing its impact on the BES? Most entities currently do not know the impact. We need to set criteria to establish the impact**.** What is missing now is protecting cyber system and functions – current CIPs do not get us there. The process we come up will need to be agreed to and understood by the industry. We want to apply a consistent level of control – not everything should be protected at high – if filtered through the right criteria – that is the key. We must make sure everyone has a minimum level of protection**.** Smaller entities need to be made aware of their impact on the larger system. We will have to resolve the issue of market sensitive data.



Functions:
1. Power Production
2. Power Distribution or Xfer
3. Voltage Support
4. Control & Operation
5. Wide Area Situational Awareness
6. Restoration
7. Stability
8. Load Management

SDT Comments on the Report

- Still concerned about process of applying everything and categorizing BES stuff – subject to penalties, but have we protected anything?
- Role intended to replays subsystem? No, it is something different
- What is generation? Staying away from it because it means different things to different people
- Question regarding the second column
- Did not consider the question the criteria but rather the level of criticality to the system
- Intent of paper to address the system in terms of functions to get to integrity of the data – address in cyber system interconnections
- Some in industry may be looking for a list – call out some items
- For BES we may offer some examples, not a list – do not want to end up with a check list – reluctant to do so this early – illustrative examples only
- Trying to identify where a system or function fits – examples may help clarify
- EMS is critical because of what it can affect – not critical itself
- Also question of ownership

4. FERC Conference Call and the TFE

Another small group (including Team Members Jeri Domingo Brewer, Kevin Perry, John Lim and Gerry Freese and David Norton and NERC staff) participated in a phone conference with FERC staff regarding the pending interpretation requests for the CIP standards requirements including the including the six wall boundary issues. The SDT members brought up the issue of the currently proposed TFE process limiting TFE requests to only those requirements where technical feasibility was specifically referenced in the standard requirement. FERC staff indicated it was never their intent to limit TFE requests in that fashion and that FERC staff would get with NERC to discuss this further. FERC noted its intent was only to sever the relationship between TFE requests and Reasonable Business Judgment and that they actually intended to broaden the applicability of the TFE request, not narrow it. FERC, NERC and the SDT small group will participate in a follow up call on June 2.

D. SDT CIP Version 3/Phase 2 Process Going Forward

1. Focusing on CIP 002 and Deferring Decisions on CIP 003-009?

The SDT discussed how or whether we need to stay within the current framework of CIP 2-9. Some believe the SDT needs to nail down the broad scope of 002 before having that discussion. The working paper is trying to capture conceptually our expected approach – may need to rephrase how we will go about modeling the existing 002-009. Perhaps the SDT can discuss the expectations about this at an upcoming meeting.

2. Seeking Expert Assistance

The Planning and Operating Committees cannot nominate anyone until June, 2009. The SDT discussed whether it might solicit the informal input of a few individuals respected in the industry. This would not be a substitute for the ongoing participation and contributions of those participating at the meetings and on the WebEx, nor the outreach to the Operating and Planning Committees, nor the briefing of the NERC Members Representative Committee. Several names were mentioned in the SDT conversation and staff agreed to coordinate with member in making the contacts and requests.

3. Concept/Working Paper Readiness for Industry Review, Level of Detail and Audience

The concept for the working paper is to put forward an approach to 002 initially and later fleshing out the detail after getting industry reactions. Many expressed concerns with the level of detail for this working paper and suggested it be more conceptual at this point.

- Use the executive summary to explain the concept without the detail in the rest of the document – the high level overview you want others to review – will not overwhelm others with the detail
- Higher level paper to send out – can not have high level in one section and more detail in others – more detail we put out the more reaction – comments we will get back
- BES continue to put out the system approach to explain change from current system
- Would have to pull back some of the details in the paper today – some of the details go to how to redraft the standards – people already talking about the paper and members are getting questions on details.
- There may need to split into two documents with a summary for the larger body and the detailed version for our use. However care should be taken in splitting the paper into two – the SDT needs input from key individuals with the qualifications necessary to look at both sides

4. Expectations for Adoption of 002

- Multiple rounds of drafts will be needed before we gain consensus with industry – should be parallel to development of standards and controls – if consensus on 002 occurs first then move to ballot but if takes longer than securities control then we may wait and issue together.
- Some prefer putting it out as a whole – less need to put out first if FERC will address TFE interpretation with NERC
- I also agree with waiting till everything is ready – but the SDT and NERC must keep industry updated with drafts – not comfortable voting without the whole package.
- This can remain an open question as needed.

VI. NEXT STEPS

A. 2009 SDT Workplan Approach

Bob Jones, SDT facilitator, noted the proposal to proceed with CIP 002's development in the remaining half of 2009 and refine it after a sequence of comments from the industry before going to the ballot.

B. Workplan Schedule

The Chair reminded people to register for the Portland Bonneville Power meeting and that the July meeting would take place in Vancouver, B.C., Canada.

C. CIP 002 Working Paper Development

The drafting team agreed to continue working on refining the working paper including taking a more conceptual approach while holding the details for consideration as the SDT begins development of the CIP 002. Categorization of the BES assets still needs refinement and help from outside experts. Scott Mix will take the lead to see if additional expertise can be provided to the sub team.

D. Process Evaluation - What has Worked, What could be Improved?

Hal Beardall reviewed with the SDT the results of the process survey undertaken in March and April. (See Appendix #7). Following the review, Stu Langton led a onsite meeting evaluation discussion and members completed written evaluation forms (See, Appendix #3)

The meeting concluded by the SDT members thanking the Chair for her hosting and for the very productive meeting and informative field trip.

The SDT adjourned at 3:45 p.m. on May 14.

Appendix # 1
Cyber Security Order 706 SDT — Project 2008-06
Draft Meeting Agenda
May 13, 2009 | 8:00 a.m. to 3:00 p.m. EDT
May 14, 2009 | 8:00 a.m. to 5:00 p.m. EDT
Bureau of Reclamation
Boulder City, NV

Proposed Meeting Objectives/Outcomes

- Receive update Phase I Recirculation Ballot results
- Review MRC presentation and input
- Receive update on TFE and VSL processes;
- Receive update on the SDT "Key Messages Task Group"
- Review, refine and adopt the Phase II White Paper as a conceptual framework going forward;
- Agree on next steps in the Work plan and assignments.

Draft Agenda

Wednesday	**May 13, 2009**
8:00 a.m.	Welcome and Opening Remarks- *Jeri Domingo-Brewer/Kevin Perry* a. Roll Call b. NERC Antitrust Compliance Guidelines c. Facilitator review of April meeting summary and adoption d. Update on SDT Team Membership
8:20 a.m.	Review of Meeting Objectives, Agenda and Meeting Guidelines- *Jeri Domingo Brewer and Bob Jones*
8:25 a.m.	Update on the Phase 1 Recirculation Ballot Results-*Jeri Domingo Brewer*
8:30 a.m.	Update on NERC Member Representative Committee May 5, 2009 Presentation
8:40 a.m.	Update on Technical Feasibility Exception (TFE) NERC Rules of Procedure Posting- *Scott Mix*
8:45 a.m.	Update on VSLs/VSRs - *David Taylor*
8:50 a.m.	Update on the "Key Messages" Task Group - *Gerry Freese*
9:20 a.m.	Overview of FERC Order and Steps to Date in the SDT Phase II Development Process- *Stu Langton*
9:30 a.m.	Phase II Concept Paper Presentation and Discussion- John Lim, Phil Huff, et al
10:30 a.m.	Break
10:30 a.m.	Phase II Concept Paper Presentation, Discussion and Refinements- John Lim, Phil Huff, et al
12:00 p.m.	Working Lunch (Return to plenary meeting at 12:45)

12:45 p.m. Phase II Concept Paper Discussion
2:50 p.m. Drafting Assignments for Thursday

3:00 p.m. Recess (Field Trip to Hoover Dam)

Thursday **May 14, 2009** (As revised May 14, 8:00 a.m.)
8:00 a.m. Welcome and Agenda Review and Review of Portland Logistics
8:05 a.m. "Key Issues" Communications Task Group Discussion and Next Steps - Gerry Freese
8:20 a.m. Phase II Concept Paper Discussion
Review of SDT Areas of Agreement with White Paper Approach and Concepts-Day One

- Recognize different audiences: develop Executive Overview (e.g. will have to protect more assets than before; will require identification of more BES assets than did before; will require different levels of protection) that clarify the intent at a high level regarding methodology.
- Address structured and unstructured threats
- Develop graphic and tabular depictions of key concepts in white paper.
- Terms and definitions - take a step back and address in content sections
- Address connectivity as an important concept
- Seek outside assistance from operating and planning committees for identifying and categorizing BES sub systems and reliability functions
- Categorization of Cyber systems

Outstanding White Paper Issues
3rd Party Review of BES Subsystem Categorization Options (pros-cons and ranking)
Identification of Essential Cyber Systems
Risk Based Approach to Security Control Selection
Final categorization of cyber systems based on overall impact on the BES
8:45 a.m. 3rd Party Review of BES Subsystem Categorization Options (pros/cons and ranking)

10:30 a.m. Break

10:45 a.m. Phase II Concept Paper- Small Group Discussion

- Identification of Essential Cyber Systems
- Risk Based Approach to Security Control Selection
- Final categorization of cyber systems based on overall impact on the BES

12:15 p.m. Working Lunch

12:45 p.m. Phase II Small Group Reports
2:00 p.m. Clarification of Next Steps on White Paper Development
White Paper Development and Release - input on BES from Operating and Planning Committees.

2:15 p.m. Break

2:30 p.m. Work plan and Schedule Issues
- TFE and the SDT - weighing the value and costs of the SDT addressing TFE in 2009
- CIP 002 - Review and Test Consensus on Developing CIP 002 for Industry Comment and Ballot

3:25 p.m. Review of SDT Member Process Evaluation and Steps Forward

4:00 p.m. Other Issues

4:30 p.m. Assignments, Next Steps and Review of Work-plan and June meeting objectives

4:45 p.m. Meeting Evaluation – What was accomplished? What helped? What can be improved?

5:00 p.m. Adjourn

Appendix # 2
Cyber Security for Order 706 Standard Drafting Team and Attendees List
May 13-14, 2009 Project 2008-06 — CS 706 SDT

Orlando, Florida

Attending in Person – SDT Members

1. Rob Antonishen	Ontario Power Generation (Tuesday and Wednesday)
2. Jim Breton	ERCOT
3. Jeri Domingo-Brewer, Chair	**U.S. Bureau of Reclamation**
4. Jackie Collett	Manitoba Hydro
5. Scott Fixmer	Senior Security Analyst Exelon Corporate Security, Exelon Corp.
6. Gerald S. Freese	Director, Enterprise Information Security America Electric Power
7. Phillip Huff	Arkansas Electric Coop Corporation
8. John Lim	CISSP, Department Manager, Consolidated Edison Co.NY
9. Frank Kim	Ontario Hydro
10. David Norton	Policy Consultant, CIPEnergy Coporation *(Tues & Wed.)*
11. **Kevin B. Perry, Vice Ch.**	Director, IT-Infrastructure, Southwest Power Pool
12. David S. Revill	Georgia Transmission Corporation
13. Scott Rosenberger	Luminant Energy
14. Kevin Sherlin	Sacramento Municipal Utility District
15. Jonathan Stanford	Bonneville Power Administration
16.Keith Stouffer	National Institute of Standards & Technology
17. John D. Varnell	Technology Director, Tenaska Power Services Co.
18.William Winters	Arizona Public Service, Inc.
1. Roger Lampilla	NERC
2. Mike Assante	NERC (Wednesday)
3. David Taylor	NERC (Wednesday)
4. Scott R. Mix	NERC
5. Tom Hoffstetter	NERC (Formerly Midwest ISO, Inc)
6. Joe Bucciero	NERC/Bucciero Assoc.
7. Robert Jones	FSU/FCRC Consensus Center (Wed. & Thursday)
8. Stuart Langton	FSU/FCRC Consensus Center
9.Hal Beardall	FSU/FCRC Consensus Center

SDT Members Attending via WebEx-Phone

19.Joe Doetzl	Manager, Information Security, Kansas City Power & Light Co.
20. Richard Kinas	Orlando Utilities Commission (Wednesday)
21. Christopher A. Peters	ICF International

SDT Members Unable to Attend

1. Jay S. Cribb	Information Security Analyst, Southern Company Services, Inc.
2. Sharon Edwards	Duke Energy

Others Attending in Person

Bob Tallman	E.ON

Others Attending via WebEx-Phone

Chris Wright	

Sam Morrell	CERT
James Bassett	Lafayette
Jason Marshall	Midwest ISO
Chris Wright	Burns & Mac

Appendix # 3 Meeting Evaluation Feedback

CYBER SECURITY ORDER 706 SDT
MAY 13-14, 2009, BOULDER CITY, NV
MEETING EVALUATION FEEDBACK

Members used the following 0 to 10 scale in evaluating the meeting: 0 means totally disagree and 10 means totally agree. The ranks reflect the average for each category statement.

1. Please assess the overall meeting.

8.29 The agenda packet was very useful.
8.71 The pre-meeting papers (White Paper and Process Evaluation Summary) were very useful.
6.17 The WebEx document display and the audio were effective
7.06 The quality of the meeting facility was good.
8.88 The objectives for the meeting were stated at the outset.
8.00 Overall, the objectives of the meeting were fully achieved.
Were each of the following meeting objectives fully achieved:
9.13 Receive update Phase I Recirculation Ballot results
8.06 Review MRC presentation and input
8.31 Receive update on TFE and VSL processes;
7.19 Receive update on the SDT "Key Messages Task Group"
8.12 Review, refine and adopt the Phase II White Paper as a conceptual framework going forward.
8.31 Agree on next steps in the Work plan and assignments.

2. Please tell us how well you believe the Team members and participants engaged in the meeting.

8.33 The Chair and Vice Chair provided leadership and direction to Team and Facilitators
8.76 The Facilitators made sure the concerns of all members were heard.
8.29 The Facilitators helped clarify and summarize issues.
8.29 The Facilitators helped members build consensus.
8.29 The Facilitators made sure the concerns of all participants were heard.
8.41 The Facilitators helped us arrange our time well.

3. What is your level of satisfaction with what was achieved at the meeting?

8.59 Overall, I am very satisfied with the results of the meeting.
8.65 Overall, the design of the meeting agenda was effective.
8.44 I was very satisfied with the services provided by the Facilitators.
8.50 I am satisfied with the outcome of the meeting.
8.60 I know what the next steps following this meeting will be.
8.00 I know who is responsible for the next steps.

4. Other comments:

What did we achieve?

- Some progress on concept paper

- Consensus on WP
- Improving consensus
- We are getting consensus on the direction the group wants to go
- We obtained a significant amount of consensus on our next steps forward. We needed a lot of direction in the working paper and I think this was achieved.
- We have a course of action that should when complete provide a substantive improvement to electric sector security.
- Major progress on the working paper
- Jon did a good job of summarizing the key points of consensus
- Need for the Key Messages" task group seems to have dissipated.

What are our biggest challenges going forward?

- Keeping to agreed consensus items
- Not getting sidetracked. Keep us on goal!
- After we figure it out…selling it to the industry who did not go through the process.
- Getting industry to agree to this direction
- A lot of work left to do. We need to stay on task
- Industry consensus
- Consensus, industries education
- Time

What suggestions do you have for making our group more productive?

- Better internet access
- Provide copies of all documents prior to meeting
- Small groups remain productive

Appendix # 4
NERC Antitrust Compliance Guidelines

I. General

It is NERC's policy and practice to obey the antitrust laws and to avoid all conduct that unreasonably restrains competition. This policy requires the avoidance of any conduct that violates, or that might appear to violate, the antitrust laws. Among other things, the antitrust laws forbid any agreement between or among competitors regarding prices, availability of service, product design, terms of sale, division of markets, allocation of customers or any other activity that unreasonably restrains competition.

It is the responsibility of every NERC participant and employee who may in any way affect NERC's compliance with the antitrust laws to carry out this commitment.

Antitrust laws are complex and subject to court interpretation that can vary over time and from one court to another. The purpose of these guidelines is to alert NERC participants and employees to potential antitrust problems and to set forth policies to be followed with respect to activities that may involve antitrust considerations. In some instances, the NERC policy contained in these guidelines is stricter than the applicable antitrust laws. Any NERC participant or employee who is uncertain about the legal ramifications of a particular course of conduct or who has doubts or concerns about whether NERC's antitrust compliance policy is implicated in any situation should consult NERC's General Counsel immediately.

II. Prohibited Activities

Participants in NERC activities (including those of its committees and subgroups) should refrain from the following when acting in their capacity as participants in NERC activities (e.g., at NERC meetings, conference calls and in informal discussions):

- Discussions involving pricing information, especially margin (profit) and internal cost information and participants expectations as to their future prices or internal costs.
- Discussions of a participant's marketing strategies.
- Discussions regarding how customers and geographical areas are to be divided among competitors.
- Discussions concerning the exclusion of competitors from markets.
- Discussions concerning boycotting or group refusals to deal with competitors, vendors or suppliers.

III. Activities That Are Permitted

From time to time decisions or actions of NERC (including those of its committees and

subgroups) may have a negative impact on particular entities and thus in that sense adversely impact competition. Decisions and actions by NERC (including its committees and subgroups) should only be undertaken for the purpose of promoting and maintaining the reliability and adequacy of the bulk power system. If you do not have a legitimate purpose consistent with this objective for discussing a matter, please refrain from discussing the matter during NERC meetings and in other NERC-related communications.

You should also ensure that NERC procedures, including those set forth in NERC's Certificate of Incorporation and Bylaws are followed in conducting NERC business. Other NERC procedures that may be applicable to a particular NERC activity include the following:

- Reliability Standards Process Manual
- Organization and Procedures Manual for the NERC Standing Committees
- System Operator Certification Program

In addition, all discussions in NERC meetings and other NERC-related communications should be within the scope of the mandate for or assignment to the particular NERC committee or subgroup, as well as within the scope of the published agenda for the meeting.

No decisions should be made nor any actions taken in NERC activities for the purpose of giving an industry participant or group of participants a competitive advantage over other participants. In particular, decisions with respect to setting, revising, or assessing compliance with NERC reliability standards should not be influenced by anti-competitive motivations.

Subject to the foregoing restrictions, participants in NERC activities may discuss:

- Reliability matters relating to the bulk power system, including operation and planning matters such as establishing or revising reliability standards, special operating procedures, operating transfer capabilities, and plans for new facilities.
- Matters relating to the impact of reliability standards for the bulk power system on electricity markets and the impact of electricity market operations on the reliability of the bulk power system.
- Proposed filings or other communications with state or federal regulatory authorities or other governmental entities.
- Matters relating to the internal governance, management and operation of NERC, such as nominations for vacant committee positions, budgeting and assessments, and employment matters; and procedural matters such as planning and scheduling meetings.

Any other matters that do not clearly fall within these guidelines should be reviewed with NERC's General Counsel before being discussed.

Appendix # 5
CYBER SECURITY ORDER 706 SDT JANUARY- DECEMBER DRAFT PROJECT SCHEDULE (REVISED MAY, 2009)

OVERVIEW

- **13 SDT FACE-TO-FACE MEETINGS**
- **MULTIPLE SDT SUBGROUP AND SUBCOMMITEES WEBEX MEETINGS**
- **2 NERC MEMBERS REPRESENTATIVE COMMITTEE MEETINGS,** (MAY & AUGUST, 2009)

CYBER SECURITY ORDER 706 SDT DRAFT SCHEDULE
JANUARY-DECEMBER, 2009

DEVELOPMENT OF CIP FRAMEWORK JAN-JUNE, 2009

1. January 7-9 SDT Meeting, Phoenix, AZ ½ / 1/½ day format. Wed-Friday

- Review of Technical Feasibility Exceptions white paper
- Review of Industry Comments on Phase 1 products - Establish and convene small groups to draft responses
- Review of Phase 2 White papers
  January 15 WebEx meeting(s)
- Small group draft responses to industry.
  January 21 WebEx meeting(s)
- Small group draft responses to industry.

2. February 2-4 SDT Meeting, 2009, Phoenix, AZ, ½ / 1/½ day format. Mon -Wed.

- Update on NERC Technical Feasibility Exceptions process
- Review of VSL process and SDT role
- Review of Phase 2 White papers, straw man and principles
- Review and Adoption of SDT Responses to Industry Comments on Phase I and Phase I Product Revisions.

3. February 18-19, SDT Meeting, Fairfax, VA

- Update on Phase I process
- Update on NERC TFE process
- Update on VSL Team process
- Review, discussion and refinement of Phase II/CIP 002 White papers, straw man and principles

4. March 10-11, SDT Meeting 2009, Orlando, FL, ½ /1/1 day format

- Update on NERC TFE process
- Update on VSL Team process
- Review and Refinement of Phase II CIP 002 Straw man Proposals

March 2 - April 1 30-day Pre Ballot
Mid-March - NERC posts TFE draft Rules of Procedure for industry comment
March 30, WebEx meeting(s) White Paper Drafting Team
April 1-10, NERC Balloting on Phase 1 Products
April 6, WebEx meeting- White Paper Drafting Team
April 8, WebEx meeting(s) - White Paper Preview- Full SDT Conference Call
April 11, 2009 Phase I Ballot Results (Quorum: 91.90% Approval: 84.06%) and Industry Comments-

5. April 14-16, SDT Meeting, Charlotte NC, ½ / 1/½ day format. Wed-Friday

- Update on NERC TFE process
- Update on VSL Team process
- Update on the NERC Critical Assets Survey
- Agree and Adopt Responses for Phase I Industry Comments- Recirculation Ballot
- Review and Refinement of Phase II Whitepaper and Progress Report to MRC

April 28 and May 6 White Paper Drafting Team Meetings - WebEx.

April 17-27 Recirculation Results: Quorum: 94.37% Approval: 88.32%

May 5, 2009, NERC Member Representative Committee Meeting, Arlington, VA- SDT progress report.

6. May 13-14, Wed.-Thursday, SDT Meeting, Boulder City NV, 2-day format

- Review MRC presentation and any input to SDT on Phase II approach
- Further SDT refinement of the Phase II White Paper.

CIP 002 DEVELOPMENT OF REQUIREMENTS, MEASURES, ETC. JUNE-DEC 2009
7. June 17-18, SDT Meeting, Portland OR, 2-day format

- Further SDT refinement and adoption of the Draft Phase II White Paper.
- Review implementation plan for June-December CIP 002- potential SDT subcommittee structure and deliverables.
- Agree on and charge subcommittees and conduct subcommittee organizational meetings

8. July 13-14, 2009 SDT Meeting, Vancouver, B.C., Canada

- SDT Subcommittees meet to organize and begin drafting revisions to CIP 002 and/or addressing assigned issues.
- SDT Plenary and Subcommittee meetings to review and respond to any industry input/comments on white paper.
- Subcommittee organizational reports to SDT
  July-August, WebEx meeting(s)
- SDT Subcommittee meetings as needed

9. August 20-21, 2009, Chicago IL

- SDT Plenary and Subcommittee meetings to develop and test support for CIP 002 products

August, 2009, **NERC Member Representative Committee**, Progress Report presentation on CIP 002 for MRC input, Winnipeg, Manitoba

10. September 9-10, 2009 Folsom, CA

- SDT Plenary review industry and MRC input on CIP 002 approach and consider and agree on refinements
- SDT Subcommittee drafting meetings- requirements etc.
- SDT Plenary Session(s)- briefings and subcommittee reports
- Review Work plan through Summer, 2010, as needed

September, WebEx meeting

- SDT Subcommittee drafting meetings

11. October 20-22, New Orleans LA

- SDT Subcommittee drafting meetings
- SDT Plenary Session(s) - briefings and subcommittee reports on CIP 002 Requirements, etc.
- Adopt Work-plan through Summer, 2010, as needed

October, WebEx meeting

- SDT Subcommittee drafting meetings

12. November 17-18, Atlanta GA

- SDT Subcommittee drafting meetings
- SDT Plenary Session(s) - briefings and subcommittee reports on CIP 002 requirements, etc.

November, WebEx meeting

- SDT Subcommittee drafting meetings

13. December 15-17, Tampa

- SDT Plenary Session(s) to review, refine and agree on Draft CIP 002 Initial post for industry review and comments
- SDT Subcommittee drafting meetings

December, WebEx meeting

- SDT Subcommittee meetings

SDT 706- 2010

- CIP 002- SDT Respond to Industry Comments, Refine CIP 002
- Initiate CIP 003-009 Development of Requirements, Measures, and Controls etc.
- Develop a full set of CIP 002-009 Standards for Industry Comment

- Refine and Submit for Industry Ballot
- NERC Board of Trustees Adopts
- FERC Approves and NERC Implements

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Appendix # 6 Phase II Working Paper

Download the paper at http://www.nerc.com/filez/standards/Project_2008-06_Cyber_Security.html

Categorizing Cyber Systems

An Approach Based on BES Reliability Functions

NERC Cyber Security Standards Drafting Team for Order 706
05/09/2009

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Appendix # 7 SDT Process Survey and Recommendations

TO: **SDT 706 Team Members**

FROM: **Jeri Domingo Brewer, Chair and Kevin Perry, Vice Chair, SDT 706.**

RE: **SDT 706 DRAFT PROCESS SUGGESTIONS GOING FORWARD**

DATE: **May 11, 2009**

Thanks again to the members who provided their thoughts and reflections on the online SDT process survey that our facilitators produced. Your responses underscore the Team's commitment to practical improvements that help us to seek to continue to improve our productivity as a team. Attached to this memo is an executive summary and the complete results *(without attribution but with respondents listed)* of the survey for your information.

Below are our thoughts and reflections based on your responses. We have organized these in 7 areas with suggestions on how we might respond to the survey results and institute practical improvements. We plan to discuss these suggestions at our upcoming meeting with an eye towards implementing those the Team believes will be helpful going forward.

1. **SEEK GREATER EFFICIENCY IN OPEN SDT DISCUSSIONS**
   - SDT members should continue to share the airtime and keep their points brief and well focused.
   - SDT facilitators should clarify the objectives of sessions at the outset and manage discussions to achieve those objectives. Use of the "parking lot" tool should be used to keep the SDT on track and bring back off-topic points.

2. **USE OF WEBEX AND PHONE-AUDIO FOR SDT MEETINGS**
   - In planning for meetings, take into account the quality of the facilities' telephone, audio web connections. This is important for the Team members and for others following the SDT process.
   - Facilitators should use WebEx to engage members who are participating by phone and ensure that meeting participants voices are clearly captured

3. **USE OF SDT SUB-GROUPS TO DRAFT PHASE I STANDARDS (OCTOBER-NOVEMBER, JANUARY-FEBRUARY)**
   - Subgroups have and will continue to be critical to making progress with the SDT given its size and the complexity of the charge.
   - Greater care should be taken in charging the subgroups with clear objectives and consistent formats and consistent definitions of terms to guide their efforts.

- Provide sufficient time for reporting back and agreement for suggestions for further refinements and consensus building.
- Continue to use small groups for drafting responses to industry comments.
- When possible, develop a draft straw man of responses that are consistent and can be refined through the SDT small and full group review and discussion.

4. USE OF STRAWMAN DRAFTS

- Straw man drafts have been effective ways to engage the SDT but multiple, competing straw man documents require more time and effort.

5. USE OF A 4-POINT ACCEPTABILITY SCALE TO PROVIDE A GAUGE OF SDT SUPPORT FOR PROPOSALS

- Facilitators should make sure the SDT is clear on draft conceptual proposals prior to using the ranking tool to test acceptability. It should be used for flushing out divergent perspectives and seeking to find common ground.

6. DISTRIBUTION OF TIMED AGENDAS AND MEETING OBJECTIVES IN ADVANCE OF SDT MEETINGS AND DETAILED MEETING SUMMARIES INCLUDING EXECUTIVE SUMMARIES AND APPENDICES.

- Continue to produce and circulate agendas with objectives
- Facilitators should be clear and explicit with the SDT when the discussion is off the agenda. When the time allotted for the discussion needs adjustment the facilitators should clarify the tradeoffs and make a proposal to chair and team.
- Make summaries available on website and let the members know and give them the precise link where they can draw it down.

7. USE OF ONSITE MEETING EVALUATION

- Use a combination of a group onsite evaluation and an individual evaluation form. Capture and summarize in the meeting summary.
- Facilitators should encourage members to provide informal side-bar feedback on process concerns that can be shared with the Chair-Vice Chair for consideration.

Cyber Security Order 706 Standard Drafting Team
On-Line Process Evaluation Survey Results (19 of 23 members)

EXECUTIVE SUMMARY
(May 12, 2009)

HOW SATISFIED ARE YOU WITH THE PROGRESS THE SDT HAS MADE AND OUTCOMES IT HAS ACHIEVED SINCE OCTOBER, 2008?

Ranking Scale	*Very Satisfied-4*	*Generally Satisfied-3*	*Somewhat Satisfied-2*	*Dissatisfied-1*	*Avg.*
Totals for	**5**	**8**	**5**	**1**	**2.9**
Totals for	**1**	**1**	**0**	**0**	**3.5**

STRENGTHS
- Productive group in spite of size
- The breadth of knowledge and experience of team members
- The independent facilitation team allows Team to focus on content
- Phase I was very successful

CHALLENGES
- Managing time effectively
- Managing external issues and pressures - Smart Grid, legislative proposals,
- Managing the impact on the SDT deliberation of high profile issue with lots of media attention.
- Phase II is getting off to a rocky start.
- Balance between discussion and decisions.
- This was a 'fast' process overall. I'd like to be further along with the Phase II ideas
- The development of these standards is complex, and our progress is non-linear.
- It is likely that we won't be able to take a direct path to the result, and will need to wander around. This, at times, may frustrate some team members more than others (and frustrate us all sometimes!).
- The process seems to work, but the progress seems difficult. I expect that once the framework is fully developed, progress will speed up.
- Fear of introducing real security to the electric sector. Given the current environment we need to shift our focus to providing justification and building confidence in the plan we have.

SDT PROCESS ITEMS
(Note: Summary comments are offered for those areas receiving less than 3.0 average)

1. USE OF WEBEX AND PHONE-AUDIO FOR SDT MEETINGS

Ranking Scale	Very Satisfied-4	Generally Satisfied-3	Somewhat Satisfied-2	Dissatisfied-1	Avg.
Totals for	**0**	**10**	**8**	**1**	**2.5**
Totals for	**1**	**1**	**0**	**0**	**3.5**

Summary of Points

- Effectiveness directly proportional to quality of teleconferencing facilities at the face-to-face site. Quality of audio and WebEx has been inconsistent.
- This working is essential to the whole premise of remote participation.
- Participating via phone is very tough to follow. It is usually hard to hear everyone plus when numerous conversations are going on at once you get lost in the noise.
- This has been a combination of process and logistical slip-ups.
- Audio quality seems to be a continuing issue.

2. USE OF WEBEX FOR SUB-TEAM MEETINGS

Ranking Scale	Very Satisfied-4	Generally Satisfied-3	Somewhat Satisfied-2	Dissatisfied-1	Avg.
Totals for	8	7	2	1	3.2
Totals for	1	1	0	0	3.5

3. USE OF SDT SUB-GROUPS TO DRAFT PHASE I STANDARDS (OCTOBER-NOVEMBER)

Ranking Scale	Very Satisfied-4	Generally Satisfied-3	Somewhat Satisfied-2	Dissatisfied-1	Avg.
Totals for	**9**	**8**	**1**	**1**	**3.3**
Totals for	**1**	**1**	**0**	**0**	**3.5**

4. USE OF SMALL GROUPS TO DRAFT RESPONSES TO PHASE I (JANUARY-FEBRUARY)

Ranking Scale	Very Satisfied-4	Generally Satisfied-3	Somewhat Satisfied-2	Dissatisfied-1	Avg.
Totals for	**8**	**10**	**1**	**0**	**3.4**
Totals for	**0**	**2**	**0**	**0**	**3.0**

5. USE OF STRAWMAN DRAFTS

Ranking Scale	Very Satisfied-4	Generally Satisfied-3	Somewhat Satisfied-2	Dissatisfied-1	Avg.
Totals for	**8**	**7**	**3**	**1**	**3.2**
Totals for	**1**	**1**	**0**	**0**	**3.5**

6. USE OF A 4-POINT ACCEPTABILITY SCALE TO PROVIDE A GAUGE OF SDT SUPPORT FOR PROPOSALS

Ranking Scale	Very Satisfied-4	Generally Satisfied-3	Somewhat Satisfied-2	Dissatisfied-1	Avg.
Totals for	**3**	**10**	**4**	**1**	**2.8**
Totals for	**1**	**1**	**0**	**0**	**3.5**

Summary of Points

- Very helpful - to hear alternate points of view and especially the expectation that dissenters need to provide alternative language and not just vote "no".
- Good mechanism for gauging general group preferences, divergent perspectives and agreements on conceptual approach. Less effective at actually garnering support for a particular approach. Can lead to too much focus on words while missing the idea.
- Need more succinct issues to vote on, or more discussion time up front to more fully flesh out broad ideas.

7. Adoption and use of a 75 percent consensus decision rule with a 2/3's quorum

Ranking Scale	*Very Satisfied-4*	*Generally Satisfied-3*	*Somewhat Satisfied-2*	*Dissatisfied-1*	*Avg.*
Totals for	**8**	**10**	**0**	**0**	**3.4**
Totals for	**1**	**1**	**0**	**0**	**3.5**

8. Distribution of timed agendas and meeting objectives in advance of SDT meetings

Ranking Scale	*Very Satisfied-4*	*Generally Satisfied-3*	*Somewhat Satisfied-2*	*Dissatisfied-1*	*Avg.*
Totals for	**9**	**7**	**1**	**0**	**3.5**
Totals for	**1**	**1**	**0**	**0**	**3.5**

9. Detailed meeting summaries including executive summaries and appendices

Ranking Scale	*Very Satisfied-4*	*Generally Satisfied-3*	*Somewhat Satisfied-2*	*Dissatisfied-1*	*Avg.*
Totals for	**9**	**8**	**1**	**0**	**3.4**
Totals for	**2**	**0**	**0**	**0**	**4.0**

10. Use of onsite meeting evaluation

Ranking Scale	*Very Satisfied-4*	*Generally Satisfied-3*	*Somewhat Satisfied-2*	*Dissatisfied-1*	*Avg.*
Totals for	**3**	**10**	**5**	**0**	**2.9**
Totals for	**2**	**0**	**0**	**0**	**4.0**

Summary of Points

- Some people are in a hurry to leave and may not give the evaluation a lot of thought.
- Comments helpful while they are fresh.
- The process is getting pretty well honed at this point.
- You may get more candid and pragmatic response with a one-on-one sidebar discussion with those that are visibly frustrated during a meeting.
- Evaluations provide an opportunity to address what isn't working

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Draft Meeting Agenda

Cyber Security Order 706 SDT — Project 2008-06

May 13, 2009 | 8 a.m.–3 p.m. EST
May 14, 2009 | 8 a.m.–5 p.m. EST
Bureau of Reclamation
Boulder City, NV

Proposed Meeting Objectives and Outcomes

- Receive update Phase I Recirculation Ballot results
- Review NERC Members Representative Committee presentation and input
- Receive update on TFE and VSL processes
- Receive update on the SDT "Key Messages Task Group"
- Review, refine, and adopt the Phase II White Paper as a conceptual framework going forward
- Agree on next steps in the Work plan and assignments

Wednesday, May 13, 2009 | 8 a.m.–3 p.m. PST (with working lunch from noon to 12:45 p.m.)

- Welcome and Opening Remarks — Roll Call; NERC Antitrust Compliance Guidelines; Facilitator review of April meeting summary and adoption; Update on SDT Membership
- Updates on — Phase 1 Recirculation Ballot Results; NERC Member Representative Committee May 5, 2009 Presentation; Technical Feasibility Exception (TFE) NERC Rules of Procedure Posting; VSLs and VSRs; and "Key Messages" Task Group
- Overview of FERC Order and dteps to date in the SDT Phase II Development Process
- Phase II Concept Paper Presentation Discussion — John Lim, Phil Huff, et al

Thursday, May 14, 2009 | 8 a.m.–5 p.m. PST (with working lunch from noon to 12:45 p.m.)

- Welcome and Agenda Review
- Phase II Concept Paper Refinements and Discussion — John Lim, Phil Huff, et al
- Phase II Concept Paper Framework Adoption and Discussion of Implementation Steps
- Review of SDT Member Process Evaluation and Steps Forward
- Assignments, Next Steps, Review of Work plan, and June meeting objectives
- Meeting Evaluation — What was accomplished? What helped? What can be improved going forward?
- FERC Approves and NERC Implements

116-390 Village Blvd.
Princeton, NJ 08540
609.452.8060 | www.nerc.com

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Meeting Summary

Cyber Security Order 706 SDT — Project 2008-06

Bonneville Power Administration
Portland, Oregon

June 17, 2009 | 8 a.m. – 5 p.m. PST
June 18, 2009 | 8 a.m. – 5 p.m. PST

Robert Jones and Stuart Langton,
Facilitation and Meeting Design
FCRC Consensus Center, Florida State University

Joe Bucciero, Bucciero Consulting, LLC
http://www.nerc.com/filez/standards/Project_2008-06_Cyber_Security.html

116-390 Village Blvd.
Princeton, NJ 08540
609.452.8060 | www.nerc.com

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Cyber Security Order 706 Standard Drafting Team
Draft Eleventh Meeting Summary,
June 17-18, 2009
Portland, OR

MEETING SUMMARY CONTENTS

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Cyber Security Order 706 Standard Drafting Team
Draft Eleventh Meeting Summary,
June 17-18, 2009
Portland, OR

EXECUTIVE SUMMARY

The Chair, Jeri Domingo-Brewer and Vice Chair Kevin Perry welcomed the members at 8:00 a.m. Joe Bucciero conducted a roll call of members and participants in the room and on the conference call for each day. The Chair reviewed the meeting objectives and Bob Jones, facilitator, reviewed with the Team and participants the proposed meeting agenda *(See appendix #1*).

Mr. Bucciero reviewed with the Team the need to comply with NERC's Antitrust Guidelines. He urged the Team and other participants in the process to carefully review the guidelines as they would cover all participants and observers.

Scott Mix provided an update briefing to the SDT noting that the posting period closed for the TFE had closed with 52 organizations providing comments over 450 pages. He reviewed his presentation made a week earlier at the NERC CIPC meeting and noted that NERC staff is now analyzing the comments. NERC staff, including SAIS and outside counsel, is reviewing comments, making responses, and preparing modifications. The NERC BOT will need to approve the resulting TFE document. There is not a requirement for another round of public comments and responses, like the ANSI standards process. The revised TFE will be sent to the Management Representative Committee (MRC) of NERC before being presented to the NERC BOT for adoption. The TFE document will be filed with FERC and will follow the same process for approval as the CIP standards.

Scott also referenced the FERC Order 706 B, which clarified that facilities within each nuclear generation plant in the United States that are not regulated by the NRC are subject to compliance with the eight mandatory Critical Infrastructure Protection (CIP) Reliability Standards, noting that NERC has reconstituted the version 1 SDT and recently convened a town hall meeting that produced a good dialogue and excellent questions.

Scott Mix, on behalf of David Taylor, NERC, also provided an update on the VSL/VRFs. They were posted in May, 2009 for industry comment, and the comment period is now closed. The 93 pages of comments from 10 entities are being reviewed by the respective NERC drafting team. Version 1 & Version 2 VSL/VRFs must be filed by July 1, 2009.

Stu Langton reviewed with the SDT the milestones in Phase 1 and Phase 2 of the SDT work. The working paper has provided a basis for developing the consensus points the SDT agreed to at its Charlotte meeting in April. Joe Bucciero, with the SDT facilitation team, reported that following the Boulder City meeting the Drafting Team has been supplemented with BES expertise from Jim Case,

Jamey Sample, Jack Bernhardsen, Jason Marshall, and Sam Merrill. Others have also been invited to participate, but have not yet done so.

John Lim and Jackie Collett jointly presented the next draft of the Phase 2 Working Paper and invited the SDT to pose clarifying questions, note concerns, and offer options for addressing the concerns. Mr. Lim noted the working paper suggests that this "proposed cyber system categorization" approach includes the consideration of NERC's mission, the essential functions necessary in achieving this mission, an impact-based methodology to categorize the BES subsystems and the associated cyber systems, and finally the deterministic derivation of an overall impact-based categorization of the cyber systems, with the anticipated application of cyber security requirements commensurate with that categorization. This parallels general approaches to risk management practices, which focus first on identifying key processes necessary for meeting high-level objectives, then drilling down into supporting processes.

Jackie Collett noted that the drafting team received help from James Case and Jason Marshall in refining the BES reliability functions and that generation was, in part, revised as a result. The Working Paper Subgroup presented examples of BES subsystems that were intended as simple ways to conceptually illustrate that while the individual impact may be small, it might be big when controlled and is the reason for a high impact determination under common control system. The challenge for the SDT in going forward is developing clear language and criteria when trying to describe these things that can capture the different aspects.

John Lim provided an overview of the current Section on 3rd Party Overview noting that two oversight entities identified in Order 706 - were Reliability Coordinators and Regional Entities. The SDT engaged in a substantial discussion of this section.

The Working Paper Subgroup also presented a new depiction of the"targets of protection" noting that the essential cyber systems don't necessarily stop there. The SDT suggested ways to provide a graphic description without the use of a target metaphor, as was included in the draft Working Paper.

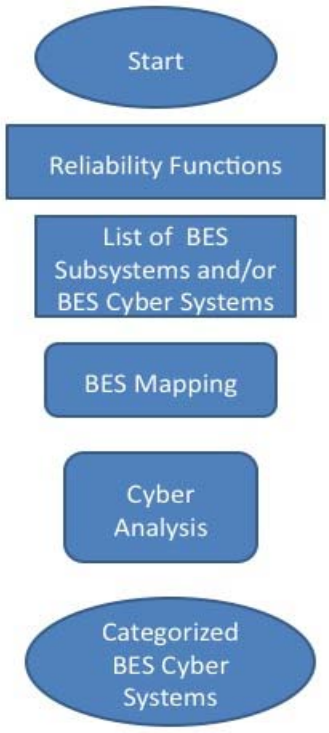
To gain a sense of the SDT and to provide a focus for ongoing SDT discussions, the facilitators asked the members to rate each section of the working paper based on their view of whether the current sections were ready for sharing with the industry (*Are the concepts contained in the working paper sections acceptable for sharing with the industry? 4= Acceptable; 3= Acceptable with minor concerns; 2= Unacceptable unless Address serious concerns; 1=Unacceptable)* Following the rating, the SDT took up a second round of focused comments and suggestions for changes to the seven sections of the document receiving less than a 3.0 average rating. These discussions occurred in the afternoon of June 17 and the morning of June 18 including:

1. 3rd Party Oversight of BES Subsystems Categorization - Review of Concerns (1.9 of 4 Avg.)
2. Defining the Target of Protection (2.5 of 4 Avg.)
3. External Cyber Systems (2.6 of 4 Avg.)
4. Categorization- BES Subsystems, Cyber Systems, and Final Cyber System
   - Categorization of BES Sub-Systems (2.8 of 4 Avg.)
   - Categorization of Cyber Assets (2.8 of 4 Avg.)

- Final Categorization of Cyber System based on Impact to BES (2.5 of 4 Avg.)

5. Identification of Essential Cyber Systems (2.7 of 4 Avg.)

The SDT broke into small groups to discuss and further develop the following scenario concerning the BES Subsystem and Cyber System categorization approach. This led to a further discussion of developing a different sequence for the categorization approach. There was broad SDT member support for this simpler graphic depiction as a working concept for inclusion in the Working Paper.



The SDT Chair, Co-chair, and Members expressed their thanks and appreciation to all those participating on the Working Paper Drafting Subgroup. Before the Vancouver meeting, John Lim agreed to work with Phil Huff, Jackie Collett, and all other interested SDT members to:

- Produce the next draft of the Working Paper, which will be circulated as a final draft for consideration in Vancouver before seeking industry comments.
- Take the review comments of the "target" and produce another graphic using an alternative depiction.
- Continue efforts to develop additional working papers for SDT review going forward on BES Risk Management and Security Controls.

Bob Jones, SDT facilitator, noted the proposal to proceed with CIP 002's development in the remaining half of 2009 and refine it after several of rounds of comments from the industry.

The Chair reminded the SDT Team Members that the SDT would try to establish the 2010 meeting schedule at the July SDT meeting in Vancouver, B.C., Canada. For the time being she noted that the August meeting will take place as scheduled in Chicago pending confirmation of available meeting space. *(Note: The venue for the August Meeting was changed to SERC's facilities in Charlotte, NC subsequent to the close of the meeting.)*

Dave Norton advised the group of a call for self-nominations closing on June 25 for a new SAR drafting team which would be defining next generation of situational awareness control tools for the BES.

The Chair (Jeri Domingo-Brewer) thanked Jon Stanford for hosting this meeting at BPA in Portland, Oregon. The Chair also noted the progress made on the draft Working Paper and, in particular, the refining and simplifying of the process flow chart in determining the categorization of cyber systems and BES System assets. The Chair thanked the Working Paper Drafting Subgroup members for an outstanding job. Members completed an onsite meeting evaluation form.

The SDT adjourned at 3:00 p.m. on June 18.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Cyber Security Order 706 Standard Drafting Team
DRAFT ELEVENTH MEETING SUMMARY,
JUNE 17-18, 2009
PORTLAND, OREGON

I. INTRODUCTIONS, AGENDA REVIEW AND REVIEW OF SDT WORKPLAN

The Chair, Jeri Domingo-Brewer, and Vice Chair Kevin Perry welcomed the SDT members and guests, and called the meeting to order at 8:00 a.m. on June 17th. Joe Bucciero conducted a roll call of members and participants in the room and on the conference call for each day *(See appendix #2*). The Chair reviewed the meeting objectives and Bob Jones, facilitator, reviewed with the Team and participants the proposed meeting agenda *(See appendix #1*).

Mr. Bucciero reviewed with the Team the need to comply with NERC's Antitrust Guidelines *(See, Appendix #3).* He urged the Team and other participants in the process to carefully review the guidelines as they would cover all participants and observers. He urged all to avoid behaviors or appearance that would be anti-competitive nature and also reminded the group of the sensitive nature of the information under discussion.

II. UPDATES

A. Technical Feasibility Exception (TFE) NERC Rules of Procedure Posting

Scott Mix provided an update briefing to the SDT noting that the posting period for the TFE had closed with 52 organizations providing comments over 450 pages. He reviewed his presentation offered a week earlier at the NERC CIPC meeting and noted that NERC staff is now analyzing the comments received on the TFE posting. All comments have been posted on the NERC web site. NERC staff is now reviewing and considering modifications to the TFEs and will try to get this done as quickly as possible. Mike Assante, the NERC CSO is the Corporate Officer in charge of content. Dave Cook, NERC General Counsel is in charge of procedure.

Mr. Mix noted several issues raised in the industry comments including:

- Making TFEs applicable to other standards where there is "triggering language"
- Requirement vs. sub requirement - anything under requirement can be covered by a TFE without change.
- CIP 003 R2.3, and/or CIP 003 R3 - an exception to an internal policy is not a compliance issue since it is not a reliability issue.
- NERC staff is currently cleaning up definitions.
- Economic security - doesn't appear in this section.

- Clarification of the Pre-approval process in terms of review and approval by regions. There will probably be a greater role than in the original posting.

Member Comments

- Has NERC considered issuing a statement on requirements/sub-requirements? The statement should cover all reporting so it is consistent.
- Any reaction from CIPC to CIP 003 R2.3? No reactions to this.
- TFE under new procedure is in effect July 1? However, the TFEs are not approved yet. If the TFE process is not approved before June 30, it is in play? If it is in play, and we have a TFE on the table, can we be held out of compliance? Problem for registered entity, ERO and regional. Self-reports of non-compliance? Bad position based on scheduling, workload.
- Adhere to the spirit of the process? Need to resolve this. Sanctions component may be adjusted in this transition period.
- Does NERC have an alternative plan?
- FERC is aware of issue and plans to discuss with NERC to handle this.
- Escalate the TFE issues to the Commission. Roger Lampila will take a note and check with Mike Assante.
- Single request covering multiple requirements for a covered asset.
- How to submit to multiple regional entities?
- Need to resolve the senior manager language - the senior manager or delegate. Why would it be any different? The company's assigned authorizing officer? Sign off on the TFE.
- Removing automatic 60 days. Maybe NERC has 60 days to extend the request. Won't be an automatic disapproval.
- NERC needs to be timely in its response.
- Mitigation plans go to regional entity.
- Will a TFE disapproval generate a spot-check? Problem is a self-report compliance plan. If you don't, self report a denied TFE. Will that invoke a spot check? Sufficient cause to trigger a spot check. No surprise. Advantage to do as a self-report.
- Canadian entities - self report to whom? To the regional entity? Follows the rules for self-reporting. Agreement in place but different for each province.
- Wide area analysis - not as justification for denying TFE. Rewording with fairness in mind - understanding the impact not necessarily for purpose of denial (maybe the first one, not subsequent ones).
- TFE's need to be dealt with on their technical merit only.
- Anticipate BOT to adopt TFE. When? No sooner than August 4-5. Realistically looking at the November meeting.
- BOT Actions without a meeting? Doesn't apply to this.
- FERC process for acceptance probably 2010.
- Reaction at CIPC? Mostly they understand.
- NERC and the industry are trying to make the best of a bad situation.

Mr. Mix concluded that:

- NERC staff, including SAIS and outside counsel, is reviewing comments, making responses, and preparing modifications. NERC BOT will authorize for adoption. There isn't a requirement for another round of public comment nor a response-by-response submittal like the ANSI standards process. Will pass by the Members Representative Committee (MRC) before presenting to BOT for authorization.
- Will follow the same process for adoption and FERC approval.
- In addition Scott referenced FERC Order 706 B on CIP standards for nuclear. NERC has reconstituted the Cyber Security Version 1 SDT. It has 180 days after issuance of the Order (Sept 15). It has met twice by teleconference and convened a 4-hour town hall meeting. Tim Roxy, Scott Mix, and Gerry Adamski were present from NERC, and Scott Morris with the NRC talked about NRC revisions and noted the newly identified critical asset plan was a good starting point for the implementation plan. Scott also noted the town hall produced a good dialogue and excellent questions

B. Update on VSLs-VRFs

Scott Mix, on behalf of David Taylor, NERC, provided an update on the VSL/VRFs. They were posted in May 2009 for industry comment, and the comment period is now closed. The 93 pages of comment received from 10 entities are being reviewed by the SAR drafting team, and Version 1 & 2 VSLs must be filed by July 1. NERC didn't receive a lot of comments on Version 2.

Member Comments

- Does the NERC BOT have authority to file even if industry rejects the VSLs? Yes, with "extenuating circumstances."

III. SDT PHASE 2/VERSION 3 DEVELOPMENT PROCESS - THE "WORKING PAPER"

A. Overview of Phase 2/Version 3 Work Plan

Stu Langton reviewed with the SDT the milestones in Phase 1 and Phase 2 of the SDT work including the work in Little Rock that framed the challenges, the subsequent development of "white papers" following the Washington D.C. meeting in December, 2008 and further review and refinement of those and other papers. This resulted in the SDT convergence on a single consensus approach in Orlando that was refined further in Charlotte and Boulder City with John Lim, Jackie Collett, and Phil Huff leading an expanded drafting team to continue to refine the draft working paper between meetings. The working paper provided a basis for

developing and testing the following consensus points in April that were subsequently offered to the NERC Members Representative Committee (MRC):

1. The Standards should require a BES impact assessment as an initial approach to categorizing BES Cyber Systems.
2. The impact categorization of Cyber Systems will be based on reliability functions of the BES to achieve Adequate Levels of Reliability.
3. The Standard's BES Impact Assessment will consider a categorization process.
4. The Standards will require oversight of the categorized list of BES assets by entity types which have a more complete wide-area view of the BES.
5. The Standards will categorize Cyber Systems supporting, either directly or indirectly, the reliability functions of the BES and apply security requirements (or controls) that are commensurate and appropriate to their potential impact on the BES.
6. The final Cyber System categorization will reflect the impact to the BES based on a loss of availability, integrity, or confidentiality of the Cyber System.
7. The Standards will provide Organizations with reasonable flexibility in applying equivalent security controls on the basis of compensating controls and environmental considerations.
8. The Standards will address the complex nature of BES functions and interconnected Cyber Systems, both within and between multiple organizations.
9. The Standards will state explicit criteria for the BES Impact Assessment.
10. The Standards will state explicit criteria for the Cyber Impact Assessment (including use and misuse of cyber systems).
11. The Standards will include a methodology to merge the BES Impact Assessment and Cyber Impact Assessment into a final Cyber System categorization.

Joe Bucciero, with the SDT facilitation team, reported that following the Boulder City meeting the Drafting Team has been supplemented with BES expertise from Jim Case, Jamey Sample, Jack Bernhardsen, Jason Marshall, and Sam Merrill. Others have also been invited to participate, but have not yet participated.

B. Phase II Working Paper Overview Presentation and SDT Discussions

On behalf of the SDT, the Chair thanked John Lim, Jackie Collett, Phil Huff, and the other members of the drafting team for working productively since the Boulder City SDT meeting and expressed her gratitude for their leadership and good efforts. John Lim and Jackie Collett jointly presented the working paper (*See Appendix #6).* They noted the expanded team met twice by phone/WebEx following the Boulder City meeting.

1. Overall SDT Comments on Working Paper

The Team engaged in an initial discussion of the working paper as part of the overview presentation. A summary of the SDT member comments are noted below. The presentation

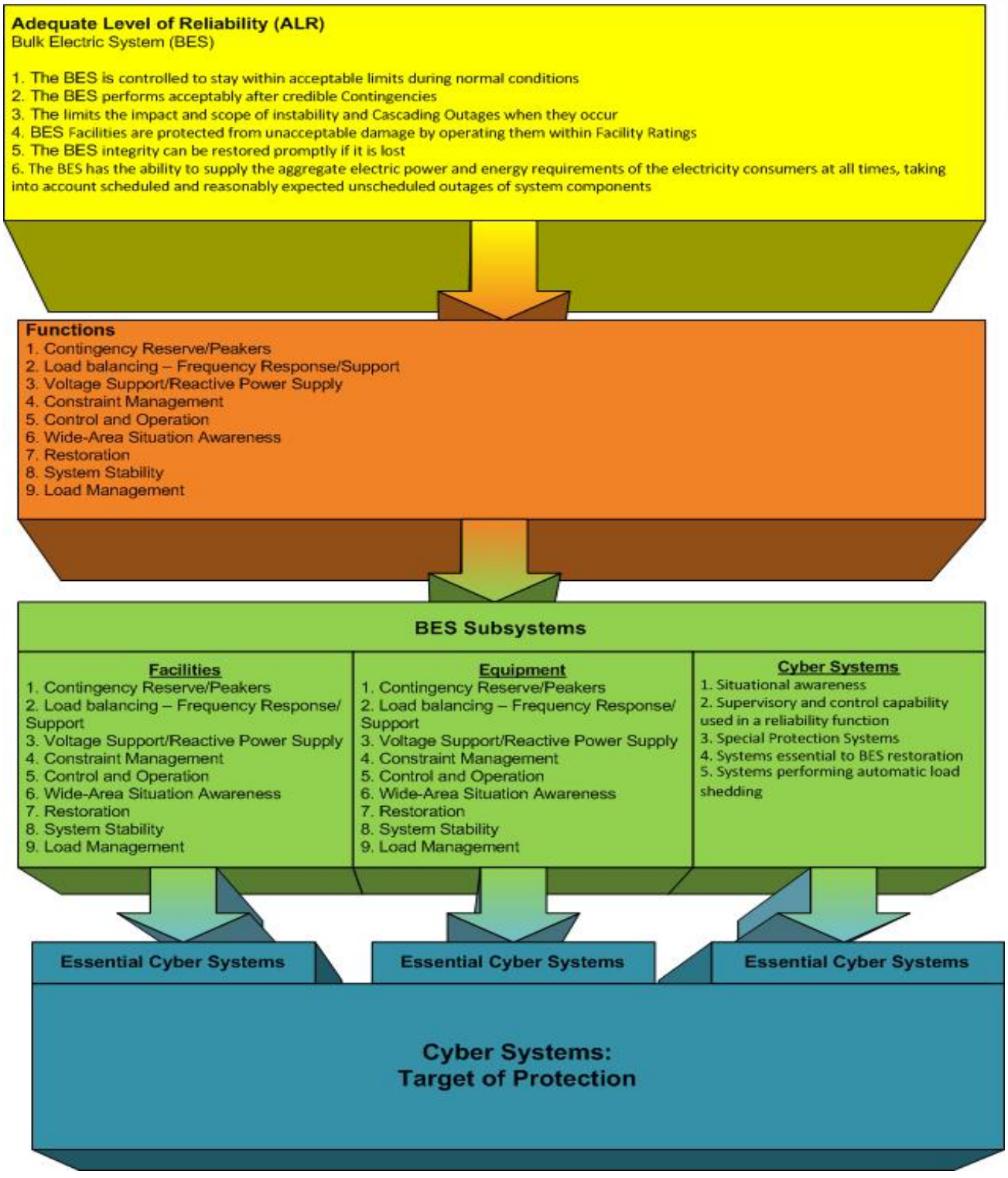
was interactive with the SDT who posed clarifying questions and offered ideas for refinements.

Member Comments- Overview

- The SDT should note that the recent Congressional testimony speaks of dealing with a "sustained cyber attack" which may be different from providing CIP protection.

2. Introduction

John Lim provided an overview for a new chart highlighting BES reliability functions and the conceptual approach the paper is taking in categorizing cyber systems:


Adequate Level of Reliability (ALR)
Bulk Electric System (BES)
1. The BES is controlled to stay within acceptable limits during normal conditions
2. The BES performs acceptably after credible Contingencies
3. The limits the impact and scope of instability and Cascading Outages when they occur
4. BES Facilities are protected from unacceptable damage by operating them within Facility Ratings
5. The BES integrity can be restored promptly if it is lost
6. The BES has the ability to supply the aggregate electric power and energy requirements of the electricity consumers at all times, taking into account scheduled and reasonably expected unscheduled outages of system components
Functions
1. Contingency Reserve/Peakers
2. Load balancing – Frequency Response/Support
3. Voltage Support/Reactive Power Supply
4. Constraint Management
5. Control and Operation
6. Wide-Area Situation Awareness
7. Restoration
8. System Stability
9. Load Management
BES Subsystems
Facilities
1. Contingency Reserve/Peakers
2. Load balancing – Frequency Response/ Support
3. Voltage Support/Reactive Power Supply
4. Constraint Management
5. Control and Operation
6. Wide-Area Situation Awareness
7. Restoration
8. System Stability
9. Load Management
Equipment
1. Contingency Reserve/Peakers
2. Load balancing – Frequency Response/ Support
3. Voltage Support/Reactive Power Supply
4. Constraint Management
5. Control and Operation
6. Wide-Area Situation Awareness
7. Restoration
8. System Stability
9. Load Management
Cyber Systems
1. Situational awareness
2. Supervisory and control capability used in a reliability function
3. Special Protection Systems
4. Systems essential to BES restoration
5. Systems performing automatic load shedding
Essential Cyber Systems
Essential Cyber Systems
Essential Cyber Systems
Cyber Systems:
Target of Protection

He noted the working paper suggests that this "proposed cyber system categorization approach includes the consideration of NERC's mission, the essential functions necessary in achieving this mission, an impact based methodology to categorize its BES subsystems and the associated cyber systems engaged in the process, and finally the deterministic derivation of an overall impact based categorization of the cyber systems, with the anticipated application of cyber security requirements commensurate with that categorization. This parallels general approaches to risk management practices, which focus first on identifying key processes necessary for meeting high level objectives, then drilling down into supporting processes."

Member Comments on the Chart

- Are the ALR references taken verbatim? Are these words "chiseled in granite"? Change to BES vs. systems. If it meets all of the following characteristics.
- Received some comments on last bullet.
- These are BES reliability functions believed to be necessary to maintain a reliable BES.
- Consider annotating the diagram to illustrate what is meant.
- The Working Paper Drafting Subgroup knew going in this would be more cumbersome than what we have.
- Should we identify the cyber assets first?
- Working Paper Drafting Subgroup presented the concept for reaction
- Identifying cyber assets first may be better in some cases. Whether you do the assets - you are coming back to same list in the end. Perhaps we can provide some flexibility on which way entities may want to go on this?
- Clarify what is the difference/distinction of a cyber impact vs. BES impact? Look at cyber impact in terms of its function and how it fits in BES. Impact of cyber device on BES subsystem.
- Positive side of big picture is that we are signaling we are proposing going in considering both aspects and how they interact to achieve the reliability outcome is important.
- Should the "hard and fast line" of over 500 kV be a minimum baseline?

3. BES Reliability Functions

Jackie Collett noted that the Working Paper Drafting Subgroup received help from James Case and Jason Marshall in refining the BES reliability functions *(pp 11-15 of the Working Paper)* and that generation was, in part, revised as a result.

Member Comments- Overview (**BOB: These are duplicate comments from the previous section above. Is that what you wanted?**)

- "Peakers"? Each will touch on some or multiple components of ALR.
- Are the ALR references taken verbatim? Are these chiseled in granite words? Change to BES vs. systems. If meets all of the following characteristics.
- Consider annotating the diagram to illustrate what is meant in different parts of the chart.

- The Working Paper Drafting Subgroup knew going in this would be more cumbersome than what we have.
- Should we identify the cyber assets first?
- Working Paper Drafting Subgroup presented the concept for reaction
- Identifying cyber assets first may be better in some cases. Whether you do the assets - you are coming back to same list in the end. Perhaps we can provide some flexibility on which way entities may want to go on this?
- Clarify what is the difference/distinction of a cyber impact vs. BES impact? Look at cyber impact in terms of its function and how it fits in BES. Impact of cyber device on BES subsystem.
- Positive side of big picture is that we are signaling we are proposing going in considering both aspects and how they interact to achieve the reliability outcome is important.
- Should the "hard and fast line" of over 500 kV be a minimum baseline?

4. Identification of BES Subsystems

The Working Paper Drafting Subgroup presented examples of BES subsystems that were intended as simple ways to conceptually illustrate that while the individual impact may be small, it might be big when controlled and is the reason for high impact for under common control system. The challenge for the SDT in going forward is developing clear language and criteria when trying to describe these things that can capture the different aspects.

Member Comments

- SDT should be careful - when we talk about "restoration" as people may tune out if they believe reliability is not the issue. Let's try to address these issues with the industry head on.
- In the Final Categorization of Cyber system- Example 1. BES Subsystem A with Relays A, B & C. What changes the BES subsystem impact.

5. Third Party Oversight

John Lim provided an overview of the current section noting that two entities were identified in FERC Order 706 - Reliability Coordinators and Regional Entities. The current draft pointed out that, "Of the 17 Reliability Coordinators in the NERC Compliance Registry, 12 are registered under multiple functions (i.e., BA, TOP, IA, TSP, TP, PC). These 12 RCs could not meet the FERC Order 706 requirement for "external" review for their other registered functions. As an example, Midwest ISO is registered as a RC, BA, PA, and TSP. Midwest ISO RC could not review the list of BES subsystems from the Midwest ISO BA while meeting the FERC requirement for an "external" review. Thus, a third-party review of the third-party review would be required."

Member comments

- RC's oversight authority? Liability and risk in determining whether an asset should have been identified or not.
- Task the RCs to provide guidance. We will need a "safe harbor".
- FRCC - Regional reliability Organization. Member services functions with FRCC - with different committees. Regional organizations that perform functions other than compliance. E.g. FRCC operating committee.
- RCs don't perform reliability function - this is separate function. They have the proper view/ability to have the proper view that REs don't have.
- Is there a conflict of interest for the REs?
- Is there a way to develop this so that you don't need a 3rd party review- because you can agree on the methodology as producing the correct result.
- RE vs. RRO issue: Different interconnections do things differently. Jurisdictional elements - RE is it right now for the new NERC ERO. RROs only exists in the previous "council" world. RROs were never functional models.
- RRO vs RE functionality - different in different areas. Varies on how functions are set up, e.g. differences between Eastern and Western interconnection?
- RC's probably come the closest for surveillance. Need to do it in a "hold harmless" environment.
- Is this an IMPO (???) like function? Technical arbiter. If they are told not to go towards the RCs, they won't go there. Not clear for how industry is overlaid on functional model.
- Conflict of interest with the Regions.
- Create a new kind of arms length entity - serious experts and knowledgeable people. This is not a small thing. No big picture.
- FERC representative, Mr. Peters, indicated that this is a difficult issue. Should be some way for companies to get assistance so they don't get nailed if they get something wrong. There will be conflict of interest on some options. He will be talking with staff and briefing new commissioner coming in soon.
- This implies analysis but how much is not clear. RC to the RE function. Not purely a statutory function. Only because compliance exists that it has to be performed. Is it reliability related? If it is falls under RC. Don't have the capacity currently to provide level of analysis.
- This is based on an electrical system view of the world.
- We need consistency.

6. Identification of Essential Cyber Systems

The Working Paper Drafting Subgroup noted that the change in the introduction of BES subsystems is consistent with the new definitions. This is the introduction of essential cyber systems.

Member Comments

- What are the key systems we need to put a focus on protecting vs. identifying high/medium/low?
- SDT is okay with the current draft section.

7. Categorization of Cyber Systems

The Working Paper Drafting Subgroup presented an overview of this section noting that:

- The draft is tentative and conceptual.
- The availability and integrity have a bigger impact than confidentiality on the BES.
- Work out how to deal with these further when SDT works on the standards and controls.

Member Comments

- How would a periphery system (AC) be lumped into groups? We will address that when we get to "target of protection" section.
- "Directly" vs. "indirectly"?
- Is this an impact assessment vs. a categorization? How does time factor into this concept? For a minute, hour, day, month a year. Does it factor into high, medium, low. Longer period for availability, shorter for integrity.
- May factor into criteria.

8. Final Categorization of the Cyber System Based on Overall Impact on the BES

The Drafting Team described the concept they are presenting as suggesting you will have finite ways to do this with the end product resulting in the same number. This categorization in turn will determine the selection of the menu of controls.

An example of the application of this approach in an evaluation matrix is shown below:

> **Note:** This table is a visual representation of what the categorization should look like, it's not the actual table.

Asset Impact -->	High	Medium	Low
Cyber Impact:			
High	5	4	3
Medium	4	3	2
Low	3	2	1

The Drafters noted that to the left is the BES system, to the right is the Cyber System, and you merge these to get final categorization.

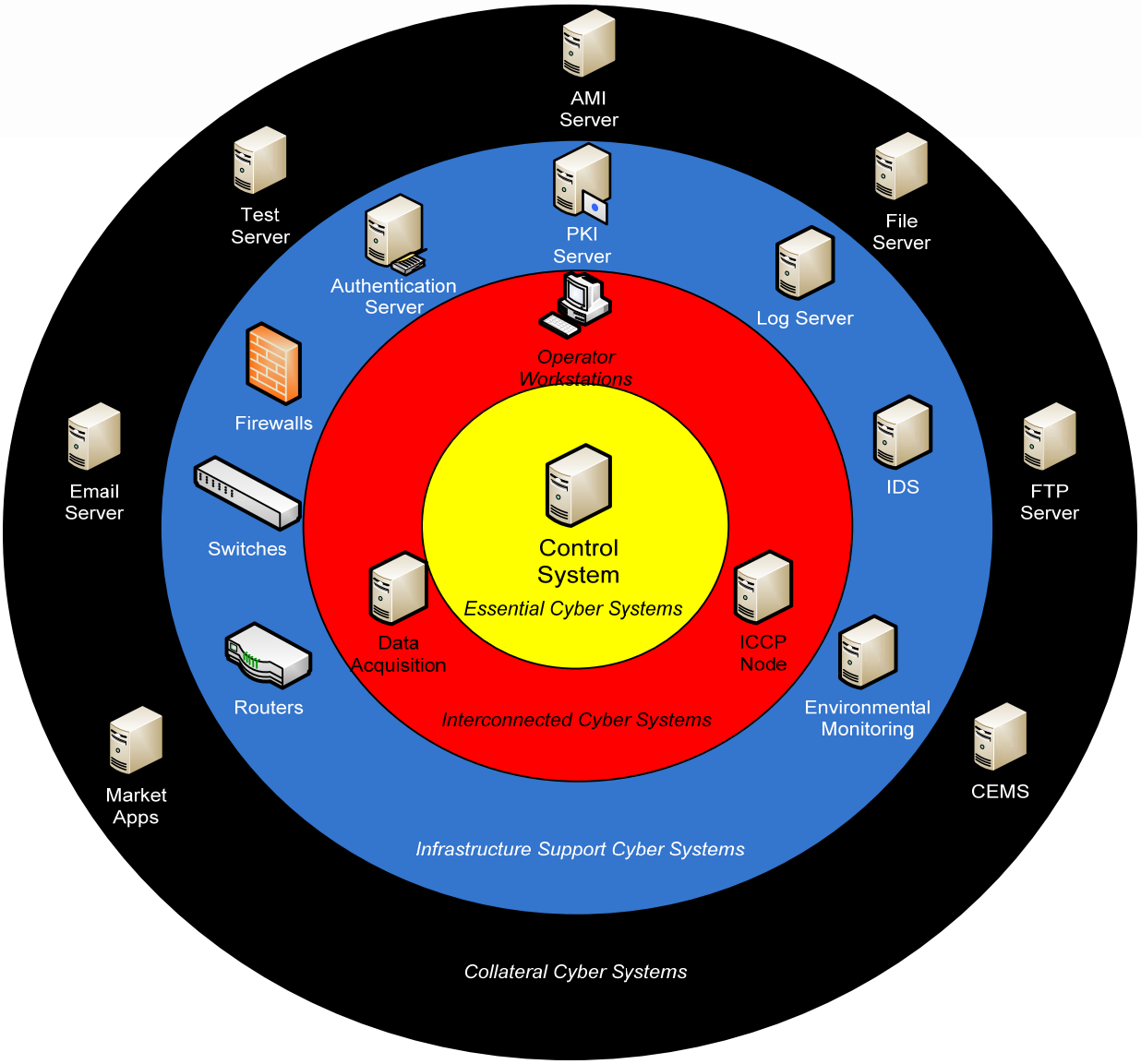
9. Target of Protection

The Drafters noted that the essential systems don't stop there:

1. Essential cyber systems - in middle, e.g. control system
2. Next: Interconnected Cyber Systems, e.g. data acquisition, ICCP node, operator workstation
3. Infrastructure Support Cyber Systems: e.g. switches, routers, firewalls, log service etc.
4. Collateral Cyber Systems: market apps, email server, test server, AMI server, etc.

Comments on Target of Protection

- EMS system in a control center? Fire suppression system and AC control system? Conceptual point is that you must protect them to some level and you can't just ignore. Level of protection depends on impact.
- Environmental monitoring and controls included. Checklist of the things you need to include. Sounds workable.



- AMI systems (smart grid) will be more in the mix going forward. Those may need more protection than collateral cyber systems.
- Market applications and control systems work together in an integrated fashion and may need to be treated together as essential.
- Is there going to be flexibility in this? Don't want the industry to draw the wrong idea from this depiction.
- Market centers playing an increasing role in reliability (nodal). They may need to be in closer to essential. E.g. retail electric provide - way you control and represent your load may make it more essential.
- Address more of these emerging entities.
- "Enabling technology" for perimeter devices and how to protect is an issue.
- Virtual systems coming in - virtual switchers and routers = where do they fit?

- Need to be clear as to what time frame we are focusing on.
- Time frame - CIP does not include planning - real time operation. Worry as well about how it is connected not just when.
- Included because it is a collateral system.
- Not all market operations/functions are day - ahead planning.
- Functions and balancing authorities - how are they treated?
- Ask what is the application doing, and how is that function impacting on the BES? Keep this in mind we may need to locate it in both realms. Real time market control system may belong in essential systems.
- As companies "virtualize" environments, functions become "cloudier." Does the level of protection change because of function or an attack perspective? If they don't perform an essential function, they will be on the collateral list.
- From the perspective of a vertically integrated utility - 8 or 9 BA functions. Who is what, where? What scared Jim Case the most when he was reliability coordinator? "spooks, schedules and tags." E.g. billing is out of this. When put IP on then it changes.
- Salience of market applications - 1 hour in the life of reliability coordinator.
- Who is running email in their control environment?
- Talking first, now, about **what** to protect then later we will get to how to protect it. Shouldn't worry now about how to do this. 1 road leads down reliability requirement another goes another way.
- E.g. OATI - market app to remote platform - used to drive AGC. Not the server, it is the data that is important not the market app unit.
- Got into contract SAS70-2- NERC CIP is in contract will be compliant. Have protection on server.
- Different systems - where is the back to maintain as a critical asset - back up email system to support - costs are significant. Layer of targets and ways we lay application - up to each SCADA engineer - won't be able to categorically say - no two will probably look alike.
- Critical server for business reasons vs. reliability.

10. External Cyber Systems

The Drafting Team provided an overview of this section noting that references to the Interconnection section in the paper. The concept is to put adequate controls to protect the whole system with contractual agreements to protect system to the level needed. The Registered Entity is responsible for protecting cyber systems.

11. Applying Security Controls

The drafting team provided an overview of the section noting that under the current standard you are either in or out, but the application of security controls will allow a greater degree of protection and this would be taken up in the hard work ahead in 2010.

C. Rating the Current Acceptability of the Working Paper Sections following the Overview

To get a sense of the SDT and to provide a focus for ongoing SDT discussions, the facilitators asked the members for rate each section on their view of whether the current sections are ready for sharing with the industry. Following the rating the SDT took up a second round of focused comments in the afternoon of June 17 and the morning of June 18.

Categorization of Cyber Systems Concepts – SDT RATING RESULTS 6-17-09
Are the concepts contained in the working paper sections ready/acceptable for sharing with the industry?
4= Acceptable**; 3**= Acceptable with minor concerns; **2**= Unacceptable unless Address serious concerns; **1**=Unacceptable

	Avg.	4	3	2	1	T
•BES RELIABILITY FUNCTIONS	3.6	11	5	1	0	17
•IDENTIFICATION OF BES SUBSYSTEMS	3.0	2	13	2	0	17
• CATEGORIZATION OF BES SUBSYSTEMS	2.8	1	11	5	0	17
• **THIRD-PARTY OVERSIGHT OF BES SUBSYSTEMS/ CATEGORIZATION**	**1.9**	**0**	**0**	**16**	**1**	17
•IDENTIFICATION OF ESSENTIAL CYBER SYSTEMS	2.7	2	8	7	0	17
•CATEGORIZATION OF CYBER SYSTEMS	2.8	2	9	6	0	17
•EXTERNAL CYBER SYSTEM DEPENDENCIES	2.6	2	7	8	0	17
•FINAL CATEGORIZATION OF CYBER SYSTEM BASED ON OVERALL IMPACT ON THE BES	2.5	4	8	4	1	17
•DEFINING THE TARGET OF PROTECTION	2.5	2	4	**11**	0	17
SECURITY CONTROLS TO THE TARGET OF PROTECTION	3.3	6	10	1	0	17

D. Second Round of SDT Comments on Working Paper

The SDT reviewed on a second round the seven sections of the Working Paper which received less than a 3.0 average rating. Members were asked to describe the concerns that led them to provide a 2 or 1 rating for a section and the SDT discussed possible options for addressing these concerns.

1. 3rd Party Oversight of BES Subsystems Categorization- Review of Concerns

Are the concepts contained in the working paper sections acceptable for sharing with the industry?
4= Acceptable; 3= Acceptable with minor concerns; 2= Unacceptable unless Address serious concerns; 1=Unacceptable

Working Paper Section	*Avg.*	4	3	2	1	*Total*
3rd Party Oversight of BES Subsystems Categorization	**1.9**	**0**	**0**	**16**	**1**	**17**

Member Comments on 3rd Party Oversight Ratings

- Were there any 2 or 1 ratings based on the level of detail? None.
- Do we need this in our concept paper? Should it be removed?
- **Audit vs. Oversight?** Concept of being audited- doesn't that imply 3rd party oversight?
- Does oversight= audit? Audits do play a role in this at an untimely expensive stage in the process.
- Analysis associated with this oversight- point is reliability not compliance.
- Let in the Reliability Coordinator and call it done?
- We need a front loaded process- what do I need to do to get it right going forward. Should not be considered audit function.
- Should we get industry feed back on having the RC do this?
- 706A- rehearing order- FERC- industry sorts out on a contractual basis.
- Voted 1 because of the belief that this section is a non-starter. Issue is fraught with problems and pitfalls. Rather than trying to propose a solution, drop it out or acknowledge and discuss all the problems that have to be overcome in order to do a 3rd party review.
- Discuss the problems vs. a solution.
- This issue is larger than CIP 002- it might be wise to take it out of paper altogether. Consider developing a separate working paper?
- Industry might respond - why don't they tell me what to protect?
- **Quality Control vs. Categorizing Cyber Systems.** Voted 2 because it doesn't fit in terms of concepts trying to communicate to the industry. More of a quality control element vs. a concept about identifying and categorizing cyber systems and assets. FERC in the order was looking directly at version 1`of CIP and its "all or nothing approach." This is a different concept that directs us towards what is most important to protect.
- The drafting group can take the verbiage out and identify there is an issue and will address going forward.
- Concerned this, as drafted, will provide a distraction from the paradigm shift suggested by the broader conceptual approach.
- Criticality level of BES and cyber asset. More impetus for 3rd party overview. Acknowledge to extent "individualism" is taken out of the process, it will be less important for this overview.

- To certain extent- we need more industry input. If we can show them there is a necessity for 3rd party oversight if we go with the old CIP approach, it will be clearer why change is needed. Everyone is responsible for security if you are connected to it. If we go with the new approach, oversight not as big an issue. Anyway we go we have a lot of work to do in this area for both 002 and for the industry.
- If we have a 3rd party analyzing these lists- we will need to provide a whole process for appeals etc. If we could come up with a way that utilities can't use "don't have any critical assets." The current draft calls for an arbitration procedure.
- Mike Assante is taking the lead. This will need to be performed.
- Last thing we want to see is increasing gamesmanship through a new approach. We must get around and place behind us those people trying to keep cyber assets off their list.
- Lots of stuff falls between the cracks. Need to keep coming back to reliability and not compliance.
- Clearly this isn't ready for prime time. Could we reword some of this? Oversight will depend on how it is written- change language- depends on how proscriptive the standards develop.
- That could get some comments from industry as to one approach or the other.
- Somebody will need to take a big picture look at this.
- Sub station - e.g. CIP 002 - task the asset owners. None of the questions focus on ownership vs. operators.
- As a practical matter, is this more bother and trouble that it is worth. Suggest pulling this out and put off to another white paper.
- We should say something but pull the "proposal".
- Question for group- do we strike it totally or do we acknowledge briefing- any issue of wide area overview will be dependent on latitude given to the entity. In favor of getting rid of it outright.
- If a Balancing Authority has the requirement for another entity to protect the other entity assets- occurs in the wide area view? Is there another way to determine?
- Everyone knows that 706 said you need oversight, so we probably have to say something. Even to say, method of oversight doesn't impact on this methodology. Have to say something about "the elephant in the room."
- Reliability considerations- don't use oversight in the paper. Give FERC time to work.
- Note that there are "other issues" in the order that the SDT is not addressing, e.g. BPA's confidentiality issue. Shouldn't place the focus in on this.

At the conclusion of the discussion, the facilitators conducted a straw poll asking members to choose the conceptual approach they preferred for this section:

- Improve it and include as a full section - 0 yes
- Strike it entirely - 10 yes
- Acknowledge in a limited way. 7 yes

The facilitators then tested the support for the following: "Regardless, we should have a group that will continue to look at this issue"–14 yes/2 no

Scott Mix agreed to craft some draft language that there are other considerations in the order that do not directly play into a categorization methodology and will be taken care of at the appropriate time. On June 18, Mr. Mix offered the following sentence to add into the Introduction of the Working Paper:

> "This paper deals only with the identification and classification of BES assets and cyber systems. There are a number of other issues raised in 706 not addressed in this paper. The Team will be soliciting industry feed back on other issues as a part of the CIP standards development process."

Member Comments

- Should be noted as a future consideration
- Focus on task at hand on this paper.
- RK: likes the words. "Dealt with separately"- through additional working paper- will the industry think "secret"
- The team will be soliciting industry feed back at a future date as part of the development process.

6. Defining the Target of Protection

Are the concepts contained in the working paper sections acceptable for sharing with the industry?

4= Acceptable; 3= Acceptable with minor concerns; 2= Unacceptable unless Address serious concerns; 1=Unacceptable

Working Paper Section	*Avg.*	4	3	2	1	*Total*
Defining the Target of Protection	**2.5**	**2**	**4**	**11**	**0**	**17**

Member Comments on Rating and Concerns

- Were there any 2's on the issue of insufficient detail? No
- Gave it a 2. Confused the issue of after categorization of systems - seemed to add a additional piece of complexity. What did it mean in terms of applying controls.
- Any box becoming compromised, becomes easy to compromise every other box. Does this imply there is less protection needed in blue vs. red ring?
- Need to look at the paper and the diagram to understand the intent. Intended to get people trying to think about. Text indicates the sequential of identification vs. relative importance.
- Target of evaluation - common criteria of security mechanisms. Each device in the target has to have a profile for that in terms of high/medium/low.
- We need to make sure it communicates message-i.e. level of importance.

- Could modify showing arrows from center out, with language saying the intent of the sequence of identification?
- The words are there. It is a presentation issue.
- We don't have any substation gear represented? Wouldn't hurt to throw a few in. Lots of people in that world.
- We could come up with another example. PLC control system in the center.
- The graphic reinforces the "control center-centric" perception of the SDT's effort. Have a couple of illustrations: 1 for control center, and 1 with a plant perspective? 2 of the same diagrams with different devices on it.
- Essential cyber assets identification- a cyber system essential to operation of BES system and have low impact if compromised.
- A relay is essential to transmission line. How does it fit into overall BES reliability- low.
- Cyber asset essential to operation? Probe collecting info on penetrating.
- High voltage transformer is essential - high impact asset electrically. This protects from overloads, high impacts.
- Epiphany - cyber asset - RTU. In the substation. High impact to the substation. Where is the substation? Or generating plan. In high congestion part of system - loss causes other issues. In rural outpost different impact. Both cases it is a high cyber system.
- Has a high BES impact - rate asset as a 5. Can't view cyber asset in a vacuum by itself. Pay attention to BES ranking as well.
- Still conflicted order in which you do things.
- Confused - "essential cyber system." When talking about cyber impact - how could it be anything other than a high? Essential cyber system - digital relay not connected to anything. Cyber impact is low or medium. Same relay but talking to other relays, maybe a high cyber impact.
- Are we mixing threat, vulnerability and impact? That may be the source of the confusion.
- Cyber system could be everything or small - flexibility of deciding for yourself. Give a broadly scoped cyber system and narrowly scoped cyber system for the targets.
- CEMS e.g. of "targets"-- power plant only, substation only, control system only,
- 2 impact ratings. Analogy to FIPS 199.
- Categorized BES subsystems as drawn as 2 independent processes.
- If the arrow goes up to cyber systems and feeds into categorization.
- Change the terminology - want to end up with a categorized assets.
- Short cut - line distance protection relay. H/M/L to line protected. Apply that to all BES lines.
- Some confusion in the terms e.g. essential cyber systems vs. "critical".
- This is the impact part of a risk analysis. Don't focus on final result of numbers as they apply to protection. Going from categorization concept into protection concept. Should be based on threat and vulnerabilities.

- May be jumping here from impact levels- to target of protection without consideration of other elements - e.g. risk analysis, threat analysis? The leap from categorization to protection without reviewing the role of risk
- Missing piece - across the top - what is the impact of the cyber asset? Where it is? What substation in. What is the BES impact.
- May need a "susceptibility score"- how much control does it have, how is it connected? Is it a stand alone, dial up? What kind of operating system does it have? Consider these attributes to determine what is its impact?
- We will deal with some of this in the control side of the analysis. Mentioned in paper that we will deal with this in the assessment of controls.
- May need to deal with this in the working paper.
- More confused. Asset impact and cyber impact - if either is high, then it is considered high?
- Talking about tentacles of control system in assets - if I can get back into control system.
- Logistic management systems - broke into system - bar code readers -
- Think in terms of security in the event of an attack. Risk - high and low. On a given day, risk changes. Make sure you have it partitioned and cover.
- Are we over complicating this process? Overwhelming number in the industry are the smaller entities without the assets to perform this function. New piece - impact of identified cyber asset on the BES. What is the risk or probability? Big companies have resources to do this kind of work. Smaller ones don't have the capacity.
- Let's not use "risk" = financial exposure. Threat vulnerability of impact or possibly "susceptibility."
- Scott Fixmer offered the following process for evaluating facilities:
    1. Id facility assets and loss impact/consequence. By type of facility.
    2. If lose asset what is the criticality (10 different considerations)
    3. Characterize the threat- e.g. is a physical or cyber attack- what are the methods.
    4. Motivation and capability of those who might carry these out.
    5. Relative ease/probability of getting caught/ and of different types of attacks being applied to assets.
    6. Identify who the attacker is likely to be.
- This helps to sort it out but there may be more mitigating factors to apply. This may be most helpful when being audited- numerical ranking of criticality. Semi qualitative.

3. External Cyber Systems

Working Paper Section	*Avg.*	4	3	2	1	*Total*
External Cyber Systems	**2.6**	**2**	**7**	**8**	**0**	**17**

Member Comments

- How many who rated this low was due to the lack of detail? 2 ratings
- Reservations - hadn't gotten a clear representation - is this all inclusive? Service level or other contractual agreement - concern about the turf to cover. Not reliability based.
- This was like an external review topic.
- This may not be helpful.
- Remove or improve?
- Take it off line- there is a lot of work n terms of what this would be. This may be a distraction and may be technically infeasible.
- Many areas this could touch. Require lots of brainstorming to understand the scope of this.
- What do we expect from industry in reacting to this? Feedback on ideas or suggestions for improving
- In the NIST management world- impact analysis and categorizing, selecting controls is next. This is a consideration in selecting controls.
- If this is about the categorization, shouldn't mix with external.
- Is this a necessary segue way? Could it be pulled out?
- Interconnections section. Compress it and move?
- Middle bullet. Consider dropping the sentence?
- Thought of this in terms of EMS consultants.
- Put in something about need to coordinate?
- Vendor connection- vs. interconnection issues?
- You are relying on their data- integrity of that system. Some coordination with provider of data.
- This is exactly what we will see/hear from the industry. We are getting a preview in this discussion.
- This is a lot of work for a couple of people. Get more participation in these kinds of efforts.
- Analogous to 3rd party?

4. Categorization - BES Subsystems, Cyber Systems and Final Cyber System

Working Paper Section	*Avg.*	4	3	2	1	*Total*
Categorization of BES Sub-Systems	**2.8**	**1**	**11**	**5**	**0**	**17**

Member Comments –Categorization of BES Sub-Systems

- More fine tuning need. This was intended as an overview
- Bright line concern with BES subsystem definition
- 3-categorization has to match the population of all possibilities - write definitions to cover the entire population. (45% of population covered?).

- Provide a quick list vs. the definitions provided. Top level or quick overview.
- This simply says categorized assets are needed - method and criteria will come later. Using VRF model of high/medium/low.
- Stop fixating on e.g. rank the criticality of BES assets somehow.
- Throws out as e.g. - industry has current CIP 002 and paper on risk assessment. Provide another example?
- Get together with the BES guys and tighten it up. Get RCs together (Jim Case, Jason, Jack Bernhardsen, etc.).
- References "event classifications" on NERC site - 5 categories. This might be a helpful analogous effort to describe levels. Specific when you see it you know which category you are in. Something along those lines? Look at this conceptually as a graded approach.
- When this goes out - lawyers and engineers will pick apart. Clarity and distinctiveness of the definitions. Will this be subject to too much speculation in terms of interpretation?
- Is industry capable of this? Many won't be able to do the analysis.
- NERC websites - events analysis - alerts, classification scale on left.
- Generator 800 mw, congested area - impact because environment around it compared with one in low congestion area. Approach - 2 identical plants in different parts of country don't have same impact.
- From a RC perspective, concern is stability. Clarify wording vs. examples. Pick something concrete.
- How does a cyber event correlate to these categories? Having a hard time in making the logical connections.
- Does nailing this down help us get our point across?
- Impact of making an impact decision. Scott Mix – items - who are we trying to cover with these standards. Internal problem before - CIP 002 self-selected out of process. Careful not to allow continue that behavior. Will this provide a loophole?

Working Paper Section	*Avg.*	4	3	2	1	*Total*
Categorization of Cyber Assets	**2.8**	**2**	**9**	**6**	**0**	**17**

Member Comments

- Needs more detail and fleshing out.
- This highlights the complexity of the issue.
- Concern we could have cyber systems not associated with BES component with h/m/l. Components not part?
- EMS/ market management system ISO/ITO, not tied to BES components - huge amount of calculations across all different components - info for situational awareness.
- Goes back to cyber system that supports a BES function- good example of cyber system that directly support a BES function vs. a BES asset.
- Okay with words, they are not overly complex. Having to do stuff with BES first. Categorize cyber systems and protect. Leverage what is out there and use that.

- Original proposal- find cyber assets--establish high water mark- high will be high and may work in simplifying. Control center is a BES asset.
- Does the language in definitions, supported by examples, make it clear as to what they are and how to categorize them?
- Correlation between asset and cyber system. Functional piece is the good part. Agree on simplification. List of functions or impacts and then go find cyber systems and map to them. Must be the correlation because we don't know which are important. Hurdle of BES asset correlation part having trouble with.
- 800 mw in Connecticut vs. Texas. Cyber protection purely- does it matter? That today one has greater impact than the other. Does the BES asset impact mean anything?
- If you are a hacker - go at lesser impact asset and go from there.

Working Paper Section	*Avg.*	4	3	2	1	*Total*
Final Categorization of Cyber System based on Impact to BES	**2.5**	**4**	**8**	**4**	**1**	**17**

Member Comments

- From cyber perspective- go for unimportant. Have to have some basic level of cyber security protection. Then may need additional protection. What that it is open to debate.
- Concerns in paper- ALR- credible contingencies don't relate to cyber issues. Don't inadvertently leave open.
- Target to get to h/m/l of systems. Leads to protected measures/controls. 003-009. Idea is to have a baseline set of minimum controls. Whatever low.
- Double impact language- asset correlation. Cyber categorization vs. impact.
- Agree we need to map the functions- through the lens of the assets or some other lens. Clarify that and the industry will understand.
- Numbers in box don't relate to audits?
- Applying controls in different ways? We will have set of controls apply to some and not to others. Threat landscape comes in. Once you get the target. Applying the catalogue- looking at moderate asset and apply controls in high way and that is what would be audited.
- If low BES impact?
- Controls are objectives- e.g. to put encryption in place. (Federal FIPS compliance).
- Five levels too complex. Three is sufficient.
- Government high/medium/low- federal sector it is applied to systems. TVA is a bad example.
- Double impact- how determine resulting impact. If you high water mark this, is this 1 size fits all/ all or nothing.

5. Identification of Essential Cyber Systems

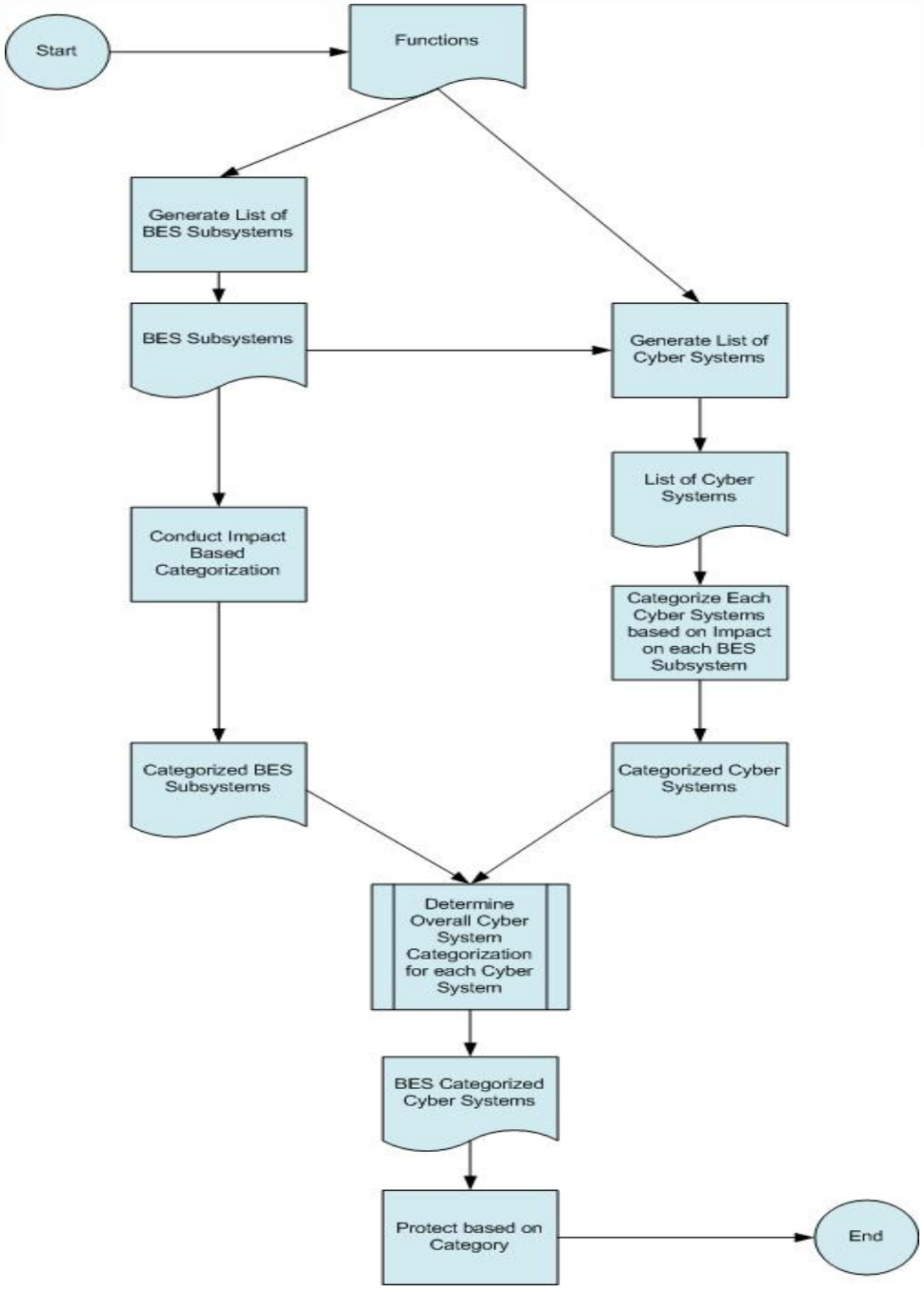
Working Paper Section	*Avg.*	4	3	2	1	*Total*
Identification of Essential Cyber Systems	**2.7**	**2**	**8**	**7**	**0**	**17**

Member Comments

- Was this meant to cover the entire population or an example? More work if intended to cover.
- Show why this would be critical. E.g. metering.
- "Essential"? Low impact essential- distinction- back office- real time. BES related cyber?

E. Review and Refinement of Working Paper Categorization Approach

On the second day, the SDT discussed whether to break into small groups to develop further guidance for refining the working paper. They considered breaking into groups focusing on: Categorization- BES, Cyber and Final; Identification of Essential Cyber Systems; and Target of Protection & External Cyber (including working on chart). They decided to have an open discussion of the categorization concept followed by the development of at least one or more scenarios to put it to a test.



1. Open Discussion on the Categorization Approach

Member Comments

- How should we approach categorization- from cyber systems or from BES asset/sub systems and then looking at cyber systems? The matrix has brought the discussion out.
- At this juncture- may need to take a second step in the matrix.

- Do we need the matrix anymore? Maybe we should talk about different concrete examples in order to identify the benefits and drawbacks of two approaches to categorization. Take an example of a cyber system approach and an example from a BES asset perspective and see if we would come up with the same cyber system.
- Reclamation's experience with 16 SCADA systems. In mapping those to the mission, people came up with different answers and not just a single interpretation for different systems and projects. In the Federal process, everything is included by default- CIP doesn't get this. FIPS 199 divides them up.
- Test cases- can make the correlation between the asset piece and the cyber asset.
- Smaller entities easier to get the cyber part?
- Don't forget that the "C" in CIP is critical not cyber. Critical BES assets that don't have a cyber component.
- We may need a SAR for physical security standards.
- NERC recent response to DHS – clear classification tier 1-3 assets- high med low- megawatts.
- Test both approaches- if both get you there. Pick the simpler one to go to the industry with.
- There is agreement on the approach. We have just engineered something and we need to test it. Will it produce the result we are looking for? The industry will also test this.
- Do we have enough details to test the model?
- FIPS 199- hard process- to get categorization process. Federal starting with a system. Tied to business/mission and mapped the two together.
- Biggest concern that is driving the parallel approach is making sure the impact of BES asset is considered when protecting cyber asset.
- Can we account for the impact of the BES asset without going through the left side using a pure cyber approach? That is the piece to test for the cyber approach.
- If both approaches work, we then agree on a couple assumptions.
- Does the actual impact of BES asset, based on where you are in the grid, have any bearing on how you protect the cyber asset?
- Lots of time, money and vested interest involved in this. In the end, we have to produce a set of standards that can be implemented by the industry, consistently complied with by the industry, from Pinecone Power to the large utilities.
- SDT has been struggling with this in terms of the overall complexity.
- You do protect your cyber assets differently. I pick PLC system in a sub station identical to one in another substation. I shouldn't need to protect at the same level. We will have more controls on the more essential system. Don't see it as overly complicated. I don't think you can come to that result by just working down the cyber side.
- "Back in the day"- cyber linkage to engineering. Don't have to sell the need any more. Cyber important. Access can be gained to trivial equipment. General frame of reference. We don't have to sell the need for linkage quite so hard.

- DHS Tiers 1, 2, 3. It is similar to the left side. If it makes sense and it helps us, it serves our purposes.
- Going to have to both- electrical assets focus- where I roll out protection. Not a one vs. the other?
- Possible test candidates considered: balancing Authorities- Test AGC from the cyber side. Test a transformer over current. Pick a restoration. Control and Operation and Load Balancing- 2 functions? Calculate ACE? Load Management-Function- Control and Operation. 2 transmission and generation operations.

The SDT broke before lunch and a small group developed the following scenario that was presented and discussed following lunch:

Scenario: A large investor-owned utility with 35,000 MW generation capacity across 103 units. One of their plants has three 800 MW generating units. A single RTU receives the control signals (pulses or set-points) for all three units. Each unit is managed with its own PLC/control system. From a span of control perspective, the SCADA/EMS at the generation control center can potentially control or impact all 35,000 MW of generation capacity.

Discussion: It does not matter whether the units are base loaded, on regulation, in reserve, or running at their maximum capacity. It is what the control system is capable of impacting, not what it can impact at this moment in time. If the SCADA/EMS can open plant substation breakers and disconnect the units from the grid, the system impacts that generation whether or not the SCADA/EMS is actually directing generation output (sending the units raise/lower pulses or MW set-points). The RTU in the plant is managing the telemetry data for all three 800 MW units, thus it can impact 2400 MW of generation capacity if it is compromised. The PLC/control system for each unit only controls its own unit, thus its impact is 800 MW. In the scenario, the SCADA/EMS system would have been categorized as High Impact, the RTU as Medium Impact, and the PLC/control system as Low Impact.

Presentation of the Scenario

- Factored in the impact of BES asset in identifying cyber assets performing the function. Identify cyber assets- may be supporting BES asset and have a greater impact.
- 2nd control system used for monitoring /situational awareness- could be pressed into service to control under abnormal situations. It has a capacity to control- not what it is used for. Ergo- higher impact based on what it potentially can do, not what it normally does.
- ICCP node - low- it can go away, I don't care. System not that important to our operations but it may be to some one else.
- All 3500 mw to reliability coordinator via ICCP. From RC perspective it is high.

- I am sending 3500 mw info to RC- categorize as a high- because of what it is actually and what is it capable of doing.

Member Comments on the Scenario and the Categorization Approach

- "Span of control" notion is critical
- If you did it from BES side get to the same result.
- It was essential to setting up scenario- to start with BES functions. It is the branching underneath we are struggling with.
- System Frequency for AGC considered? Yes. How do you ensure you haven't missed something from an audit perspective?
- How to demonstrate to auditor under CIP 002- that you are at least mapping the functions.
- When you de-construct the functions and look at interactions necessary to support the function.
- The key is you started with function.
- Standard should seek to ensure effectiveness. Are you protecting the right thing and how well protecting is the next phase? Could overlook a core piece – in 002 specify mandatory criteria you have to look at.
- If I didn't look at substation first, I wouldn't have known of the problem upstream.
- Factors in BES asset impact with span of control without having to categorize the BES asset.
- Class the RTU as a medium. 2400 mw plant depending on where it is could be low or high in terms of BES impact. Because of where it is and its impact on BES.
- System impact assessment based on modeling of BES - lots of work. NPCC has done it that way.
- Start with impact of asset on the BES.
- Should we give the entity the choice to which side to chose?
- BES asset view point - system conditions change.
- Problem on the Cyber side. Restoration- how to identify a cyber system that supports restoration for a cranking path? Starting from cyber side - numerous elements in BES system- to identify what cyber systems are related to them. A cyber system can support multiple BES functions. Find all cyber assets in the cranking path. Will first find the BES assets.
- Do you need to categorize and impact assess? Yes you do.
- Don't mix cyber and physical systems?
- Some functions it may be done, other functions it may not be done.
- Missed common load generator.
- Sounds like we are saying we need to do both. Eliminate arrow between the 2 paths.
- Cyber perspective - span of control concept on BES side - merge together have a super list. Not two competing process. In the end consider BES. If only do left side you may miss or lower the rating mistakenly.
- Focus on cyber subsystems that directly support BES.

- It is iterative approach (but back and forth, not circles).
- Two parallel supporting efforts to get a super list vs. one subordinate of the other.
- Goal of a categorization of cyber system- consistent methodology.
- Implicit in doing both approaches is the assumption that you have an incomplete inventory on one side or the other. If you had a complete inventory of cyber assets do that side only. With a complete inventory of BES, do that one side?
- Give some more flexibility to do what they want
- Horizontal line should go away at top. Impact assessment of BES assets is a question of what to address first. The impact of BES asset shouldn't alter the level of the
- Generate list of BES subsystems under functions. One system supports moving power and one that support analysis and wide area view.
- It is the "span of control" that we are driving at.
- We are not asking the entity to devise a methodology to do an impact categorization. Standard will provide the criteria to assess and categorize their assets.
- Planning uses catastrophic conditions as a base.
- Try to remove the impression that one side is subordinate to the other. However can't be done in a vacuum. Have to understand the electric system.
- Try to create a single line for the diagram?
- If IT, supporting operations side of business. Start with generating list of cyber systems. Will have a hard time completing an assessment. If you don't start with functions - how do you know?
- The standard needs to give industry the criteria for the categorization.
- Give a list of functions? Will that change -
- Operating functions - these have already been defined by the industry. Version 5 of the functional model -
- However, note that functions are different from functional model. E.g. Entergy - single registered entity with six different functional models. Implementation convention within the organization.

- The reliability functions are applicable to you. Functional model - is not that clean.
- Rely on the functions and then map to BES and cyber assets. Will need lots more detail in the boxes in terms of text explaining the boxes.
- If you took BES analysis - called it "criticality" of specific elements - Cyber analysis- look at consequence of compromising and give it ranking. Where is the synthesis point - gives your impact. Take impact merge with "susceptibility" - and get to your impact
- Interconnectivity is at play? Yes.
- Do we want to say in certain areas of the working paper that the SDT is not sure of the answer? We need to present something with conviction, but not at a great level of detail.
- Link the last box to the next process
- Like the model that has emerged, it should be consistent with the Working Paper but not as detailed. Reflects more flexibility and identifies the big concepts.
- Bottom box is the outcome of the process- identifying what you need to protect- and arriving at the appropriate categorization
- What is the span of control?

- Existing 002 and this? Wrapping all within the reliability function. Every BES asset will be protected at some level.
- Can the SDT live with this conceptual graphic depiction for inclusion in the working paper? Yes.
- Can I go through this? Can't disregard but may not start with inventory of BES assets.
- What is the expectation of the BES analysis, i.e. what will be done with the analysis? All cyber assets inventoried.
- What to do with the BES analysis. Not all 115 relays need the same protection.
- BES analysis? What if left fed into the right vs. working in parallel. Feed this into cyber analysis/ span of control exercise?
- Default BES analysis is high - then purely assessment of cyber assets.
- BES changing all the time? System accounts for contingencies. Changing so much? No.
- We need 75-80% of relays to work when we need them.
- Consider US DHS - Tier I II Critical assets each sector tasked to come up with criteria based list. How to figure out where "big uglies" are. Tier 1 - most impactful. High capacity, high voltage. Tier 2 - size and scope. Tier 3 - everything else. This could eliminate the need for extensive analysis.
- Conceptual language drafted to codify into a standard. This becomes the analysis-identify and classify as a mapping exercise - Find cyber assets BES mapping (criteria) and analysis (use DHS tiers)
- Is this an external process? BES system comparing against criteria?
- Does BES mapping belong here? External process to this sequence? Entity still must categorize. Something needed to verify that mapping is still correct?
- Do once a year. Don't devise the criteria every year. Established outside an entity's process.
- Criteria should appear in a Reliability Standard.
- BES Subsystems vs. assets. Control center are included.
- Restoration is included in Tiers 1,2, + 3.
- Does this pull distribution into criteria?
- IT is a linear model with the same components. Using the DHS = tiers as a departure point. Stand alone standard.
- Perhaps CIP 002 (include the tiers) and CIP 003 features cyber characterization

Member Final Comments on the New Graphic

- Broad support for this depiction on SDT.
- Both start with reliability functions. This is a single vs. parallel path.
- This has BES mapping.
- Big difference - don't need 3rd party oversight of categorization of subsystems.
- More a performance based model - how well did you do the mapping and applying the controls.
- Less a black and white compliance exercise.

- How big a deviation with the current document? Language may need to be clearer that criteria will be provided.
- The diagram doesn't conflict with philosophy behind the working paper.
- Scope of impact and span of control are good concepts.
- SDT should plagiarize content of DHS- refer in more general terms. If want to avoid confusion, pick up concepts without numbers.

2. Identification of Essential Cyber Systems

Member Comments

- Other synonyms for "Essential": Vital, crucial, fundamental, critical, Quintessence-Imperative, indispensible, germane, etc.
- BES cyber systems. Intent to distinguish market systems. Corp cyber assets - we don't want to think about. Control systems and things impacting control systems.
- Is more information needed on "essentiality" criteria mapping? Cross sector cyber security working group.
- Sam Merrill's document? Scott will get this and share it with SDT.
- Equivalent levels between bulk and cyber side. E.g. non routable no longer an in/out criteria. Everything is in, but to a degree.
- Ramifications for Canadian? If DHS, tier 1 and tier 2. If the Canadians can adapt or augment, based on these concepts, there is no issue, much like NIST.

F. SDT CIP Version 3/Phase 2 Process Going Forward

1. Drafting Group Follow Up Steps before Vancouver

Members expressed thanks and appreciation to all those participating on the Drafting Team and to John, Phil and Jackie for leading a tremendous effort in "taking us down this road." John Lim agreed to work with Phil Huff and all other interested SDT members to:

- Produce the next draft which will be circulated as a final draft for consideration and adoption in Vancouver before seeking industry comments on the concepts.
- Take the SDT comments on the "target" section and produce another graphic using an alternative depiction.

The following members agreed to joint the drafting group: Dave Norton, Dave Revell, Jon Stanford, Joe Doetzl, Jay Cribb, Jim Breton and Kevin Perry. The BES experts will be joining and working with the team as well. NERC produced a 2 page statement of work for the experts: they will help finish working paper and requirement statements; be available to respond to draft posting comments associated with pieces; and have no expectation of a need to travel.

There will be additional working papers developed for SDT review going forward including:

- BES Risk Management concept paper
- Security Control concept paper.

IV. NEXT STEPS

A. 2009 SDT Workplan Approach and Schedule

Bob Jones, SDT facilitator, noted the proposal to proceed with CIP 002's development in the remaining half of 2009 and refine it after a sequence of rounds of comments from the industry before going to the ballot.

Member Comments

- Regardless of what the controls are, nothing/no one will be able to tell us how to solve the CIP 002 challenge. This is clear in reviewing the five competing bills in congress.
- The SDT should stay as focused on CIP 002 related. Let the political winds blow wherever.
- Always will think about controls and some hierarchy. We should focus on the "what" in the short term.
- For the SDT December release- we should consider picking some security control to give as an example as to what it means in terms of high medium low on a password protection.
- We don't have too bad a set of controls- 003 -009 will serve us for a little while.
- Focus on CIP 002 only? A little bit of both.
- Flagging issues for the industry that need to be done.
- Highly desirable –the sooner we get the concept out to industry the more time they will have to read and digest.
- Decoupled approach, multiple levels of analysis- more time they have to get comfortable with concept, the better.
- Industry will provide us with comments.
- When the operating people got on the team. Reaction was surprising- they pointed out that this is really a paradigm shift from the operating standpoint.

The Chair reminded people that the SDT would try to establish the 2010 meeting schedule at the July SDT meeting in Vancouver, B.C. Canada. For the time being she noted that the August meeting will take place as scheduled in Chicago pending confirmation of available meeting space. SDT will be notified soon if we need to change locations.

B. Other Items

Dave Norton advised the group of a call for self-nominations closing on June 25 for a new SAR drafting team which would be defining next generation of situational awareness control tools for the BES. Going out to operations and planning only. This is fundamentally a systems

project - command and control, remote telemetry. Part of what they want to do is constrained by what actually can be done. He suggested this will be highly interrelated with the 706 SDT's efforts and they will need more cyber perspectives from people who know how to run high speed wide area networks. It will be related to the further development of the smart grid and the use of the internet. He believes presently there are mostly vendors and academics interested in serving as members. As all of these intersect at the BES there is a need to get involved, and provide some cyber visibility.

He also noted that a big document was released today on 291 smart grid interoperability.
http://www.nist.gov/smartgrid/InterimSmartGridRoadmapNISTRestructure.pdf
It has a big section on cyber security with lots of financial resources behind this effort. The report's introduction includes the following context:

> "In early 2009, responding to President Obama's energy-related national priorities, NIST acted to accelerate progress and promote stakeholder consensus on Smart Grid interoperability standards. On April 13, NIST announced a three-phase plan to expedite development of key standards.
> This document is input into the first phase: engaging utilities, equipment suppliers, consumers, standards developers and other stakeholders in a participatory public process to identify applicable Smart Grid interoperability standards, gaps in currently available standards and priorities for new standardization activities.
> NIST awarded the Electric Power Research Institute (EPRI) a contract to engage Smart Grid stakeholders and develop a draft interim standards roadmap; NIST will use this document as a starting point in developing a NIST interim "roadmap" for Smart Grid interoperability standards. EPRI technical experts compiled and distilled stakeholder inputs, including technical contributions made at two EPRI-facilitated, two-day, public workshops. Other inputs include the accomplishments of six domain expert working groups established by NIST in 2008, and the cyber security coordination task group established in 2009. To date, hundreds of people have participated in the road mapping process."

C. Closing

The Chair thanked Jon Stanford for hosting the meeting and noted that she and Kevin appreciated the spirited debate that was honest, painful, but did make some progress in particular refining and simplifying the flow chart. The SDT is now aware of the concept of paradigm shift and will continue to incorporate broad spectrum of background and experiences represented around the table. Once again she thanked the Drafting Group members for an outstanding job.
Members completed an onsite meeting evaluation form *(See, Appendix #3).*
The SDT adjourned at 3:00 p.m. on June 18.

Appendix # 1
Project 2008-06 Cyber Security Order 706 SDT
Draft Meeting Agenda
June 17, 2009 | 8:00 a.m. to 5:00 p.m. PDT
June 18, 2009 | 8:00 a.m. to 5:00 p.m. PDT
Bonneville Power Administration
905 NE 11th Ave
Portland, OR

Proposed Meeting Objectives/Outcomes

- Receive update on TFE and VSL/VRF processes
- Receive update on the SDT "Key Messages Task Group"
- Review and refine the CIP Version 3 Working Paper as a conceptual framework going forward in plenary and small groups;
- Agree on next steps in the Work plan and assignments.

Draft Agenda
Wednesday June 17, 2009

8:00 a.m. Welcome and Opening Remarks- Jeri Domingo-Brewer/Kevin Perry
a. Roll Call
b. NERC Antitrust Compliance Guidelines
c. Facilitator review of May 13-14 Boulder City meeting summary and adoption

8:20 a.m. Review of Meeting Objectives, Agenda and Meeting Guidelines - Jeri Domingo Brewer and Bob Jones

8:30 a.m. Update on Technical Feasibility Exception (TFE) NERC Rules of Procedure - Scott Mix
Update on VSLs/VRFs - Scott Mix

9:20 a.m. Overview of Steps to Date in the SDT CIP Version 3 (Phase 2) Development Process - Stu Langton

9:40 a.m. CIP Version 3 Categorizing Cyber Systems Working Paper - Big Picture Concepts Presentation - John Lim, Jackie Collett

10:45 a.m. Break

11:00 a.m. CIP Version 3 Working Paper Review and Discussion of Key Outstanding Issues - John Lim, Jackie Collett, et al

12:30 p.m. Working Lunch (Return to plenary meeting at 1:15)

1:15 p.m. CIP Version 3 Working Paper Review and Discussion of Key Outstanding Issues - John Lim, Jackie Collett, et al

	Test for SDT Consensus and Endorsement of Big Picture Concepts
2:45 p.m.	Consider Small Group Key Issue Breakouts
3:00 p.m.	Break
3:00 p.m.	Small Group Discussion of Key Outstanding Issues
5:00 p.m.	Recess

Thursday June 18, 2009

8:00 a.m.	Welcome and Agenda Review
8:10 a.m.	CIP Version 3 Small Group Reports – Plenary Session
10:00 a.m.	Break
10:15 a.m.	CIP Version 3 Small Group Reports – Plenary Session
12:00 p.m.	Working Lunch
12:45 p.m.	CIP Version 3 Working Paper(s) Refinements and Discussion - Small Group or Plenary
2:45 p.m.	Break
3:00 p.m.	Next Steps and SDT CIP Version 3 Process Working Paper(s) Assignments Initial discussion of CIP 002 Version 3 SDT Subgroup Structure in 2009 (Requirements, Measures, etc.) Consensus Testing of Development of CIP 002 Version 3 for Industry Comment and Ballot in early 2010 apart from Other CIP Standards Review of Next Steps and Work Plan
4:30 p.m.	Review July Meeting Objectives
4:45 p.m.	Meeting Evaluation - Review June Meeting Progress (What was accomplished? What helped? What can be improved going forward?)
5:00 p.m.	Adjourn

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Appendix # 2
Cyber Security for Order 706 Standard Drafting Team and Attendees List
May 13-14, 2009 Project 2008-06 — CS 706 SDT
Orlando, Florida

Attending in Person – SDT Members

1. Rob Antonishen	Ontario Power Generation *(Tuesday and Wednesday)*
2. Jeri Domingo-Brewer, Chair	**U.S. Bureau of Reclamation**
3. Jay S. Cribb	Information Security Analyst, Southern Company Services, Inc.
4. Joe Doetzl	Manager, Information Security, Kansas City Power & Light Co.
5. Scott Fixmer	Senior Security Analyst Exelon Corporate Security, Exelon Corp.
6. Gerald S. Freese	Director, Enterprise Information Security America Electric Power
7. Phillip Huff	Arkansas Electric Coop Corporation
8. John Lim	CISSP, Department Manager, Consolidated Edison Co. NY
9. Frank Kim	Ontario Hydro
Richard Kinas	Orlando Utilities Commission
10. David Norton	Policy Consultant, CIP Entergy Corporation
11. **Kevin B. Perry, Vice Ch.**	Director, Critical Infrastructure Protection, Southwest Power Pool
12. Christopher A. Peters	ICF International
13. David S. Revill	Georgia Transmission Corporation
14. Kevin Sherlin	Sacramento Municipal Utility District
15. Jonathan Stanford	Bonneville Power Administration
16.Keith Stouffer	National Institute of Standards & Technology
1. Roger Lampilla	*NERC*
2. Scott R. Mix	*NERC*
3. Joe Bucciero	*NERC/Bucciero Assoc.*
4. Robert Jones	*FSU/FCRC Consensus Center (Wed. & Thursday)*
5. Stuart Langton	*FSU/FCRC Consensus Center*

SDT Members Attending via Webex/Phone

17. Jim Breton	ERCOT
18. Jackie Collett	Manitoba Hydro
19. Scott Rosenberger	Luminant Energy

SDT Members Unable to Attend

1. Sharon Edwards	Duke Energy
2. John D. Varnell	Technology Director, Tenaska Power Services Co.
3.William Winters	Arizona Public Service, Inc.

Others Attending in Person

Darrell Hobbs	NU Energy
Chris Ewing	SEL
Curt Wilkins	BPA
Kim Long	Duke Energy
Forrest Gist	CH2MHill
Clark Goodlett	CH2MHill
Robert L. Windus	CH2MHill

Others Attending via Webex/Phone

James Bassett	Lafayette
Steve Dougherty	
Mike Fischette	
Travis Jaffrey	
Jason Marshall	Midwest ISO
Sam Merrell	CERT
Hoang No	
Mike Peters	FERC
Chris Wright	Burns & Mac

Appendix # 3 Meeting Evaluation Feedback

CYBER SECURITY ORDER 706 SDT
JUNE 17-18, 2009, PORTLAND, OR
MEETING EVALUATION FEEDBACK FOR INCLUSION IN FACILITATOR'S REPORT

Use the following 0 to 10 scale in evaluating the meeting: 0 means totally disagree and 10 means totally agree. A summary of the SDT responses will be placed in the Meeting Summary

1. Please assess the overall meeting.

7.5 The agenda packet was very useful.
8.0 The pre-meeting paper (Working Paper) was very useful.
8.5 The WebEx document display and the audio were effective
9.4 The quality of the meeting facility was good.
9.0 The objectives for the meeting were stated at the outset.
7.4 Overall, the objectives of the meeting were fully achieved.
Were each of the following meeting objectives fully achieved:
9.3 Receive update on TFE and VSL/VFR processes
N/A Receive update on the SDT "Key Messages Task Group"
7.4 Review, refine and adopt the CIP Version 3 Working Paper as a conceptual framework going forward in
plenary and small groups;
7.9 Agree on next steps in the Work plan and assignments.

2. Please tell us how well you believe the Team members and participants engaged in the meeting.

8.3 The Chair and Vice Chair provided leadership and direction to Team and Facilitators
8.8 The Facilitators made sure the concerns of all members were heard.
8.5 The Facilitators helped clarify and summarize issues.
8.0 The Facilitators helped members build consensus.
8.6 The Facilitators made sure the concerns of all participants were heard.
7.3 The Facilitators helped us arrange our time well.

3. What is your level of satisfaction with what was achieved at the meeting?

7.8 Overall, I am very satisfied with the results of the meeting.
8.3 Overall, the design of the meeting agenda was effective.
8.7 I was very satisfied with the services provided by the Facilitators.
8.0 I am satisfied with the outcome of the meeting.
7.3 I am satisfied with the progress we are making as a Team.
8.8 I know what the next steps following this meeting will be.
8.4 I know who is responsible for the next steps.

4. Other comments (use other side)

It's just painfully slow…So was building Rome…☺

What did we achieve?

- Significant breakthrough on working paper concept
- Synthesis of the BEX/Cyber process tracks
- We got the entire team on-board with the document. Progress was made, but was painful
- Refine flow-chart

What are our biggest challenges going forward?

- Team acceptance of revisions stemming from meeting
- Industry acceptance of new approach
- Getting something done before congress tells us what to do!
- Finalizing the concept paper
- Organizing the SDT to evolve the standards

What suggestions do you have for making our group more productive?

- Try to control chasing of rabbit trails
- Put end to repetitive arguments/discussions
- Don't know what…
- There should be a more cncerted effort to research existing work (such as the DHS Tier I/Tier II document) that may be beneficial to the progress of the group
- Organize for results
- Smaller groups
- Iterative development
- Organize by capabilities
  - Experience
  - Capability/expertise
  - BES function
  - Interest
- Too much open group dialogue – letting 25 people weigh-in on all issues is
- arduous/counter-productive.
- We need to come to each meeting ready to make decisions – Decide/Act

Appendix # 4
NERC Antitrust Compliance Guidelines

I. General

It is NERC's policy and practice to obey the antitrust laws and to avoid all conduct that unreasonably restrains competition. This policy requires the avoidance of any conduct that violates, or that might appear to violate, the antitrust laws. Among other things, the antitrust laws forbid any agreement between or among competitors regarding prices, availability of service, product design, terms of sale, division of markets, allocation of customers or any other activity that unreasonably restrains competition.

It is the responsibility of every NERC participant and employee who may in any way affect NERC's compliance with the antitrust laws to carry out this commitment.

Antitrust laws are complex and subject to court interpretation that can vary over time and from one court to another. The purpose of these guidelines is to alert NERC participants and employees to potential antitrust problems and to set forth policies to be followed with respect to activities that may involve antitrust considerations. In some instances, the NERC policy contained in these guidelines is stricter than the applicable antitrust laws. Any NERC participant or employee who is uncertain about the legal ramifications of a particular course of conduct or who has doubts or concerns about whether NERC's antitrust compliance policy is implicated in any situation should consult NERC's General Counsel immediately.

II. Prohibited Activities

Participants in NERC activities (including those of its committees and subgroups) should refrain from the following when acting in their capacity as participants in NERC activities (e.g., at NERC meetings, conference calls and in informal discussions):

- Discussions involving pricing information, especially margin (profit) and internal cost information and participants' expectations as to their future prices or internal costs.
- Discussions of a participant's marketing strategies.
- Discussions regarding how customers and geographical areas are to be divided among competitors.
- Discussions concerning the exclusion of competitors from markets.
- Discussions concerning boycotting or group refusals to deal with competitors, vendors or suppliers.

III. Activities That Are Permitted

From time to time decisions or actions of NERC (including those of its committees and

subgroups) may have a negative impact on particular entities and thus in that sense adversely impact competition. Decisions and actions by NERC (including its committees and subgroups) should only be undertaken for the purpose of promoting and maintaining the reliability and adequacy of the bulk power system. If you do not have a legitimate purpose consistent with this objective for discussing a matter, please refrain from discussing the matter during NERC meetings and in other NERC-related communications.

You should also ensure that NERC procedures, including those set forth in NERC's Certificate of Incorporation and Bylaws are followed in conducting NERC business. Other NERC procedures that may be applicable to a particular NERC activity include the following:

- Reliability Standards Process Manual
- Organization and Procedures Manual for the NERC Standing Committees
- System Operator Certification Program

In addition, all discussions in NERC meetings and other NERC-related communications should be within the scope of the mandate for or assignment to the particular NERC committee or subgroup, as well as within the scope of the published agenda for the meeting.

No decisions should be made nor any actions taken in NERC activities for the purpose of giving an industry participant or group of participants a competitive advantage over other participants. In particular, decisions with respect to setting, revising, or assessing compliance with NERC reliability standards should not be influenced by anti-competitive motivations.

Subject to the foregoing restrictions, participants in NERC activities may discuss:

- Reliability matters relating to the bulk power system, including operation and planning matters such as establishing or revising reliability standards, special operating procedures, operating transfer capabilities, and plans for new facilities.
- Matters relating to the impact of reliability standards for the bulk power system on electricity markets, and the impact of electricity market operations on the reliability of the bulk power system.
- Proposed filings or other communications with state or federal regulatory authorities or other governmental entities.
- Matters relating to the internal governance, management and operation of NERC, such as nominations for vacant committee positions, budgeting and assessments, and employment matters; and procedural matters such as planning and scheduling meetings.

Any other matters that do not clearly fall within these guidelines should be reviewed with NERC's General Counsel before being discussed.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Appendix # 5
CYBER SECURITY ORDER 706 SDT JANUARY- DECEMBER DRAFT PROJECT SCHEDULE *(REVISED MAY, 2009)*

CYBER SECURITY ORDER 706 SDT MEETING SCHEDULE

OCTOBER 2008-DECEMBER, 2010

DEVELOPMENT OF CIP FRAMEWORK OCTOBER 2008-JULY, 2009

1. October 6-7, 2008, NIST, Gaithersburg, MD, Review of CIP 002-009, Agreement on Phase 1/Version 2 approach
2. October 20-21, Sacramento, CA, Phase 1/Version 2 Development
3. November 12-14, 2008, Little Rock, Phase 1/Version 2 Adoption; Phase 2/Version 3 Process review
4. December 4-5, 2008, Washington D.C., Phase 2/Version 3 review and debate, white papers assigned.
5. January 7-9 SDT Meeting, Phoenix, AZ ½ / 1/½ day format. Wed-Friday

- Review of Technical Feasibility Exceptions white paper
- Review of Industry Comments on Phase 1 products- Establish and convene small groups to draft responses
- Review of Phase 2 White papers

January 15 Webex meeting(s)

- Small group draft responses to industry.

January 21 Webex meeting(s)

- Small group draft responses to industry.

6. February 2-4 SDT Meeting, 2009, Phoenix, AZ, ½ / 1/½ day format. Mon-Wed.

- Update on NERC Technical Feasibility Exceptions process
- Review of VSL process and SDT role
- Review of Phase 2 White papers, strawman and principles
- Review and Adoption of SDT Responses to Industry Comments on Phase 1 and Phase 1 Product Revisions.

7. February 18-19, SDT Meeting, Fairfax, VA

- Update on Phase 1 process
- Update on NERC TFE process
- Update on VSL Team process
- Review, discussion and refinement of Phase 2/CIP 002 White papers, strawman and principles

8. March 10-11, SDT Meeting 2009, Orlando, FL, ½ /1/1 day format

- Update on NERC TFE process
- Update on VSL Team process
- Review and Refinement of Phase 2 CIP 002 Strawman Proposals

March 2- April 1 30-day Pre Ballot
Mid-March- NERC posts TFE draft Rules of Procedure for industry comment

March 30, WebEx meeting(s) White Paper Drafting Team
April 1-10, NERC Balloting on Phase 1 Products
April 6, WebEx meeting- White Paper Drafting Team
April 8, WebEx meeting(s) - White Paper Preview- Full SDT Conference Call
*April 11, 2009 Phase 1 Ballot Results (*Quorum: 91.90% Approval: 84.06%) *and Industry Comments-*

9. April 14-16, SDT Meeting, Charlotte NC, ½ / 1/½ day format. Wed-Friday

- Update on NERC TFE process
- Update on VSL Team process
- Update on the NERC Critical Assets Survey
- Agree and Adopt Responses for Phase 1 Industry Comments- Recirculation Ballot
- Review and Refinement of Phase 2 Whitepaper and Progress Report to MRC

April 28 and May 6 White Paper Drafting Team Meetings/Webex
April 17-27 Recirculation Results: Quorum: 94.37% Approval: 88.32%
May 5, 2009, NERC Member Representative Committee Meeting, Arlington, VA- SDT progress report.

10. May 13-14, Wed.-Thursday, SDT Meeting, Boulder City NV, 2-day format

- Review MRC presentation and any input to SDT on Phase 2 approach
- Further SDT refinement and discussion of the Phase 2 White Paper.

June, Working Paper Drafting Team Meetings/WebEx, June 8 & June 15, 2008

11. June 17-18, SDT Meeting, Portland OR, 2-day format

- Further SDT refinement of the Draft CIP Version 3 Working Paper(s).
- Review SDT development process for June-December 2009
- Discuss potential SDT subcommittee structure and deliverables.

June, WebEx meeting(s)

- Working Paper Sessions including inputs from selected industry personnel to help establish BES Categorization Criteria
- Agree on and charge SDT subcommittees

12. July 13-14, 2009 Vancouver, B.C., Canada

- SDT Plenary session to review and respond to any input/comments on Working Paper
- Adopt Version 3 CIP Working Paper for industry review
- Confirm SDT Subcommittees and Deliverables
- Conduct subcommittee organizational meetings
- SDT Subcommittees meet to begin drafting assigned issues and deliverables
- Subcommittee organizational and deliverable reports to SDT

July, WebEx meeting(s)

- Working Paper Sessions including inputs from selected industry personnel to help finalize BES Categorization Criteria
- SDT Subcommittee meetings (as needed)

CIP 002 DEVELOPMENT OF REQUIREMENTS, MEASURES, ETC. AUG.-DEC 2009

13. August 20-21, 2009, Chicago IL

- SDT Plenary session to review and respond to any industry input/comments on Working Paper
- SDT Plenary and Drafting Subgroup meetings to develop and test support for deliverable CIP 002 provisions

*August, 2009, **NERC Member Representative Committee***
Progress Report and presentation on new CIP Version 3 Working Paper-Concept-Reliability Standards on Cyber Security for MRC input, Winnipeg, Manitoba

August, WebEx meeting(s)

- SDT Subgroup meetings (as needed)

14. September 9-10, 2009 Folsom, CA

- SDT Plenary session to review and respond to any additional industry input/comments on Working Paper
- SDT Plenary session to review MRC input on approach to Version 3 CIP Reliability Standards on Cyber Security and consider and agree on refinements

- SDT Subgroup drafting meetings- prepare deliverables
- SDT Plenary Session(s)- provide briefings and Subgroup reports
- Review Work Plan through Summer, 2010, as needed
- Establish SDT Meeting Dates and Locations for Jan-December 2010

September, WebEx meeting

- SDT Subcommittee drafting meetings

15. October 20-22, New Orleans LA

- SDT Subgroup drafting meetings
- SDT Plenary Session(s) - Subgroup reports on CIP 002 deliverables
- SDT Subcommittee drafting meetings
- Review, Revise and Adopt Work Plan through Summer, 2010, as needed
- Confirm Meeting Dates and Locations for Jan-December 2010

October, WebEx meeting

- SDT Subcommittee drafting meetings

16. November 17-18, Atlanta GA

- SDT Plenary Session(s) – to review and refine CIP 002 deliverables from SDT Subcommittees
- SDT Subcommittee drafting meetings to refine products based on SDT input

November, WebEx meeting

- SDT Subcommittee drafting meetings to finalize drafts

17. December 15-17, Tampa

- SDT Plenary Session(s) to review, refine, and agree on and adopt CIP 002 deliverables of new Categorizing BES and Cyber Systems Standard
- Agree on initial Posting of draft CIP 002 for industry review and comment

December, WebEx meeting

- SDT Subgroup meetings

DEVELOPMENT OF OTHER CIP STANDARDS- JAN.-DEC 2010

SDT Meetings 18-30. 2010 *(12 SDT monthly meetings and subgroup webex meetings as needed)*

- SDT Responds to Industry Comments on Initial and Subsequent Postings of CIP 002, Version 3 *(may be multiple comment periods, as required)*
- Refine the CIP 002 and submit new CIP 002 Version 3 Standard for Balloting while permitting industry to rely on CIP 003-009 until the full suite is reviewed and presented for balloting.
- Initiate Development of the full suite of CIP Reliability Standards on Cyber Security including Requirements, Measures, Controls, etc.
- Submit the full suite of CIP Reliability Standards on Cyber Security for Industry Comment
- Refine and Submit the full suite of CIP Standards for Industry Ballot
- NERC Board of Trustees Adoption of the full suite of Standards
- FERC Approves and NERC Implements the full suite of CIP Standards

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Appendix # 6 Phase II Working Paper

http://www.nerc.com/filez/standards/Project_2008-06_Cyber_Security-RF.html

Categorizing Cyber Systems

An Approach Based on BES Reliability Functions

NERC Cyber Security Standards Drafting Team for Order 706
06/15/2009 –Team

This draft Categorizing Cyber Systems paper is a “Work in Progress” that is meant to convey the initial thoughts and ideas that should be addressed and considered by the full CSO706 SDT as part of the deliberations related to the revised CIP Reliability Standards addressing Cyber Security. This is a Working Concept Paper, and is subject to change as these initial concepts are addressed and discussed by the SDT.

TABLE OF CONTENTS

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Meeting Agenda

Cyber Security Order 706 SDT — Project 2008-06

June 17, 2009 | 8 a.m. – 5p.m. PDT
June 18, 2009 | 8 a.m. – 5p.m. PDT

Proposed Meeting Objectives — Outcomes

- Receive update on TFE and VSL/VRF processes
- Receive update on the SDT "Key Messages Task Group"
- Review and refine the CIP Version 3 Working Paper as a conceptual framework going forward in plenary and small groups
- Agree on next steps in the Work plan and assignments

Wednesday, June 17, 2009

Welcome and Opening Remarks — Jeri Domingo Brewer — Kevin Perry

a. Roll Call
b. NERC Antitrust Compliance Guidelines
c. Facilitator review of May 13–14 Boulder City meeting summary and adoption

Review of Meeting Objectives, Agenda and Meeting Guidelines — Jeri Domingo Brewer and Bob Jones

- Update on Technical Feasibility Exception (TFE) NERC Rules of Procedure — Scott Mix
- Update on VSLs/VRFs — Scott Mix
- Update on the "Key Messages" Task Group — Gerry Freese
- Overview of Steps to Date in the SDT CIP Version 3 (Phase 2) Development Process — Stu Langton
- CIP Version 3 Categorizing Cyber Systems Working Paper – Big Picture Concepts Presentation — John Lim and Jackie Collett

Break

- CIP Version 3 Working Paper Review and Discussion of Key Outstanding Issues — John Lim, Jackie Collett, et al

Working Lunch (Return to plenary meeting at 1:15 p.m.)

116-390 Village Blvd.
Princeton, NJ 08540
609.452.8060 | www.nerc.com

- CIP Version 3 Working Paper Review and Discussion of Key Outstanding Issues – John Lim, Jackie Collett, et al
- Test for SDT Consensus and Endorsement of Big Picture Concepts
- Consider Small Group Key Issue Breakouts

Break

- Small Group Discussion of Key Outstanding Issues

Recess

Thursday, June 18, 2009

Welcome and Agenda Review

- CIP Version 3 Small Group Reports — Plenary Session

Break

- CIP Version 3 Small Group Reports — Plenary Session
- Working Lunch
- CIP Version 3 Working Paper(s) Refinements and Discussion — Small Group or Plenary

Break
Next Steps and SDT CIP Version 3 Process

- Working Paper(s) Assignments
- Initial discussion of CIP 002 Version 3 SDT Subgroup Structure in 2009 (Requirements, Measures, etc.)
- Consensus Testing of Development of CIP 002 Version 3 for Industry Comment and Ballot in early 2010 apart from Other CIP Standards
- Review of Next Steps and Work Plan
  Review July Meeting Objectives
  Meeting Evaluation — Review June Meeting Progress (What was accomplished? What helped? What can be improved going forward?)

Adjourn

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Meeting Summary
Cyber Security Order 706 SDT — Project 2008-06

July 13, 2009 | 8 a.m.–5 p.m. PST
July 14, 2009 | 8 a.m.–5 p.m. PST
Vancouver, British Columbia, Canada

Robert Jones, Stuart Langton, and Hal Beardall
Facilitation and Meeting Design
FCRC Consensus Center, Florida State University

Joe Bucciero, Bucciero Consulting, LLC

http://www.nerc.com/filez/standards/Project_2008-06_Cyber_Security.html

Adopted by SDT 706, August 21, 2009

116-390 Village Blvd.
Princeton, NJ 08540
609.452.8060 | www.nerc.com

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Meeting Summary Contents

EXECUTIVE SUMMARY

The Chair, Jeri Domingo-Brewer and Vice Chair Kevin Perry welcomed the members. Joe Bucciero conducted a roll call of members and participants in the room and on the conference call for each day. The Chair reviewed the meeting objectives and Bob Jones, facilitator, reviewed with the team and participants the proposed meeting agenda.

Mr. Bucciero reviewed the need to comply with NERC's Antitrust Guidelines. He urged the team and other participants in the process to carefully review the guidelines as they cover all participants and observers.

Kevin Perry made the presentation the Technical Feasibility Exception (TFE) and the NERC Rules of Procedure posting and Gerry Adamski, NERC's Director of Standards offered additional information on behalf of Scott Mix who was not able to attend the meeting. Kevin noted several areas that are under review and Mike Assante was leading a "tiger team" with regional entity representatives to address a number of issues that have been raised in the industry comments received to date. Gerry Adamski noted the plan to submit to NERC Board of Trustees for review and adoption at the upcoming August meeting has been delayed until the next BOT meeting in the Fall given the open issues and the need to clarify the implications and questions for NERC's implementation including how to capture the process in the 2010 plan and budget. NERC hopes to produce a final TFE process sometime next year before FERC. The members discussed the range of questions and issues that had been raised by the industry and both the interim and final TFE.

David Taylor provided an update report to the SDT on VSLs and VRFs noting that he does not expect that the SDT will need to address or deal with this going forward as the assigned SDT is handling the process. The SDT discussed the Smart Grid effort that is being led by NIST. Keith Stouffer reported that the effort is addressing system level requirements from the top down and component level details from the bottom up. They are working with 800-53 NIST and ISA 99 work and are keenly aware of the work of the SDT. He also referenced the work now on ISA 99 — Part 4 — detailed cyber security for industrial control systems. These requirements will be harmonized with other activities.

NERC requested that the SDT review its CIP-006-1 Interpretation. The CIP Standards Interpretation Team met the first day over lunch to reconsider the interpretation of CIP-006-1 requested by SCE&G regarding the need to physically protect Critical Cyber Assets that are dial-up accessible but do not use a routable protocol. The interpretation was previously approved by the industry but not yet submitted to the FERC for approval. The interpretation asserted that the exclusion of such Critical Cyber Assets is a correct interpretation of the standard. The team examined CIP-002-1, CIP-005-1, and CIP-006-1, along with the FAQ for the Version 1 CIP standards and determined that the exclusion might not have been written had the standards been developed with present day knowledge, the interpretation team agreed and the SDT concurred that the interpretation approved by the ballot body and the NERC Board of Trustees is a correct interpretation of CIP-006-1, Requirement R1.1.

Stu Langton reviewed the milestones in Version 2 and Version 3 of the SDT work and the SDT convergence on a single consensus approach in Orlando that was refined further in Charlotte, Boulder City and Portland with John Lim and Phil Huff leading an expanded drafting team to continue to refine the paper between meetings. Joe Bucciero, with the SDT facilitation team, reported that following the Portland meeting the SDT has been supplemented with additional members and BES expertise and has produced its proposed concept paper for the SDT's review and adoption.

On behalf of the SDT, the Chair thanked John Lim, Phil Huff and the other members of the drafting team for working productively since the Portland SDT meeting and bringing to Vancouver a proposed concept paper that can be adopted by the SDT for sharing with the industry as the basis for the SDT's efforts in developing the Version 3 standards. John Lim presented the working paper noting the significant changes and improvements that emerged from the Portland SDT meeting. The SDT discussed the paper, agreed to some minor wording changes and agreed that the paper would be archived. The SDT agreed that industry comments should be focused on the development of CIP-002 requirements in the key areas set forth in the concept paper. Following the discussion the SDT unanimously adopted the concept paper as revised for sharing with the industry and agreed to develop a draft cover letter and comment form for posting with the paper. The team discussed a "game plan" for communications with the industry on the working concept paper and agreed to post the paper, brief the Members Representative Committee and present a Webinar in August and provide an update on progress at the NERC October workshop in Dallas, Texas.

The Chair reviewed the July-December 2009 work plan proposal circulated in advance noting that all members of the SDT would participate in at least one of five proposed subgroups drawn from the concept paper, (i.e. Reliability Functions; List of BES Subsystems and/or BES Cyber Systems; BES Mapping; Cyber Analysis; and Definition and Selection of Controls. Member noted their preferences and the Chair and Vice Chair made assignments guided by those preferences. Each subgroup was charged to draft requirements for consideration by the SDT to be included in a draft CIP-002 Version 3 to be shared with the industry in December 2009.

On the afternoon of the first day and the morning of the second day the five subgroups met in parallel conducting organizational sessions to: review scope of the assigned topic; identify areas that may need development of related CIP-002 requirements; determine what information they will need going forward; select a leader/spokesperson, a scribe and a timekeeper; sketch out a work plan, including a meeting schedule in order to get the work done by the October SDT meeting. Finally the subgroups were asked to draft questions for their topic for use in the concept paper comment form.

The SDT discussed the roles that would be played by the members, subgroup members, subgroup leaders, and a coordinating team and staff. On the second day the SDT agreed that it would be helpful to develop a set of consistent coordination guidelines for the subgroups.

The Chair reviewed the schedule for getting the concept paper, announcement and comment form finalized and posted on the NERC website for industry comment. She expressed the hope that this could be accomplished for NERC posting by the week of July 20. The Chair thanked the members for their hard work together and in the subgroups and commended them on the adoption of the concept paper and the development of the announcement and comment form. The SDT adjourned at 3:00 p.m. on July 14.

I. Introductions, Agenda, and SDT Work plan Review

The Chair, Jeri Domingo-Brewer and Vice Chair, Kevin Perry welcomed the members and Joe Bucciero conducted a roll call of members and participants in the room and on the conference call *(See appendix #2*). The Chair reviewed the meeting objectives and Bob Jones, facilitator, reviewed the proposed meeting agenda *(See appendix #1*). The SDT adopted the May 13–14 and June 17–18 meeting summary without comment or objection.

Mr. Bucciero reviewed the need to comply with NERC's Antitrust Guidelines *(See Appendix #3).* He urged the team and other participants in the process to carefully review the guidelines as they would cover all participants and observers. He urged all to avoid behaviors or appearance that would be anti-competitive nature and also reminded the group of the sensitive nature of the information under discussion.

II. UPDATES

A. Technical Feasibility Exception (TFE) NERC Rules of Procedure Posting

Kevin Perry made the presentation and Gerry Adamski, NERC Vice President and Director of Standards, offered additional information on behalf of Scott Mix who was not able to attend the meeting. Mr. Perry noted several areas that are under review by NERC. Mike Assante, NERC Chief Security Officer, is leading a "tiger team" with regional entity representatives to address a number of issues that have been raised in the industry comments received to date. Gerry Adamski noted that the plan to submit to NERC Board of Trustees for review and adoption at the upcoming August meeting has been delayed until the next BOT meeting in the Fall in light of the open issues and the need to clarify the implications and questions for NERC's implementation. Following its consultation with the regional entity representatives, NERC BOT hopes to adopt a final TFE process sometime next year to submit to FERC.

SDT Comments on TFEs

- Lots of questions have been raised but not yet answered.
- What are the advantages and disadvantages to NERC centrally processing all TFEs or RE's processing?
- Will TFE requests to Regional Entity be evaluated/approved or rejected in the context of CIP audits or spot check?
- Is it resolved as to whether the interim process limits TFEs to the 9 requirements? No. Proposed changes to NERC ROP (footnote 1).
- May add more requirements to list — e.g. CIP-004 R3 — personnel risk assessment.
- What role will statutory law play with the TFE? Bargaining unit agreements?
- CIP-007 R2.3 — Ports and services — document compensating measures. TFR
- CIP-007 R3.2 — Monitoring and alerts. Document compensating measures
- Submit TFE by secured means? 30 days before audit or spot check. Should they do it at point of compliance? We don't currently have a secure means yet for submission. A submittal form is under review by NERC.

- Concerns have been expressed that entities will be reluctant to submit the information on the submittal form
- TFE — remedy shortcomings and get approved if TFE rejected. Within 30 days- respond and get TFE.
- Does the violation period start when TFE rejected? NERC's intent is that the violation period begins with effective date of rejection notice but that didn't make it into the bulletin.
- There are also no penalties for frivolous filings in the current draft.
- In the proposal and interim bulletin, it doesn't cite reasons why entity could request a TFE e.g. operational, safety concerns, and conflicts with other standards.
- Is there a concern about opening up to all reliability requirements? Limit to CIP standards?
- CIP spot checks currently work with 13 requirements, none of which provide for TFE requests.
- Are pieces of TFEs covered for CIP-007? Don't have to file for that? It says "it will be documented" no TFE there now.
- The "Tiger Team" will be discussing the meaning of "where technically feasible" compliant if the entity demonstrates can't comply for technical reasons. Will there be a subset of requirements for which TFE can be received? Or will it be more open to real technical infeasibility? Lawyers are proposing tight control of the TFE.
- Some Canadian jurisdictions have issues regarding the TFE reporting through regional entities and/or NERC (e.g. Ontario). Is NERC looking to regional entities to sort through issues? If entity unsure can they work with REs vs. NERC? Should entity approach and work through RE or go through NERC directly?
- REs have presented a proposal which addresses the subject of Canadian entities. Is there an issue with submitting to NERC vs. RE? NERC expected all data on site in context with audit. Logistically and practically this won't work.
- In Ontario different frameworks been proposed about who should or not report to RE? E.g. IESO contracts. In a July 1 letter, certain entities should respond directly to the regional entity which is not currently the case. Hydro One is unclear about this. They are NERC registered entities.
- Joint regional proposal — NERC should evaluate "class type TFEs" and identify acceptable outcomes and provide for these. E.g. standards don't accommodate — field devices, anti virus etc. If we know classes of devices, we should identify acceptable alternatives to meet reliability.
- We must distinguish between interim process and long-term process.
- There is industry concern about different answers for same equipment within and across regions. The industry needs consistent methodology across all NERC regions.
- Regions are aware of this concern. They suggest the RC ask the entity to identify if other regions are being asked to address the TFE. These need the same response.
- Is our focus on interim procedures? Shouldn't we keep our eye on the longer term? Interim may look a lot like the final procedure. This will not be wasted work.

B. VSLs and VRFs

David Taylor provided an update report to the SDT on VSLs and VRFs. He noted that the SDT is making progress having developed comment forms with posting for pre-ballot review in early August. He noted that he does not expect that the SDT will need to address or deal with this going forward.

C. Update on other Related Cyber Security Initiatives

The SDT discussed the Smart Grid effort that is being led by NIST. Keith Stouffer reported on the effort led by Annabelle Lee at NIST that is addressing system level requirements from the top down and component level details from the bottom up. They are working with 800-53 NIST and ISA 99 work and are keenly aware of the work of the SDT. They have weekly telephone conferences which some members of the SDT participate and are following.

He also referenced the work now on ISA 99- Part 4 — detailed cyber security for industrial control systems. These requirements will be harmonized with other activities. They are developing their own requirements document.

Currently the categorization approach under review contains four levels of response at a system level. Next they will be developing detailed component level requirements. A proposed security compliance institute might set forth requirements which vendors can build products consistent with and have their products certified by the institute. He noted that at the upcoming ISA Expo in fall, 2009 the requirements document is scheduled to be presented for review.

Member Comments

- Is there any consideration to coordinating and synchronizing schedules and linkages among these efforts? What is the perception of the pace of the SDT's work? The perception is the SDT is not as slow as other groups.
- The Smart Grid effort is politically charged with a short time frame. Some believe the speed they are moving at will not result in effective and acceptable products.
- NIST cyber security documents are defining requirements. But what and who are the requirements to be applied to? Are they being written for those applying for DOE RFPs/grants from the $4.5 billion allocated for the smart grid? Are they also intended for those responsible with the electric grid?
- The system level requirements would apply across the whole grid — detailed cyber security requirements for different aspects of the grid. They are looking at what requirements are in the standards.
- Are there any NERC security initiatives that connect with the SDT efforts? Mike Assante will keep the SDT apprised of this.
- Nuclear initiatives? NERC alerting. Hydra — any thing needed to be known? Potential in future with hydra — BOT approved process in 2008. All procedural aspects being balloted going forward. Expedited standards development process.
- Order 706 B-Nuclear plants — how to carry forward initiatives? Development of an MOU with NRC and NERC is being developed. Development of exemption process for nuclear plants is under consideration as well as alternatives to NERC CIP umbrella under the NRC

jurisdictions. The implementation schedule for when nuclear plants held to standards is the subject of a conference call tomorrow with FERC, NERC and NRC. NERC must file by September 15, 2009, under a FERC order. NEI taken an active role on behalf of members.

- How will the process play out in terms of auditing? NERC, Regions, and NRC taking over? Permit to take more active role over auditing even though jurisdiction within NERC is still under consideration.
- NRC may a conduct audit with compliance proceeding turned over the RE.
- Looks like timeframe for proposal will dovetail with CIP Version 2 efforts. Will be handled through FERC approval of Version 2. Plants looking at Version 2 in compliance.

III. CIP-006-1 Interpretation

NERC requested that the CIP review its CIP-006-1 Interpretation. The CIP Standards Interpretation Team met the first day over lunch to reconsider the interpretation of CIP-006-1 requested by SCE&G regarding the need to physically protect Critical Cyber Assets that are dial-up accessible but do not use a routable protocol. The interpretation was previously approved by the industry but not yet submitted to the FERC for approval. The interpretation asserted that the exclusion of such Critical Cyber Assets is a correct interpretation of the standard. The FERC has questioned whether the interpretation is valid, believing that the original interpretation evaluated the Additional Compliance Information as opposed to the requirement.

The team examined CIP-002-1, CIP-005-1, and CIP-006-1, along with the FAQ for the Version 1 CIP standards and determined the following:

- CIP-006-1 contains Additional Compliance Information that was referenced in the interpretation, specifically.
- D-1.4.4 — for dial-up accessible Critical Cyber Assets that use non-routable protocols, the Responsible Entity shall not be required to comply with Standard CIP-006 for that single access point at the dial-up device. This additional compliance information is supported by language in the CIP-002-1 and CIP-005-1 standards and the Version 1 FAQ that clearly document the intent of the original standards drafting team.
- Put simply, the Critical Cyber Asset that does not utilize a routable protocol and is “dial-up” accessible does not have to be within an Electronic Security Perimeter per CIP-005-1, Requirement R1.2. As the CCA is not within an ESP, it is not included in protection requirement of CIP-006-1, Requirement R1.1.

While the exclusion might not have been written had the standards been developed with present day knowledge, the interpretation team agreed and the SDT concurred that the interpretation approved by the ballot body and the NERC Board of Trustees is a correct interpretation of CIP-006-1, Requirement R1.1 when viewed in the context of the complete set of Version 1 (and 2) CIP Cyber Security Standards. Any shortcomings of the requirements themselves must be remedied through standards development action.

IV. SDT Phase II — Version 3 Development Process — the “Working Paper”

A. Overview of Phase II — Version 3 Work Plan

Stu Langton reviewed the milestones in Version 2 and Version 3 of the SDT work including the work in Little Rock that framed the challenges, the subsequent development of the SDT "white papers" following the Washington D.C. meeting in December 2008 and further review and refinement of those and other papers. *(See Appendix # 5)* This resulted in the SDT convergence on a single consensus approach in Orlando that was refined further in Charlotte, Boulder City and Portland with John Lim and Phil Huff leading an expanded drafting team to continue to refine the paper between meetings. The working paper provided a basis for developing and testing the following consensus points in April that were subsequently offered to the NERC industry Members Representative Committee in May 2009. These included:

1. The standards should require a BES impact assessment as an initial approach to categorizing BES Cyber Systems.
2. The impact categorization of Cyber Systems will be based on reliability functions of the BES to achieve Adequate Levels of Reliability.
3. The standard's BES Impact Assessment will consider a categorization process.
4. The standards will require oversight of the categorized list of BES assets by entity types which have a more complete wide-area view of the BES.
5. The standards will categorize Cyber Systems supporting, either directly or indirectly, the reliability functions of the BES and apply security requirements (or controls) that are commensurate and appropriate to their potential impact on the BES.
6. The final Cyber System categorization will reflect the impact to the BES based on a loss of availability, integrity, or confidentiality of the Cyber System.
7. The standards will provide Organizations with reasonable flexibility in applying equivalent security controls on the basis of compensating controls and environmental considerations.
8. The standards will address the complex nature of BES functions and interconnected Cyber Systems, both within and between multiple organizations.
9. The standards will state explicit criteria for the BES Impact Assessment.
10. The standards will state explicit criteria for the Cyber Impact Assessment (including use and misuse of cyber systems).
11. The standards will include a methodology to merge the BES Impact Assessment and Cyber Impact Assessment into a final Cyber System categorization.

Joe Bucciero, with the SDT facilitation team, reported that following the Portland meeting the SDT has been supplemented with additional members and BES expertise and has produced its proposed paper for the SDT's review and adoption.

B. Phase II Concept Paper Overview Presentation and SDT Adoption of the Concept Paper

On behalf of the SDT, the Chair thanked John Lim, Phil Huff and the other members of the drafting team for working productively since the Portland meeting and bringing a proposed concept paper that can be adopted by the SDT to share with the industry as the basis for the SDT's efforts in developing the Version 3 CIP-002 standards. John Lim presented the working

paper noting the significant changes that emerged from the Portland SDT meeting (*See Appendix #9).* He noted the expanded team met twice by phone and WebEx following the Portland meeting. Following the presentation, the Chair thanked the team members and others who produced an outstanding product. A motion was made by John Lim, and seconded by Phil Huff, to adopt the paper by the SDT to post for industry comment. The following member comments were offered in the discussion of the motion.

Member Comments on the Motion to Adopt the Concept Paper

- Do generation assets = networking equipment? DCS control system — switches can be critical assets. Cyber or BES consideration? Cyber consideration — more detail than the paper addresses at the conceptual level.
- Network issues = supporting SCADA communications? More detail vs. conceptual, however look at the "Target of protection" illustrations.
- Pp 12 BES subsystem e.g. Load balancing function: Plant control room- change from "center"? Guideline — control center vs. room. This was intended to reflect the same campus environment, 1 facility multiple rooms. Guidelines as a "room"(s).
- SDT agreed to change control centers to "room(s).
- Contingency reserve section. Any units company has 150 mw? This is done by hardware — shared groups multiple owners of same equipment.
- What level trying to drive at? 150 mw? Not looking at individual units. 10 150 mw in a plant.
- How can we head off and deal with the industry "CIP-002-009 mentality?" Will there be a mountain of documentation for every digital asset? Every digital asset in BES and everything it talks to as well? Everything will now be at least a "low."
- How will we handle industry comments back on the concept? Is the SDT bound to all aspects of the concept paper? The SDT should consider the concept paper as complete and out for industry comment. The input on the concept paper will help the SDT as it develops CIP-002-009 standards and requirements going forward.
- The SDT should consider the lessons learned in the CIPC guidelines approach. The comment form was structured to ask the industry to comment on particular issues. This approach could directly facilitate efforts for the SDT to use the input as the process goes forward
- The SDT should work today and tomorrow to develop a clear and structured comment form for the concept paper.
- Important to convey that this is a "big picture concept approach" signaling the direction of changes from previous versions in terms of approach (vs. Version 1 and 2). The cover letter/announcement will be crucial in setting the stage.
- Make sure the concept paper has Reference line numbers and invites suggestion.
- Will there be an opportunity for industry to say maybe this is too much? Yes.
- Concerns with the idea that this paper will never see a character changed in it is overblown. These tend to become reference archived documents. We should clarify to the industry that the SDT will not mount concerted effort to respond to every comment and seek to adjust the

concept paper accordingly. But as we develop the requirements and address industry concerns, we can update the concept paper as appropriate.

- We have to do a selling job on both concept paper and standards themselves. We need to convince the industry that this is the right approach. While this may look to the industry to be onerous, in reality it will be easier, more consistent, easier to comply with standards over the longer term. The industry will build upon, not lose the work they have put into the CIP to date.
- We need to consider as we write requirements how the entity can demonstrate compliance with the requirement. Today it is an exercise with mountains of paperwork. We should try to address this as we go forward.
- Concept Paper will be archived as a background document. Address comments by incorporating responses in the first draft of CIP-002 requirements.
- The concept paper has provided a visual representation of our ideas. Agree that industry is wary of documents.
- Jackie Collett offered to take a look at the concept paper with the "Queen's" English in mind. The chair accepted the offer.
- The SDT needs to let industry know we are making progress. We should be prepared to present at the NERC October 14–15 Dallas workshop this approach as a "paradigm shift" in cyber security.

Following the discussion the SDT unanimously adopted the concept paper as revised for sharing with the industry and agreed to develop a draft of a comment form for the paper.

The team discussed a "game plan" for communications with the Industry on the working concept paper and agreed to the following steps:

1. Post in July the Working Concept Paper for Comment and Suggestions (with a cover and comment form with key questions to be developed on July 14 by the subgroups and the SDT);
2. Presentation of the concept paper to MRC on August 4, 2009;
3. Webinar(s) to the Industry in August 2009; and
4. Presentation of the industry comment and SDT progress at NERC Workshop on Compliance and Cyber Security (October 14–15, 2009)

V. Development of Concept Paper, Draft Announcement, and Comment Form

On the second day the SDT agreed to develop a draft announcement and comment form. Each of the 5 subgroups was asked to draft questions for the industry to respond to in each of their areas. The SDT believed this would help to solicit industry comments that the sub-groups could use in developing draft requirements. The Chair, with assistance of staff drafted an announcement and cover letter for the paper which was reviewed, refined, and adopted by the SDT. (*See Appendix #11*) The subgroups presented their draft questions to the SDT which offered suggestions. The subgroups then redrafted their questions and the SDT adopted the following for use in the comment form to be posted with the concept paper:

Reliability Functions

1. Is the concept of the categorizing by function instead of by asset clear? If not why?
2. The BES Reliability Functions listed in the "BES Function" column of the table were not meant to be comprehensive. Are there any others functions we need to address and why?

BES Subsystems and BES Cyber Systems

1. Does the methodology presented in the Identification of BES Subsystems and the Identification of BES Cyber Systems sections capture all of the systems that will need to be protected to achieve an acceptable level of reliability? What other issues need to be considered?

BES Mapping

1. The concept paper proposes that all identified BES subsystems are mapped into categories based on pre-defined criteria which reflect their impact on the reliability and operability of the BES: this mapping will be based on pre-defined criteria in the functions they provide or support, which determine the level of that impact. Do you agree with this approach and if not, what alternative suggestions do you have?
2. The paper gave an example of High, Medium and Low impact levels. What do you believe is the appropriate number of levels for impact mapping of the BES subsystems?
3. Do you prefer discrete thresholds or performance based criteria for mapping BES sub-systems? E.g. MW values as opposed to percentage of total generation. Please explain.

Cyber Analysis

1. Section X.X, Categorization of Cyber Systems, describes how an entity determines the impact a specific Cyber System has on to its assigned BES reliability functions. Do you agree with this process described in the concept paper? Please explain.
2. Section X.X, Final Categorization of Cyber Systems Based on Overall Impact on the BES, describes an example process of how an entity combines the BES impact mapping and Cyber System impact analysis to determine the overall impact a Cyber System has on the BES. Do you agree with this process described in the concept paper? Please explain.
3. Section X.X, Defining the Target of Protection, describes how an entity determines the set of Cyber Assets necessary to provide security assurance in the BES functions the Cyber System performs. Do you agree with this process described in the concept paper? Please explain.

Definition and Selection of Controls

1. Provide your company's thoughts on applying different levels of protection (i.e. security controls) based on characteristics and impact categories of specific BES cyber systems (e.g. transmissions substations, generating plants, control centers) as discussed in Section XX of the concept paper.
2. Section XX of the paper introduces the concept of a library of security controls:
    a. What sources would you recommend the drafting team consider when developing a library of security controls for protecting categorized BES cyber systems?

b. What specific challenges would you anticipate in implementing controls from among a library of security controls?

The SDT agreed that the Chair will oversee the final agreed upon edits to the adopted concept paper, announcement, and comment forms. She indicated she would circulate it to the members for one last look later in the week and then work with NERC to post it for an industry comment period the week of July 20.

VI. CIP-002 SUBGROUPS

A. Introduction, Organization, Appointment and Charge to the CIP-002 Subgroups

In advance of the meeting the Chair and Vice Chair circulated to members a proposal for the work plan from July–December, 2009. The Chair reviewed the proposal which set forth roles and responsibilities and included involving all members of the SDT in at least one of five proposed subgroups to develop draft requirements for consideration by the SDT to be included in a draft CIP-002 Version 3. Through SDT Subgroups and the full SDT, an initial draft of CIP-002 requirements and measures would be produced by December 2009 consistent with the Working Paper concepts and consensus points. In the fall of 2009, the SDT would begin initial drafting of the standards that will replace the current versions of CIP-003 through CIP-009 in parallel with the CIP-002 posting and balloting. In 2010 the SDT would respond to industry comments and post the new CIP-002-009 for balloting later in 2010-2011.

Building on the Working Paper, the following topical SDT subgroups were proposed and agreed to by the SDT to develop an initial set of CIP-002 requirements:

1. Reliability Functions
2. List of BES Subsystems and/or BES Cyber Systems
3. BES Mapping
4. Cyber Analysis
5. Definition and Selection of Controls (sample control or set of controls from the controls catalogue as a “proof of concept”).

Each SDT member present ranked, in order of preference, their interest in participating in each of the 5 subgroups. (*See Appendix #7*). In light of preferences, the Chair and Vice Chair proposed the following composition for the 5 working groups:

Subgroup Name	Members and Observers
Reliability Functions	John Varnell (1), Jim Brenton (1), Dave Norton, Rich Kinas, Doug Johnson, James Bassett
List of BES Subsystems and/or BES Cyber Systems	Jackie Collett, Scott Rosenberger, Jay Cribb, and Gerry Freese.
BES Mapping	John Lim (1), Jeri D. Brewer (1), Dave Revill (2)

	Sharon Edwards and Kevin Sherlin
Cyber Analysis	Chris Peters, Phil Huff , Rob Antonishen, Frank Kim and Joe Doetzl. Sam Merrell and Mike Toecker
Definition and Selection of Controls	Kevin Perry, Bill Winters, Jon Stanford, Keith Stouffer. Peter Schneider

On the morning of day two, Stu Langton presented some tips and guidelines for the subgroup leaders and members on small group discussion and shared leadership. *(See, Appendix 10)*

B. Subgroup Organizational Meetings and Comment Form Questions

On the afternoon of the first day the 5 groups met in parallel organizational sessions to: review scope of topic and identify areas that may need development of related CIP-002 requirements; determine what information they will need going forward; select a leader/spokesperson, a scribe and a timekeeper; sketch out a work plan, including meetings, to get the work done by the October SDT meeting. Subgroups reported back at the end of day one and day two the issues they identified and their plans going forward.

1. Reliability Functions Subgroup

This subgroup agreed that John Varnell will serve as the subgroup lead and Jim Breton would serve as the subgroup scribe and Rich Kinas would perform the timekeeper role. They agreed to the request of James Basset, IPS and Doug Johnson, Commonwealth Edison to help with the subgroup's work. They met both the first and second day of the meeting. John reported the group will plan on meeting weekly starting with July 20 and use WebEx and offered the following report on their work:

Purpose: Define Reliability Functions for new CIP-002-3 (Version 3) NLT Oct 2009 Meeting

Members attending (July 13) in Vancouver, BC: John Varnell, Chair, Jim Brenton, EROCT, Secretary, Rich Kinas, Sgt at Arms/Time keeper, Dave Norton, not in Conf call (may be on bench) James Bassett, IPS, Observer Doug Johnson, Commonwealth Edison

Schedule: Weekly Meetings — WebEx and conference calls — Richard Kinas (set first WebEx for July 20 at 9 a.m. CDT)

Goals and Objective: Fully defined basic reliability functions prior to the October SDT meeting using key inputs from those who have not been previously involved with team efforts(Observers: Doug Johnson (NERC OC member) and James Basset). Need to provide list of key Reliability Functions to BES Mapping Group ASAP

Needed Resources: Review functions:

- Executive Summary of Paper and ALRs (from the CA Guidelines),
- Version 4 and 5 Functional Model,
- Draft Working Paper, and
- Reliability Functional Model Technical Document,

- CA and CCA Identification Guidelines.

Initial Activity:
ID functional model elements needed for reliability--Then break down for each Functional Entity.

Major Activities reported to Full Team

1) Set schedule to discuss weekly with key team of members and observers — Done
2) Structured organization — John Leads, Jim types, Rich watches as timekeeper and Sgt at Arms
3) Collect and distribute Five key documents to all team members — Done

Out of Scope: We may not be able to develop Detailed Requirement Specs since this is a structural segment of the overall model, and does not lend itself to detail requirement specification TBD with John Varnell.

Concept Paper Comment Form Questions regarding Reliability Functions

- Is the concept of the categorizing by function instead of by asset clear? If not why?
- The BES Reliability Functions listed in the "BES Function" column of the table were not meant to be comprehensive. Are there any others functions we need to address and why?

2. List of BES Systems/BES Cyber Systems Subgroup
Jackie Collett is the Subgroup lead, Jay Cribb will serve as scribe and Scott Rosenberger will serve as timekeeper and Gerry Freese will serve as a member.

The Subgroup met on both days and reported to the SDT the following 10 key questions they will be exploring in developing their recommendations:

a) We need definitions and requirements from other standards that apply (Contingency Reserve, etc). Will the BES Reliability group be providing these?
b) How do we handle systems that cross functional model entities?
c) What is the definition of "system"? (This is foundational).
d) Will there be minimum criteria to be on the lists?
e) What is the methodology for identifying BES assets and cyber assets?
f) How do we limit the cyber assets included in 'connections'? What are the boundary conditions for BES systems/cyber systems?
g) How do we handle the dynamic nature of the grid and the BES systems/assets? Example: Contingency Reserve is a MW threshold and the units designated for it may change often.
h) What is "common mode failure"? It is used several times in the white paper.
i) How do we handle controls at the 'perimeter' vs. controls on every 'inside' asset/component?
j) What is the proper granularity of "system" identification?

Concept Paper Comment Form Questions regarding List of BES Subsystems

- Does the methodology presented in the Identification of BES Subsystems and the Identification of BES Cyber Systems sections capture all of the systems that will need to be protected to achieve an acceptable level of reliability? What other issues need to be considered?

3. BES Mapping Subgroup

John Lim will serve as leader, Sharon Edwards as scribe, Dave Revill (as timekeeper), Kevin Sherlin and Jeri Domingo Brewer as members. They reviewed and agreed on the subgroup's scope as primarily defining criteria/ numerical thresholds. They noted they needed input from the reliability function subgroup and they would need to address overlap and coordination as their output is our input. In terms of Impact level (for example, DHS tiers) the subgroup will define the number of levels that will be used.

The subgroup brainstormed the following:

- Review DHS Critical Asset Tiers, NERC Event Classification Criteria, NERC Critical
  - Other documents may help us including the DHS Critical Tiers
  - NERC Event Classification Criteria — guidance for people to classify events
  - NERC Critical Asset Guideline
  - Guideline for Critical Cyber Asset identification
- Asset Risk Assessment Guide
- Other NERC Reliability Standards
- Get input from our own shops as to their level of support for the various concepts and thresholds

The subgroup agreed to meet once per week in the near term on Wednesdays at 3 p.m. EST. The next meeting would be on August 5 from 3 to 5 p.m. by phone. Also the group will meet early for the August drafting team meeting at 1 p.m. on the day prior, which is August 19, face to face at a meeting place TBD.

Assignments for subsequent meeting: Take the DHS and the BES and CA Guideline and get comments from the operating groups.

The group developing the following initial input/questions for the comment form which were reviewed by the SDT with suggestions for refinements and consolidation:

- Would the industry prefer criteria for minimum thresholds & then the industry can define whether they want to do more?
- Please provide your thoughts on the appropriate thresholds to establish criticality.
- Does your company support numeric thresholds for categorizing generation?
- Does your company support numeric thresholds for categorizing substations?

- Does your company support a numeric threshold for categorizing control centers?
- The paper proposes a categorization of all BES assets
  - Do you support this concept?
  - Why or why not?
- The paper proposes categories based on pre-defined criteria
  - Do you support this approach?
  - If not, what alternative method do you suggest?
- What do you believe is the appropriate number of levels for categorization of the BES assets?
- Do you have other suggestions for categorization of assets?

Following their presentation to the SDT, the subgroup refined and consolidated a proposed list of 3 questions:

Concept Paper Comment Form Questions regarding BES Mapping

- The concept paper proposes that all identified BES subsystems are mapped into categories based on pre-defined criteria which reflect their impact on the reliability and operability of the BES: this mapping will be based on pre-defined criteria in the functions they provide or support, which determine the level of that impact. Do you agree with this approach and if not, what alternative suggestions do you have?
- The paper gave an example of High, Medium and Low impact levels. What do you believe is the appropriate number of levels for impact mapping of the BES subsystems?
- Do you prefer discrete thresholds or performance based criteria for mapping BES sub-systems? E.g. MW values as opposed to percentage of total generation. Please explain.

4. Cyber Analysis Subgroup

Phil Huff will serve as leader, Chris Peters as scribe, and Rob Antonishen as timekeeper, Frank Kim and Joe Doetzl will serve as members. Sam Merrell and Mike Toecker will participate as observers. The subgroup will seek to address "defining the target of protection" and dealing with 3rd party interconnections. The reported on the following issues to the SDT:

- Interconnections — how to address of about cyber assets- functional perspective or within controls.
- Lots of interface with security controls in terms of what the impact categories will be, how many levels we need and interface with the selection of controls.
- Risk analysis in selecting controls. Look at how to implement risk assessment to replace the TFE process, work with controls group. Somewhere between cyber analysis and controls

In the discussion of the report one members urged the subgroup to keep in mind that the standards process needs to produce measurable requirements which may be challenges to do in the context of risk analysis.

Concept Paper Comment Form Questions regarding Cyber Analysis

- Section X.X, Categorization of Cyber Systems, describes how an entity determines the impact a specific Cyber System has on to its assigned BES reliability functions. Do you agree with this process described in the concept paper? Please explain.
- Section X.X, Final Categorization of Cyber Systems Based on Overall Impact on the BES, describes an example process of how an entity combines the BES impact mapping and Cyber System impact analysis to determine the overall impact a Cyber System has on the BES. Do you agree with this process described in the concept paper? Please explain.
- Section X.X, Defining the Target of Protection, describes how an entity determines the set of Cyber Assets necessary to provide security assurance in the BES functions the Cyber System performs. Do you agree with this process described in the concept paper? Please explain.

5. Definition and Selection of Controls Subgroup

Keith Stouffer will serve as Subgroup leader and they will employ floating scribes and timekeepers among the members: Kevin Perry, Bill Winters and Jon Stanford. Peter Schneider will participate as an observer. They discussed how best to organize the controls framework. Should it be the same as the CIPS have; or the 27001, NIST framework, or the ISA 99 framework? They agreed to work on keeping the current CIP structure and framework but propose collapsing Standards 005 and 007 into a single standard. They will use work from ISA 99 and 853 and map them into a CIP structure. They agreed to work with 3 levels of security controls. Keith noted that the subgroup hopes to have a strawman of the control set done for SDT review by the next SDT meeting in August in Charlotte.

They will take current ISA 99 foundational requirements and start looking at samples of controls for examples. They hope to show examples of low, moderate and high to demonstrate to the industry how it will work and what it will change. The subgroup will work by email between meetings.

Concept Paper Comment Form Questions regarding Definition and Selection of Controls

- Provide your company's thoughts on applying different levels of protection (i.e. security controls) based on characteristics and impact categories of specific BES cyber systems (e.g. transmissions substations, generating plants, control centers) as discussed in Section XX of the concept paper.
- Section XX of the paper introduces the concept of a library of security controls:
    - What sources would you recommend the drafting team consider when developing a library of security controls for protecting categorized BES cyber systems?
    - What specific challenges would you anticipate in implementing controls from among a library of security controls?

C. Subgroup Roles, Responsibilities, Coordination and Guidelines

The SDT discussed the roles that would be played by SDT members, subgroup members, subgroup leaders a coordinating team and staff.

On the second day the SDT agreed that it would be helpful to develop a set of coordination guidelines for the subgroups and suggested:

- Each subgroup should create its own email distribution list to share documents and ideas
- When a subgroup is ready to issue something to the SDT PLUS List, the subgroup leader will send it electronically to Joe Bucciero and he will send it out to the SDT PLUS List.
- Subgroups are expected to meet and coordinate their activities between SDT Meetings. Each subgroup leader will work with the Coordinating Group between SDT Meetings to report on progress and ensure coordination among the 5 subgroups.

VII. NEXT STEPS AND CLOSING

The Chair reviewed with the SDT the schedule for getting the concept paper, the announcement and comment form finalized and posted on the NERC website for industry comment. She suggested this could be accomplished by the week of July 20.

The Chair thanked the members for their hard work together and in the subgroups and commended them on the adoption of the concept paper.

The Chair noted that she and Kevin appreciated and thanked on behalf of the SDT the Drafting Group members for an outstanding job in bringing the SDT to consensus on the concept paper.. Members completed an onsite meeting evaluation form *(See, Appendix #3).*
The SDT adjourned at 3:00 p.m. on July 14.

APPENDICES TABLE OF CONTENTS

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Appendix # 1— Meeting Agenda

Monday, July 13, 2009 | 8 a.m.–5 p.m. PDT
Tuesday, July 14, 2009 | 8 a.m.–5 p.m. PDT
Vancouver, B.C. Canada

Proposed Meeting Objectives and Outcomes

- Receive update on TFE and VSL/VRF processes;
- Review, refine, and adopt the CIP Version 3 Working Paper as a conceptual framework going forward;
- Test SDT consensus on the NERC Request for Response for Interpretation CIP 006-1;
- Agree on SDT 002 Drafting Subgroups organization;
- Convene SDT 002 Drafting Subgroups organizational sessions and report back to SDT; and
- Agree on next steps and assignments.

Monday July 13, 2009

1. **Welcome and Opening Remarks — Jeri Domingo-Brewer and Kevin Perry**
   - Roll Call; NERC Antitrust Compliance Guidelines
   - Facilitator review of May 13–14 Boulder City, NV meeting summary and adoption; and
   - Facilitator review of June 17–18 Portland, OR meeting summary and adoption
2. **Review of Meeting Objectives, Agenda, and Meeting Guidelines — Jeri Domingo Brewer, and Bob Jones**
3. **Update on Technical Feasibility Exception NERC Rules of Procedure — Scott Mix**
4. **Update on VSLs and VRFs — David Taylor**
5. **Update on Other Related Cyber Security Initiatives — SDT Members**
6. **Overview of Steps to Date in the CIP Version 3 (Phase 2) Development Process — Stu Langton**
7. **CIP Version 3 Categorizing Cyber Systems Working Paper — Presentation — John Lim, Phil Huff et al**
8. **Key Outstanding Issues — John Lim, Phil Huff et al**
9. **Proposed CIP-002 Subgroup Process-Members Complete Preference Forms**
10. **Working Lunch — Convene SAR Interpretation Team to Review possible Responses to NERC on Interpretation of CIP 006-1**
11. **Review SAR Interpretation Team Proposed Response to NERC Request for Interpretation of CIP-006-1**
12. **CIP Version 3 Working Paper — Resolve Any Key Issues — John Lim, Phil Huff et al**
13. **Test Consensus and Seek Adoption of the Working Paper for Industry Review**

14. **Review SDT Communication Plan — MRC Meeting, Posting Paper for Comment (14 days), SDT Webinar, Comment Period (30 days)**
15. **Review CIP-002 Work Plan Proposal and Proposed Subgroups and Membership**
16. **Adjourn**

Tuesday July 14, 2009

1. **Welcome and Agenda Review — Jeri Domingo-Brewer**
2. **Summary of Day One Outcomes — Bob Jones**
3. **Subgroup Protocols — Herding Cats 101 — Stu Langton**
4. **Organizational Sessions of the CIP-002 Subgroups — Small Group Breakouts**
5. **CIP-002 Drafting Group Reports and SDT Input — Plenary Session**
6. **Next Steps and CIP Version 3 Process and Work Plan — Review Proposed 2010 Meeting Schedule**
7. **Review Charlotte August Meeting Objectives**
8. **Meeting Evaluation**
9. **Adjourn**

Appendix # 2

Attendees List
July 13–14, 2009 Vancouver, BC

Attending in Person — SDT Members

1. Rob Antonishen	Ontario Power Generation
2. Jeri Domingo-Brewer, Chr.	U.S. Bureau of Reclamation
3. Jim Breton	ERCOT
4. Jackie Collett	Manitoba Hydro
5. Jay S. Cribb	Information Security Analyst, Southern Company Services
6. Gerald S. Freese	Director, Enterprise Info. Security America Electric Pwr.
7. Phillip Huff	Arkansas Electric Coop Corporation
8. John Lim	CISSP, Department Manager, Consolidated Edison Co. NY
9. Frank Kim	Ontario Hydro
10. Kevin B. Perry, Vice Ch.	Director Critical Infrastructure Protection, Southwest Power Pool
11. Christopher A. Peters	ICF International
12. David S. Revill	Georgia Transmission Corporation
13. Scott Rosenberger	Luminant Energy
14.Keith Stouffer	National Institute of Standards & Technology
15. John D. Varnell	Technology Director, Tenaska Power Services Co.
16.William Winters	Arizona Public Service, Inc.
1. Roger Lampilla	NERC
3. Joe Bucciero	NERC/Bucciero Assoc.
4. David Taylor	NERC
5. Gerry Adamski	NERC
6. Robert Jones	FSU/FCRC Consensus Center (Wed. & Thursday)
7. Stuart Langton	FSU/FCRC Consensus Center

SDT Members Attending via WebEx and Phone

17. Joe Doetzl	Manager, Information Security, Kansas City Pwr. & Light Co.
18. Rich Kinas	Orlando Utilities Commission
19. Sharon Edwards	Duke Energy
20. Kevin Sherlin	Sacramento Municipal Utility District
21. Jonathan Stanford	Bonneville Power Administration

Others Attending in Person

Sam Merrill	CERT/SEI
Michael Toecker	BMcD
Peter Schneider	Subnet Solutions

Others Attending via WebEx and Phone

James Bassett	Lafayette
Mark Braendle	ABB
Mark Grace	
Doug Johnson	ConEd
Travis Jeffery	
Kim Long	Duke
Jerry Mannerino	
Mike Mertz	SCE
Hoang Ngo	RI Eng
Nitin Patel	
Mike Sanders	SoCal
Robin Siewart	EON

Appendix # 3 — Meeting Evaluation Feedback Summary

Members used the following 0 to 10 scale in evaluating the meeting: 0 means totally disagree and 10 means totally agree.

1) **Please assess the overall meeting.**
   9.14 The agenda packet was very useful.
   8.29 The pre-meeting papers (White Paper and Process Evaluation Summary) were very useful.
   7.33 The WebEx document display and the audio were effective
   7.21 The quality of the meeting facility was good.
   9.29 The objectives for the meeting were stated at the outset.
   9.50 Overall, the objectives of the meeting were fully achieved.
   Were each of the following meeting objectives fully achieved:
   9.29 Receive update on TFE and VSL/VRF processes;
   9.29 Review, refine and adopt the CIP Version 3 Working Paper as a conceptual framework going forward;
   9.30 Test SDT Consensus on the NERC Request for Response for Interpretation CIP 006-1;
   9.29 Agree on SDT 002 Drafting Subgroups organization;
   8.93 Convene SDT 002 Drafting Subgroups organizational sessions and report back to SDT; and
   8.67 Agree on next steps and assignments.

2) **Please tell us how well you believe the Team members and participants engaged in the meeting.**
   8.93 The Chair and Vice Chair provided leadership and direction to Team and Facilitators
   9.14 The Facilitators made sure the concerns of all members were heard.
   9.07 The Facilitators helped clarify and summarize issues.
   7.73 The Facilitators helped members build consensus.
   7.93 The Facilitators made sure the concerns of all participants were heard.
   8.43 The Facilitators helped us arrange our time well.

3) **What is your level of satisfaction with what was achieved at the meeting?**
   9.07 Overall, I am very satisfied with the results of the meeting.
   8.36 Overall, the design of the meeting agenda was effective.
   8.93 I was very satisfied with the services provided by the Facilitators.
   9.00 I am satisfied with the outcome of the meeting.
   9.29 I know what the next steps following this meeting will be.
   9.43 I know who is responsible for the next steps.

4) **Other comments:**
   What did we achieve?
   - Approved concept paper; organized for development of requirement language.
   - White paper is done
   - Approving the whitepaper provided a basis for moving forward.
   - Sub group, updates, scheduling.
   - Approval and concept paper

   What are our biggest challenges going forward?

- Moving along the same path
- Industry consensus
- V3, control development
- Moving concepts to reality through requirements. Maintaining group involvement in a recession.
- Keeping sub group momentum.
- Achieved drafting so COP 002- Approval to catalog of controls.

What suggestions do you have for making our group more productive?

- Set up earlier to start on schedule
- Better facilities for subgroup meetings. Internet access for everyone.
- Continue levering sub groups.
- Problems with room on 1st day could have been better resolved.

Appendix # 4 — NERC Antitrust Compliance Guidelines

I. General

It is NERC's policy and practice to obey the antitrust laws and to avoid all conduct that unreasonably restrains competition. This policy requires the avoidance of any conduct that violates, or that might appear to violate, the antitrust laws. Among other things, the antitrust laws forbid any agreement between or among competitors regarding prices, availability of service, product design, terms of sale, division of markets, allocation of customers or any other activity that unreasonably restrains competition.

It is the responsibility of every NERC participant and employee who may in any way affect NERC's compliance with the antitrust laws to carry out this commitment.

Antitrust laws are complex and subject to court interpretation that can vary over time and from one court to another. The purpose of these guidelines is to alert NERC participants and employees to potential antitrust problems and to set forth policies to be followed with respect to activities that may involve antitrust considerations. In some instances, the NERC policy contained in these guidelines is stricter than the applicable antitrust laws. Any NERC participant or employee who is uncertain about the legal ramifications of a particular course of conduct or who has doubts or concerns about whether NERC's antitrust compliance policy is implicated in any situation should consult NERC's General Counsel immediately.

II. Prohibited Activities

Participants in NERC activities (including those of its committees and subgroups) should refrain from the following when acting in their capacity as participants in NERC activities (e.g., at NERC meetings, conference calls and in informal discussions):

- Discussions involving pricing information, especially margin (profit) and internal cost
- information and participants' expectations as to their future prices or internal costs.
- Discussions of a participant's marketing strategies.
- Discussions regarding how customers and geographical areas are to be divided among competitors.
- Discussions concerning the exclusion of competitors from markets.
- Discussions concerning boycotting or group refusals to deal with competitors, vendors or suppliers.

III. Activities That Are Permitted

From time to time decisions or actions of NERC (including those of its committees and subgroups) may have a negative impact on particular entities and thus in that sense adversely impact competition. Decisions and actions by NERC (including its committees and subgroups)

should only be undertaken for the purpose of promoting and maintaining the reliability and adequacy of the bulk power system. If you do not have a legitimate purpose consistent with this objective for discussing a matter, please refrain from discussing the matter during NERC meetings and in other NERC-related communications.

You should also ensure that NERC procedures, including those set forth in NERC's Certificate of Incorporation and Bylaws are followed in conducting NERC business. Other NERC procedures that may be applicable to a particular NERC activity include the following:

- Reliability Standards Process Manual
- Organization and Procedures Manual for the NERC Standing Committees
- System Operator Certification Program

In addition, all discussions in NERC meetings and other NERC-related communications should be within the scope of the mandate for or assignment to the particular NERC committee or subgroup, as well as within the scope of the published agenda for the meeting.

No decisions should be made nor any actions taken in NERC activities for the purpose of giving an industry participant or group of participants a competitive advantage over other participants. In particular, decisions with respect to setting, revising, or assessing compliance with NERC reliability standards should not be influenced by anti-competitive motivations.

Subject to the foregoing restrictions, participants in NERC activities may discuss:

- Reliability matters relating to the bulk power system, including operation and planning matters such as establishing or revising reliability standards, special operating procedures, operating transfer capabilities, and plans for new facilities.
- Matters relating to the impact of reliability standards for the bulk power system on
- electricity markets, and the impact of electricity market operations on the reliability of the bulk power system.
- Proposed filings or other communications with state or federal regulatory authorities or other governmental entities.
- Matters relating to the internal governance, management and operation of NERC, such as nominations for vacant committee positions, budgeting and assessments, and
- employment matters; and procedural matters such as planning and scheduling meetings.

Any other matters that do not clearly fall within these guidelines should be reviewed with NERC's General Counsel before being discussed.

APPENDIX # 5
Meeting Schedule
October 2008–December 2010

Development of CIP Version 2 and Version 3 Framework

October 2008–July 2009

1. October 6–7, 2008 — Gaithersburg, MD Reviewed CIP-002-CIP-009, Agreed on Version 2 approach.

2. October 20–21 —Sacramento, CA CIP-002-CIP-009 Version 2 development

3. November 12–14, 2008 — Little Rock, AR CIP-002-CIP-009 Version 2 adoption for comment and balloting; CIP-002-CIP-009 Version 3 process reviewed.

4. December 4–5, 2008 — Washington D.C. CIP-002-CIP-009 Version 3 reviewed and debated, SDT member white papers assigned.

5. January 7–9 — Phoenix, AZ, Reviewed Technical Feasibility Exceptions white paper**,** reviewed industry comments on CIP-002-CIP-009 Version 2 products — established small groups to draft responses, reviewed Version 3 white papers.

January 15 — WebEx meeting(s) Small group drafted responses to industry Version 2 comments.

January 21 — WebEx meeting(s) Small group drafted responses to industry Version 2 comments.

6. February 2–4, 2009 — Phoenix, AZ Update on NERC Technical Feasibility Exceptions process**,** VSL process and SDT role**,** review of Version 3 White papers, strawman and principles**,** reviewed and adopted SDT responses to industry comments on Version 2 and Version 2 Product Revisions.

7. February 18–19, 2009 — Fairfax, VA Update on Version 2 process**,** NERC TFE process and VSL Team process; reviewed, discussed and refined Version 3 CIP-002 White papers, strawman, and principles.

8. March 10–11, 2009 — Orlando, FL Update on NERC TFE and VSL and VRF Team process and review and refine Version 3 CIP-002 Strawman Proposals

March 2–April 1, 2009 — 30-day Pre Ballot

Mid-March — NERC posts TFE draft Rules of Procedure for industry comment

March 30, 2009 — WebEx meeting(s) White Paper Drafting Team

April 1–10 — NERC Balloting on Version 2 Products

April 6, 2009 — WebEx meeting — White Paper Drafting Team

April 8, 2009 — WebEx meeting(s) — White Paper Preview- Full SDT Conference Call

April 11, 2009 — Version 2 Ballot Results (Quorum: 91.90% Approval: 84.06%) and Industry Comments-

9. April 14–16, 2009 — Charlotte NC Update on NERC TFE process, VSL Team process and NERC Critical Assets Survey; agreed and adopted responses for Version 2 industry comments for recirculation ballot; reviewed and refined Version 3 whitepaper and consensus points and progress report to NERC Member Representative Committee (MRC) May meeting.

April 28 and May 6, 2009 — White Paper Drafting Team Meetings and WebEx

April 17–27, 2009 — Recirculation Results: Quorum: 94.37% Approval: 88.32%

May 5, 2009 — NERC MRC Meeting, Arlington, VA- SDT progress report.

10. May 13–14, 2009 — Boulder City NV Reviewed MRC presentation and further SDT refinement and discussion of the Version 3 White Paper.

June 8 and June 15, 2009 — Working Paper Drafting Team Meetings and WebEx

11. June 17–18, 2009 — Portland OR Further SDT refinement of the draft CIP Version 3 Working Paper(s), reviewed SDT development process for June-December 2009; discussed potential SDT subcommittee structure and deliverables.

June — WebEx meeting(s)

- Working Paper drafting group sessions including inputs from selected industry personnel to help establish BES categorization criteria

CIP-002 Development of Requirements, Measures, Etc. July-December 2009

12. July 13–14, 2009 in Vancouver, B.C., Canada

- SDT plenary session to review, refine, and adopt SDT Working Paper
- Adopt SDT response to NERC for Interpretation of CIP-006-1
- Review and adopt proposal for CIP-002 Subgroups and Deliverables
- Convene subgroup organizational meetings to develop work plans
- Adopt 2010 Meeting Schedule

July–August Interim WebEx meeting(s)

- CIP-002 Subgroup meetings (as needed)
- CIP-002 Coordination Team meeting (as needed)

August 3–5, 2009 in Winnipeg, Manitoba **NERC Member Representative Committee**

Progress Report and presentation on new CIP Version 3 Working Paper-Concept- Reliability Standards on Cyber Security for MRC input.

13. August 20–21, 2009 in Charlotte, NC

- SDT Plenary session to review and respond to MRC input on Working Paper/CIP-002 Concepts
- SDT Subgroup and plenary meetings to develop CIP-002 requirements and "proof of concept" control (s).

July–September — 45-day Industry Comment Period on CIP-002 Concept Working Paper

NERC Webinar

August–September Interim WebEx meeting(s)

- CIP-002 Subgroup meetings (as needed)
- CIP-002 Coordination Team meeting

14. September 9–10, 2009 in Folsom, CA

- SDT plenary session to review and respond to any additional industry comments on Working Paper and CIP-002 Concepts
- SDT subgroup drafting meetings- consider industry comments, draft requirements and "proof of concept" control (s).
- SDT plenary session(s) Subgroup reports on requirements
- Review of CIP-002 Standards, Requirements, Measures, and Outline
- Address coordinating issues.
- Establish SDT meeting dates and proposed locations for January–December 2010

September–October Interim WebEx meeting(s)

- CIP-002 Subgroup meetings (as needed)
- CIP-002 Coordination Team meeting

15. October 20–22, 2009 in New Orleans, LA

- SDT Subgroup drafting meetings — day one
- SDT Plenary Session(s) — day two subgroup reports on CIP-002 requirements
- Review and refine initial draft of CIP-002 single text

October–November Interim WebEx meeting(s)

- CIP-002 Coordination Team meeting

16. November 17–18, 2009 in Tampa, FL

- SDT plenary session(s) — to review and refine CIP-002 standard, requirements, measures and controls.

November–December Interim WebEx meeting(s)

- Drafting teams as needed to finalize drafts
- CIP-002 Coordination Team meeting

17. December 15–17, 2009 in Atlanta, GA

- SDT plenary session(s) to review, refine, and agree on and adopt CIP-002 standard, requirements, measures and controls.
- Agree on initial posting of draft CIP-002 for industry review and comment.

Refinement of CIP-002 and Development of Other CIP Standards

January–December 2010

(12 SDT monthly meetings and subgroup WebEx meetings as needed)

- SDT responds to industry comments on initial and subsequent postings of CIP-002, Version 3 (may be multiple comment periods, as required)
- Refine the CIP-002 through the comment period and submit new CIP-002 Version 3 Standard for Balloting along with the catalogue of controls (i.e. CIP-003-CIP-009 or its successor) OR
- Ballot CIP-002 while permitting industry to rely on CIP 003-CIP-009 until the full suite of controls (i.e. CIP-003-CIP-009 or its successor) is reviewed and presented for balloting.
- Submit the full suite of CIP Reliability Standards on Cyber Security for Industry Comment
- Refine and Submit the full suite of CIP standards for industry ballot
- NERC Board of Trustees adoption of the full suite of standards
- FERC approves and NERC Implements the full suite of CIP standards

Proposed 2010 Meeting Schedule

January 20–21 — Wednesday–Thursday	July 14–15, Wednesday–Thursday
February 17–18 — Wednesday–Thursday or February 16–18 — Tuesday–Thursday	August 11–12, Wednesday–Thursday
March 10–11 — Wednesday–Thursday or March 9–11 — Tuesday–Thursday	September 8–9, Wednesday–Thursday
April 14–15 — Wednesday–Thursday or April 13–15 — Tuesday–Thursday	October 13–14, Wednesday–Thursday or October 12–14
May 12–13 — Wednesday–Thursday	November 17–18, Wednesday–Thursday
June 9–10 — Wednesday–Thursday or June 9–11 — Tuesday–Thursday	December 15–16, Wednesday–Thursday

Appendix # 6
Project 2008-06 Cyber Security Order 706 SDT CIP-002 Work plan Proposal — July 2009

A. CIP-002 Work plan Objectives

1. Establish the overall schedule and milestones for developing the new CIP reliability standards on cyber security
2. Involve all members of the SDT in at least one of five proposed subgroups to develop draft requirements for consideration by the SDT to be included in a draft CIP-002 Version 3.
3. Present the SDT Working Paper (Categorization of Cyber Systems) to the NERC Member Representative Committee at its August 2009 meeting.
4. Post, host a webinar, and receive and consider industry comments on the Working Paper in August-September 2009 as the SDT drafts CIP-002 Version 3.
5. Through SDT Subgroups and the full SDT, produce an initial draft of CIP-002 requirements and measures by December 2009 that are consistent with the Working Paper concepts and consensus points.
6. Seek and respond to industry comment and post the new CIP-002 for balloting in 2010
7. Begin initial drafting of the standards that will replace the current versions of CIP-003 through CIP-009 in parallel with the CIP-002 posting and balloting.
8. Prepare and issue the replacements for CIP-003 through CIP-009 for posting and balloting in 2010/2011.

B. Proposed CIP-002 Subgroups

Building on the Working Paper, the following topical subgroups are proposed to develop an initial set of CIP-002 requirements:

1. Reliability Functions
2. List of BES Subsystems and/or BES Cyber Systems
3. BES Mapping
4. Cyber Analysis
5. Definition and Selection of Controls (sample control or set of controls from the controls catalogue as a "proof of concept").

C. Proposed Steps for Forming CIP-002 Subgroups- Vancouver

1. On day one, ask each SDT member to rank in order of preference their interest in participating in each of the 5 subgroups. In light of preferences, propose composition for the 5 working groups with 3-6 members in each.
2. On day two, convene the 5 groups in parallel and ask members to: 1) review scope of topic and identify areas that may need development of related CIP-002 requirements; 2) determine what information they will need going forward; 3) select a leader/spokesperson, a scribe and a timekeeper; 4) sketch out a work plan, including meetings, to get the work done by the October SDT meeting. Subgroups will report back their plans on Day 2 of the Vancouver Meeting to the SDT.

3. Where possible, provide staff /facilitator support for the subgroups.
4. Follow up with SDT members not attending the Vancouver meeting for team placement, as needed.

D. Roles and Responsibilities

1. **CSO706 SDT Members.** Review, build consensus, and adopt a draft CIP-002 by December 2009. Members will also begin parallel development efforts in 2010 to draft the new standards that will eventually replace the current CIP-003 through CIP-009 standards once the requirements and measures for the new CIP-002 standard have been defined and vetted.

2. **CIP-002 Subgroup Members.** Subgroup members will be responsible for producing a draft set of requirements related to their topic prior to the October 20-22 SDT meeting. Subgroup members will be responsible for selecting a leader/spokesperson, a scribe and a timekeeper.

3. **CIP-002 Subgroup Leaders.** The Leader will be responsible for leading and facilitating the subgroup's effort in creating and implementing a plan (deliverables, timeline, assignments, review and consideration of industry comments) in consultation with members and with help, as needed, by staff and facilitators.

4. **CIP-002 Coordinating Team.** The SDT Chair and Vice Chair along with the Subgroup Leaders and facilitators will participate on a Coordinating Team that will meet by conference call in advance of each monthly SDT meeting through October 2009 to address any duplication of tasks, identify needs for coordination among the subgroups and vetting of the approaches being considered by each of the subgroups to help smooth the way for preparation of a complete draft of CIP-002 to be reviewed, refined, and adopted in November and December 2009.

5. **Staff and Facilitation Support.** Where/when needed and/or requested, facilitation or other staff support will be provided to the subgroups.

Appendix # 7 — SDT Member Subgroup Assignments

Subgroup Name	Members and Observers
Reliability Functions	John Varnell (1), Jim Brenton (1), Dave Norton, Rich Kinas, Doug Johnson, James Bassett
List of BES Subsystems and/or BES Cyber Systems	Jackie Collett, Scott Rosenberger, Jay Cribb, and Gerry Freese.
BES Mapping	John Lim (1), Jeri D. Brewer (1), Dave Revill (2) Sharon Edwards and Kevin Sherlin
Cyber Analysis	Chris Peters, Phil Huff, Rob Antonishen, Frank Kim and Joe Doetzl. Sam Merrell and Mike Toecker
Definition and Selection of Controls	Kevin Perry, Bill Winters, Jon Stanford, Keith Stouffer. Peter Schneider

Subgroup Preference Form

(Jeri DB, Chris P, Keith s, Jay C, John L., Jim Breton, John Varnell, Dave Revill, Kevin P, Phil H, Rob A., Bill W. Jackie Collett , Jon Stanford, Dave Norton, Scott R, Frank Kim

No forms: Rich Kinas, Sharon Edwards, Gerry Freese, Kevin Sherlin,

Reliability Functions
Potential members: **John Varnell (1), Jim Brenton (1), Dave Norton,**

[Preferences: JDB (5) CP (4) KS (5) JCr (5) JL (3) **JB (1) JV (1**) DR (5) KP (5) PH (5) RA (5) **JC (2)** JS (5) DN SR (5) FK (5)]

List of BES Subsystems and/or BES Cyber Systems

Potential members: **Jackie Collett (1), Scott Rosenberger (1), Jay Cribb (2) (Sharon Edwards), (Gerry Freese)**

[Preferences: JDB (3) CP (5) KS (3) JCr (2) JL (4), JB (5) JV (3) DR (4) KP (4) PH (4) RA (4) JC (1) JS (5) DN, SR (1) FK (3)]

BES Mapping
Potential members: **John Lim (1), Jeri D. Brewer (1), Dave Revill (2) (Rich Kinas)**

[Preferences JDB (1) CP (3) KS (4), JCr (4) JL (1) JB (4) JV (2) DR (2) KP (2) PH (3) RA (2) JC (3) JS (5) DN SR (5) FK (4)]

Cyber Analysis

Proposed members: **Chris Peters (1), Phil Huff (1), Rob Antonishen (1), Frank Kim (1) (Kevin Sherlin)**

[Preferences: JDB (2), CP (1) KS (5) JCr (3) JL (2) JB (2) JV (5) DR (3) KP (3) PH (1) RA (1) BW (2) JC (4) JS (3) DN, SR (2) FK (1)]

Definition and Selection of Controls
Proposed members: **Kevin Perry (1), Bill Winters (1), Jon Stanford (1), Keith Stouffer (1)**

[Preferences: CP (2) KS (1) JCr (1) JL (5) JB (3) JV (4) DR (1) KP (1) PH (2) RA (3) BW (1) JC (5) JS (1)
JDB (4) DN, SR (3)]

Appendix # 8
Version 3 SDT Points of Consensus — April 16, 2009

A. The Standards should require a BES impact assessment as an initial approach to categorizing BES Cyber Systems.

B. The impact categorization of Cyber Systems will be based on reliability functions of the BES to achieve Adequate Levels of Reliability.

C. The Standard's BES Impact Assessment will consider a categorization process.

D. The Standards will require oversight of the categorized list of BES assets by entity types which have a more complete wide-area view of the BES.

E. The Standards will categorize Cyber Systems supporting, either directly or indirectly, the reliability functions of the BES and apply security requirements (or controls) that are commensurate and appropriate to their potential impact on the BES.

F. The final Cyber System categorization will reflect the impact to the BES based on a loss of availability, integrity, or confidentiality of the Cyber System.

G. The Standards will provide Organizations with reasonable flexibility in applying equivalent security controls on the basis of compensating controls and environmental considerations.

H. The Standards will address the complex nature of BES functions and interconnected Cyber Systems, both within and between multiple organizations.

I. The Standards will state explicit criteria for the BES Impact Assessment.

J. The Standards will state explicit criteria for the Cyber Impact Assessment (including use and misuse of cyber systems).

K. The Standards will include a methodology to merge the BES Impact Assessment and Cyber Impact Assessment into a final Cyber System categorization.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Appendix # 9 — Phase II Working Paper

http://www.nerc.com/filez/standards/Project_2008-06_Cyber_Security-RF.html

Categorizing Cyber Systems

An Approach Based on BES Reliability Functions

NERC Cyber Security Standards Drafting Team for Order 706

07/15/2009 — Team

TABLE OF CONTENTS

Appendix #10
Herding Cats 101
Some Tips on Small Group Discussion and Shared Leadership

Purposes:

- Increase Member Participation
- Idea-Creation
- Problem-Solving, Product-Development
- Consensus-Building

Needs:

- Adequate Time
- Leadership
- Right-Size, Right-Composition
- Right Space/Technology, Connecting with others
- Full member engagement and active listening

Some Tips for Leaders and Members:

1. Clarify purpose, tasks, and end results (products/outcomes)
2. Select leaders to organize, chair, keep-records of discussion and proposals, keep-time
3. Create a timed agenda/schedule (get group input, review, and agreement)
4. Identify challenges regarding issues or tasks
5. Identify shared values and principles to guide
6. Use questions to guide (and get them right)
7. Involve everyone in discussion and work
8. Review/summarize discussions frequently and re-clarify question/task
9. Stimulate discussion (brainstorm, nominal group process, strawman drafts, etc.)
10. Use visuals to communicate and connect ideas
11. Connect with absent members
12. Be evaluative (review decisions, processes, and performance).

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Appendix #11 — Working Concept Paper Draft Announcement 7-14-09

July XX, 2009

TO: INDUSTRY STAKEHOLDERS

RE: **REQUEST FOR INFORMAL SUGGESTIONS AND COMMENTS REGARDING THE CONCEPTS CONTAINED IN THE CSO 706 SDT WORKING CONCEPT PAPER "CATEGORIZING CYBER SYSTEMS AN APPROACH BASED ON BES RELIABILITY FUNCTIONS"**

Ladies and Gentlemen:

In 2008, FERC Order 706 paragraph 236 directed the ERO to develop modifications to Standard CIP-002-1 Cyber Security – Critical Cyber Asset Identification to address their concerns regarding: (1) need for ERO guidance regarding the risk-based assessment methodology; (2) scope of critical assets and critical cyber assets; (3) internal, management, approval of the risk-based assessment; (4) external review of critical assets identification; and (5) interdependency analysis.

A Standards Drafting Team (SDT) was appointed by the NERC Standards Committee on August 7, 2008 to develop these modifications as part of Project 2008-06 – Cyber Security Order 706. The SDT has been charged to review each of the CIP reliability standards and address the modifications identified in the FERC Order 706. The SDT began meeting in October, 2008.

The SDT believes the CIP-002 standard and requirements provide a foundation for effective cyber security to protect the systems that support a reliable Bulk Electrical System (BES). After months of deliberation, the SDT is considering an approach to CIP-002 that identifies and categorizes critical assets and critical cyber assets according to impacts on reliability functions. This approach is outlined in the attached draft working paper, *Categorizing Cyber Systems: An Approach Based on BES Reliability Functions*.

The Team seeks informal industry feedback and suggestions on the concepts presented in the attached draft working paper. The SDT seeks suggestions and comments particularly regarding four areas set forth in the draft working paper: BES Reliability Functions; Identification of BES subsystems and/or BES Cyber systems; BES Mapping; Cyber Analysis. The informal industry feedback will be considered by the SDT in developing CIP-002 draft requirements. A draft CIP-002 standard will be posted for formal industry comment as part of the ANSI standards development process later this year.

The concepts presented in the draft working paper, propose a broader and more comprehensive cyber security approach to protect the systems that support a reliable BES. The draft working paper deals primarily with the identification and classification of BES assets and cyber systems.

The SDT has provided a form for industry participants to offer their informal suggestions and comments on the concepts in the draft working paper.

Suggestions and Comments Due: September 1, 2009

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Meeting Agenda

Cyber Security Order 706 SDT — Project 2008-06

Monday, July 13, 2009 | 8 a.m.–5 p.m. PDT
Tuesday, July 14, 2009 | 8 a.m.–5 p.m. PDT
Vancouver, B.C. Canada

Proposed Meeting Objectives and Outcomes

- Receive update on TFE and VSL/VRF processes;
- Review, refine, and adopt the CIP Version 3 Working Paper as a conceptual framework going forward;
- Test SDT consensus on the NERC Request for Response for Interpretation CIP 006-1;
- Agree on SDT 002 Drafting Subgroups organization;
- Convene SDT 002 Drafting Subgroups organizational sessions and report back to SDT; and
- Agree on next steps and assignments.

Monday July 13, 2009

1. **Welcome and Opening Remarks — Jeri Domingo-Brewer and Kevin Perry**
   - Roll Call; NERC Antitrust Compliance Guidelines
   - Facilitator review of May 13–14 Boulder City, NV meeting summary and adoption; and
   - Facilitator review of June 17–18 Portland, OR meeting summary and adoption
2. **Review of Meeting Objectives, Agenda, and Meeting Guidelines — Jeri Domingo Brewer, and Bob Jones**
3. **Update on Technical Feasibility Exception NERC Rules of Procedure — Scott Mix**
4. **Update on VSLs and VRFs — David Taylor**
5. **Update on Other Related Cyber Security Initiatives — SDT Members**
6. **Overview of Steps to Date in the CIP Version 3 (Phase 2) Development Process — Stu Langton**
7. **CIP Version 3 Categorizing Cyber Systems Working Paper — Presentation — John Lim, Phil Huff et al**
8. **Key Outstanding Issues — John Lim, Phil Huff et al**
9. **Proposed CIP-002 Subgroup Process-Members Complete Preference Forms**
10. **Working Lunch — Convene SAR Interpretation Team to Review possible Responses to NERC on Interpretation of CIP 006-1**

11. **Review SAR Interpretation Team Proposed Response to NERC Request for Interpretation of CIP-006-1**
12. **CIP Version 3 Working Paper — Resolve Any Key Issues — John Lim, Phil Huff et al**
13. **Test Consensus and Seek Adoption of the Working Paper for Industry Review**
14. **Review SDT Communication Plan — MRC Meeting, Posting Paper for Comment (14 days), SDT Webinar, Comment Period (30 days)**
15. **Review CIP-002 Work Plan Proposal and Proposed Subgroups and Membership**
16. **Adjourn**

Tuesday July 14, 2009

1. **Welcome and Agenda Review — Jeri Domingo-Brewer**
2. **Summary of Day One Outcomes — Bob Jones**
3. **Subgroup Protocols — Herding Cats 101 — Stu Langton**
4. **Organizational Sessions of the CIP-002 Subgroups — Small Group Breakouts**
5. **CIP-002 Drafting Group Reports and SDT Input — Plenary Session**
6. **Next Steps and CIP Version 3 Process and Work Plan — Review Proposed 2010 Meeting Schedule**
7. **Review Charlotte August Meeting Objectives**
8. **Meeting Evaluation**
9. **Adjourn**

Phase 2 SDT Points of Consensus — April 16, 2009

A. The Standards should require a BES impact assessment as an initial approach to categorizing BES Cyber Systems.

B. The impact categorization of Cyber Systems will be based on reliability functions of the BES to achieve Adequate Levels of Reliability.

C. The Standard's BES Impact Assessment will consider a categorization process.

D. The Standards will require oversight of the categorized list of BES assets by entity types which have a more complete wide-area view of the BES.

E. The Standards will categorize Cyber Systems supporting, either directly or indirectly, the reliability functions of the BES and apply security requirements (or controls) that are commensurate and appropriate to their potential impact on the BES.

F. The final Cyber System categorization will reflect the impact to the BES based on a loss of availability, integrity, or confidentiality of the Cyber System.

G. The Standards will provide Organizations with reasonable flexibility in applying equivalent security controls on the basis of compensating controls and environmental considerations.

H. The Standards will address the complex nature of BES functions and interconnected Cyber Systems, both within and between multiple organizations.

I. The Standards will state explicit criteria for the BES Impact Assessment.

J. The Standards will state explicit criteria for the Cyber Impact Assessment (including use and misuse of cyber systems).

K. The Standards will include a methodology to merge the BES Impact Assessment and Cyber Impact Assessment into a final Cyber System categorization.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Project 2008-06 Cyber Security Order 706 SDT

Work plan Proposal, July 2009

A. CIP-002 Work Plan Objectives

1. Establish the overall schedule and milestones for developing the new CIP reliability standards on cyber security
2. Involve all members of the SDT in at least one of five proposed subgroups to develop draft requirements for consideration by the SDT to be included in a draft CIP-002 Version 3.
3. Present the SDT Working Paper (Categorization of Cyber Systems) to the NERC Member Representative Committee at its August 2009 meeting.
4. Host a webinar, and receive and consider industry comments on the Working Paper in August-September 2009 as the SDT drafts CIP-002 Version 3.
5. Through SDT Subgroups and the full SDT, produce an initial draft of CIP-002 requirements and measures by December 2009 that are consistent with the Working Paper concepts and consensus points.
6. Seek and respond to industry comment and post the new CIP-002 for balloting in 2010.
7. Begin initial drafting of the standards that will replace the current versions of CIP-003 through CIP-009 in parallel with the CIP-002 posting and balloting.
8. Prepare and issue the replacements for CIP-003 through CIP-009 for posting and balloting in 2010–2011.

B. Proposed CIP-002 Subgroups

Building on the Working Paper, the following topical subgroups are proposed to develop an initial set of CIP-002 requirements:

1. Reliability Functions
2. List of BES Subsystems and/or BES Cyber Systems
3. BES Mapping
4. Cyber Analysis
5. Definition and Selection of Controls (sample control or set of controls from the controls catalogue as a "proof of concept")

C. Proposed Steps for Forming CIP-002 Subgroups — Vancouver

1. On day one, ask each SDT member to rank in order of preference their interest in participating in each of the 5 subgroups. In light of preferences, propose composition for the 5 working groups with 3-6 members in each.
2. On day two, convene the 5 groups in parallel and ask members to: 1) review scope of topic and identify areas that may need development of related CIP-002 requirements; 2) determine what information they will need going forward; 3) select a leader/spokesperson, a scribe and a timekeeper; 4) sketch out a work plan, including meetings, to get the work done by the October SDT meeting. Subgroups will report back their plans on Day 2 of the Vancouver Meeting to the SDT.

3. Where possible, provide staff /facilitator support for the subgroups.
4. Follow up with SDT members not attending the Vancouver meeting for team placement.

D. Roles and Responsibilities

1. **CSO706 SDT Members.** Review, build consensus, and adopt a draft CIP-002 by December 2009. Members will also begin parallel development efforts in 2010 to draft the new standards that will eventually replace the current CIP-003 through CIP-009 standards once the requirements and measures for the new CIP-002 standard have been defined and vetted.
2. **CIP-002 Subgroup Members.** Subgroup members will be responsible for producing a draft set of requirements related to their topic prior to the October 20-22 SDT meeting. Subgroup members will be responsible for selecting a leader/spokesperson, a scribe and a timekeeper.
3. **CIP-002 Subgroup Leaders.** The Leader will be responsible for leading and facilitating the subgroup's effort in creating and implementing a plan (deliverables, timeline, assignments, review and consideration of industry comments) in consultation with members and with help, as needed, by staff and facilitators.
4. **CIP-002 Coordinating Team.** The SDT Chair and Vice Chair along with the Subgroup Leaders and facilitators will participate on a Coordinating Team that will meet by conference call in advance of each monthly SDT meeting through October 2009 to address any duplication of tasks, identify needs for coordination among the subgroups and vetting of the approaches being considered by each of the subgroups to help smooth the way for preparation of a complete draft of CIP-002 to be reviewed, refined, and adopted in November and December 2009.
5. **Staff and Facilitation Support.** Where/when needed and/or requested, facilitation or other staff support will be provided to the subgroups.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Cyber Security Order 706 SDT Meeting Schedule
October 2008 — December, 2010

Development of CIP Framework October 2008 — July, 2009

1. October 6–7, 2008 — **NIST, Gaithersburg, MD,** Review of CIP 002-009, Agreement on Phase 1 Version 2 approach

2. October 20–21, 2008 — **Sacramento, CA,** Phase 1 Version 2 Development

3. November 12–14, 2008 — **Little Rock,** Phase 1 Version 2 Adoption; Phase 2 Version 3 Process review

4. December 4–5, 2008 — **Washington D.C.,** Phase 2 Version 3 review and debate, white papers assigned

5. January 7–9 — **Phoenix, AZ**

- Review of Technical Feasibility Exceptions white paper
- Review of Industry Comments on Phase 1 products- Establish and convene small groups to draft responses
- Review of Phase 2 White papers

January 15 Webex meeting

- Small group draft responses to industry

January 21 WebEx meeting

- Small group draft responses to industry

6. February 2–4 — **Phoenix, AZ**

- Update on NERC Technical Feasibility Exceptions process
- Review of VSL process and SDT role
- Review of Phase 2 White papers, strawman and principles
- Review and Adoption of SDT Responses to Industry Comments on Phase 1 and Phase 1 Product Revisions

7. February 18–19 — **Fairfax, VA**

- Update on Phase 1 process
- Update on NERC TFE process
- Update on VSL Team process
- Review, discussion and refinement of Phase 2 CIP-002 White papers, strawman and principles

8. March 10–11 — **Orlando, FL**

- Update on NERC TFE process
- Update on VSL Team process
- Review and Refinement of Phase 2 CIP 002 Strawman Proposals

March 2–April 1 30-day Pre Ballot

Mid-March — NERC posts TFE draft Rules of Procedure for industry comment

March 30 — WebEx meeting White Paper Drafting Team

April 1–10 — **NERC Balloting on Phase 1 Product**

April 6 — WebEx meeting — White Paper Drafting Team

April 8 — Webex meeting — White Paper Preview- Full SDT Conference Call

April 11 — Phase 1 Ballot Results (Quorum: 91.90% Approval: 84.06%) and Industry Comments-

9. April 14–16 — **Charlotte, NC**

- Update on NERC TFE process

- Update on VSL Team process
- Update on the NERC Critical Assets Survey
- Agree and Adopt Responses for Phase 1 Industry Comments- Recirculation Ballot
- Review and Refinement of Phase 2 Whitepaper and Progress Report to MRC

April 28 and May 6 — White Paper Drafting Team Meetings and Webex

April 17–27 — Recirculation Results: Quorum: 94.37% Approval: 88.32%

May 5 — NERC Member Representative Committee Meeting, Arlington, VA — SDT progress report

10. May 13–14 — Boulder City NV

- Review MRC presentation and any input to SDT on Phase 2 approach
- Further SDT refinement and discussion of the Phase 2 White Paper

June — Working Paper Drafting Team Meetings and WebEx — June 8 and June 15, 2009

11. June 17–18 — Portland OR

- Further SDT refinement of the Draft CIP Version 3 Working Paper(s).
- Review SDT development process for June-December 2009
- Discuss potential SDT subcommittee structure and deliverables.

June, WebEx meeting(s)

- Working Paper Sessions including inputs from selected industry personnel to help establish BES Categorization Criteria

CIP 002 Development of Requirements, Measures, Etc. July-Dec 2009

12. July 13–14, 2009 — Vancouver, B.C., Canada

- SDT Plenary session to review, refine, and adopt Working Paper
- Adopt Responses to NERC for Interpretation of CIP-006-1
- Review and Adopt Proposal for CIP-002 Subgroups and Deliverables
- Convene subgroup organizational meetings to develop work plans
- Adopt 2010 Meeting Schedule

July-August Interim WebEx meeting(s)

- CIP 002 Subgroup meetings (as needed)
- CIP 002 Coordination Team meeting (as needed)

August 3–5, 2009 — Winnipeg, Manitoba — **NERC Member Representative Committee** Progress Report and presentation on new CIP Version 3 Working Paper Concept — Reliability Standards on Cyber Security for MRC input

13. August 20–21, 2009 — Charlotte NC

- SDT Plenary session to review and respond to MRC comments on Working Paper and CIP-002 Concepts
- SDT Subgroup and Plenary meetings to develop CIP-002 requirements and “proof of concept” control(s)

August-September — 45-day Industry Comment Period on CIP-002 Working Paper
NERC Webinar

August-September Interim WebEx meeting(s)

- CIP 002 Subgroup meetings (as needed)
- CIP 002 Coordination Team meeting

14. September 9–10, 2009 — Folsom, CA

- SDT Plenary session to review and respond to any additional industry comments on Working Paper and CIP-002 Concepts
- SDT Subgroup drafting meetings — consider industry comments, draft requirements and "proof of concept" control(s)
- SDT Plenary Session(s) — Subgroup reports on requirements
- Review of CIP-002 standard, requirements, and measures outline
- Address coordinating issues
- Establish meeting dates and proposed locations for January-December 2010

September-October Interim WebEx meeting(s)

- CIP-002 Subgroup meetings (as needed)
- CIP-002 Coordination Team meeting

15. October 20–22 — New Orleans LA

- SDT Subgroup drafting meetings — day one
- SDT Plenary Session(s) — Day Two Subgroup reports on CIP-002 requirements
- Review and refine initial draft of CIP 002 single text

October-November Interim WebEx meeting(s)

- CIP-002 Coordination Team meeting

16. November 17–18 — Tampa, FL

- SDT Plenary Session(s) — to review and refine CIP-002 single text — standard, requirements, measures and controls.

November-December Interim WebEx meeting(s)

- Drafting teams as needed to finalize drafts
- CIP 002 Coordination Team meeting

17. December 15-17, Atlanta, GA

- SDT Plenary Session(s) to review, refine, and adopt CIP-002 standard, requirements, measures, and controls.
- Agree on initial posting of draft CIP-002 for industry review and comment

Refinement of CIP-002 and Development of Other CIP Standards — January-December 2010

SDT Meetings 18-30. 2010 (12 SDT monthly meetings and subgroup WebEx meetings as needed)

- SDT Responds to Industry Comments on Initial and Subsequent Postings of CIP-002, Version 3 (may be multiple comment periods, as required)
- Refine the CIP-002 through the comment period and submit new CIP-002 Version 3 Standard for Balloting along with the catalogue of controls (i.e. CIP-003-009 or its successor) **OR**
- Ballot CIP-002 while permitting industry to rely on CIP-003-009 until the full suite of controls (i.e. CIP-003-009 or its successor) is reviewed and presented for balloting.
- Submit the full suite of CIP Reliability Standards on Cyber Security for Industry Comment
- Refine and Submit the full suite of CIP Standards for Industry Ballot
- NERC Board of Trustees Adoption of the full suite of Standards
- FERC Approves and NERC Implements the full suite of CIP Standards

Proposed 2010 Meeting Schedule

January 20–21	July 14–15
February 17–18 or February 16–18	August 11–12
March 10–11 or March 9–11	September 8–9
April 14–15 or April 13–15	October 13–14 or October12–14
May 12–13	November 17–18
June 9–10 or June 9–11,	December 15–16

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Draft Meeting Summary

Cyber Security Order 706 SDT — Project 2008-06

August 20, 2009 | 8 a.m.–5 p.m. PST
August 21, 2009 | 8 a.m.–4 p.m. PST
Charlotte, NC

SDT 706 August 20-21 Meeting Summary Contents

116-390 Village Blvd.
Princeton, NJ 08540
609.452.8060 | www.nerc.com

EXECUTIVE SUMMARY

The Chair, Jeri Domingo-Brewer and Vice Chair, Kevin Perry welcomed the members and Joe Bucciero conducted a roll call of members and participants in the room and on the conference call *(See appendix #2*). The chair reviewed the meeting objectives and Bob Jones, facilitator, reviewed the proposed meeting agenda *(See appendix #1*). The SDT adopted the July 13–14 meeting summary without comment or objection on Friday morning.

Mr. Bucciero reviewed the need to comply with NERC's Antitrust Guidelines *(See Appendix #3).* He urged the team and other participants in the process to carefully review the guidelines as they would cover all participants and observers. He urged all to avoid behaviors or appearance that would be anti-competitive nature and also reminded the group of the sensitive nature of the information under discussion.

Vice Chair Kevin Perry announced, effective at end of October meeting, he will be stepping away from the SDT due to his responsibilities with his new job. He later suggested four principles to bear in mind as we develop the new standards requirements: remove variability; remove arbitrary decision making; criteria (requirements/controls) must be clearly understandable; and criteria performance must be auditable — the entity must be able to demonstrate compliance.

Mr. Langton reviewed the CIP-002 work plan between August and December 2009 which the SDT adopted at its meeting in Vancouver and set up subgroups and some ground rules for their work and coordination with each other. The monthly agenda planning meetings with the Chair and Vice Chair have been expanded to include a leadership coordination meeting with the leads from each of the five subgroups. He noted the five subgroups have about four months to finish work of developing the CIP-002 draft to be released for industry comment in December 2009.

Jeri Domingo-Brewer briefed the SDT on the chair and vice chair's presentation to the Standards Committee on a conference call earlier in August. The chair and vice chair agreed to provide the Committee with a "heads up" if there are any issues that might affect the SDT's ability to get the job done in a timely fashion.

Kevin Perry and Scott Mix made the presentation on the development of the Technical Feasibility Exception process. Mr. Perry described the work of a NERC "Tiger Team" led by Mike Assante, NERC Chief Security Officer, with regional entity representatives to address a number of issues that have been raised in the industry comments received to date. Scott noted that the plan is to submit to NERC Board of Trustees for review and adoption at the October meeting following its consultation with the regional entity representatives. NERC BOT hopes to adopt a final TFE process sometime next year to submit to FERC.

On the first day the SDT discussed the current situation with the TFE process and whether the SDT should support efforts to find a standards solution approach to the challenge presented by TFE interim process in advance of the adoption of CIP Standards Version 3. Mr. Perry noted

that NERC's current view is that explicit or implicit "enabling language" references in the CIP standards will be required for an entity to request a TFE. Mr. Perry noted the current timelines associated with the NERC ROP.

Kevin Perry presented a proposal to the SDT to consider a relatively focused and narrow effort undertaken by a small team of SDT members to build upon the "Technical Feasibility Exceptions Matrix of Applicable Requirements" that he and others in the industry have been developing. It would propose a broader interim TFE process that will allow for a safe harbor for technical feasibility exceptions granted in the interim. An alternative presented by Gerry Freese would be to create a broader effort that would address the TFE and other interpretation issues raised by CIP Version 1 and Version 2. The SDT then identified the following pros and cons related to the proposals.

On day two, Mr. Perry noted he was withdrawing his proposal from day one and offered the following points for a new proposal in light of yesterday's discussion: The SDT should consider expressing support for the use of the NERC Urgent Action process to address the current TFE dilemma. This was done with the 1200 standard. He described the steps in the process and the SDT discussed the intent of the urgent action process and whether to adopt a resolution urging the Standards Committee to consider an urgent action approach. The facilitators noted this was an important issue and there seemed to be support for the SDT to help in some way to facilitate a solution.

After review of a possible resolution, the chair suggested instead that she draft a statement to the chair of the Standards Committee which should note that the SDT has identified an urgent challenge for the industry and that the Standards Committee should consider how to address the gaps that have been identified in terms of Version 2 of CIP standards and the proposed TFE procedure. The statement would note the SDT looked at trying to help with a solution given the skills, abilities and experience on the team, but the time needed would take away from the SDT's main charge and ability to complete the current work plan in a timely fashion. There could then be a summary of various options and implications in terms of the SDT work plan and the matrix attached. The team agreed by common consent that the chair should prepare and send a statement consistent with the spirit of the SDT's review and discussion.

Scott Mix reported on Dave Taylor's behalf that Version 1 is complete with a 92% quorum and 84% approval rate. This has been submitted to FERC on July 30. It will be adopted by FERC rule or by NOPR. Version 2 VSLs and VRFs is in the 30-day pre ballot review period. The expectation is for the second ballot to conclude in early October. NERC anticipates that FERC will take action on the CIP Version 2 standards in September/October 2009 as an Order or a NOPR. The SDT Webinar scheduled for next week was described by Phil Huff

The SDT reviewed the Subgroup process for developing CIP 002. Scott Mix noted that the SDT should begin focusing on both the content and format of a NERC standard and pointed to the possibility of a short set of clear requirements backed up by more detailed appendices or attachments.

CIP-002 Subgroup Reports presented their progress reports on day one and a follow up report on day two from their subgroup meetings.

Reliability Functions Subgroup leader John Varnell reviewed a draft list of assets the Subgroup was developing. He noted they haven't added any more functions but did combine some functions and expand on what was meant by each. He noted they hope to have a complete list by the end of the meeting. On day two he presented the following 9 functions noting each had a set of sub functions:

1. Dynamic response
2. Balancing Load and Generation
3. Controlling Frequency (real power)
4. Controlling Voltage (reactive power)
5. Managing Constraints
6. Control & Operation
7. Restoration of BES
8. Situational awareness
9. Inter-Entity coordination and communication

The List of BES Subsystems/BES Cyber systems Subgroup leader, Jay Cribbs presented an overview of the work done since the Vancouver meeting. Subgroup Leader Jackie Collett was on vacation but the group met once in the interim. He described the subgroup scope and expected output. He noted the subgroup has identified a list of issues and questions ("in this phase the subgroup is coming up with all questions and no answers") that will guide their efforts to develop draft requirements. On day two he offered the following points:

1. We will not outline the process for "how" to create the lists. The white paper gives flexibility in the creation of the lists and allows entities to take a primarily cyber systems oriented view if they wish.
2. Assets and systems that are below the mapping team's "Low" thresholds could be included as minimum criteria in our requirements. This should address the concern over having a "negligible" ranking without requiring us to have an explicit 'negligible' impact category.
3. Are the 'R' statements at the right level? In the current CIP-002, each asset category has its own 'R' statement but we think this is unnecessary.

In terms of next steps he noted the subgroup would:

- Convene the remainder of our team to gather input and wordsmith our requirements.
- Obtain and incorporate the work of the Reliability Functions team into our requirements.
- Work with the Mapping team to determine minimum requirements for our lists.

BES Mapping Subgroup leader John Lim noted they met twice since Vancouver and have reviewed and used/borrowed concepts from three key documents: a set of critical asset

guidelines; the NERC DHS proposal for tiering BES assets (3 tiers) depending on impact on reliability of BES; and a classification of events. The resulting first draft of Requirement #2 will address how responsible entities will apply set of criteria to map list from requirement to high/medium and low tiers. The Subgroup is still debating this but it appears that there is a fundamental problem with hard thresholds. While there is more work to be done, it appears that High impact is the most important to be clear on, then Moderate impact. And then all else remaining may be in Low.

On day two John Lim presented the Subgroup's report noting they have lively discussions in the last few days. Changed the format to a matrix for a number of assets in 3 sections: Control Centers and Back up Control Centers; Transmission; and Generation. There was a general aversion to thresholds. If we have to use thresholds, provide the way for entities to say if I meet the threshold with engineering analysis. The common thread is that this will require a lot of use of engineering analysis. John will take last 2 days of discussion; redraft the standard requirement format previously to reflect the discussion. He noted the following issues as outstanding: coordinating with the first 2 groups: functions and BES subsystems. Have a session with Phil Huff to ensure consistency with analysis in both groups.

Phil Huff presented a report on the Cyber Analysis Subgroup's work since Vancouver. He reviewed the 3 teams the Subgroup has formed: Cyber impact categorization; target of protection team; and external cyber systems. Phil reviewed the inputs and outputs of the Cyber System Categorization Process and described the objectives. Phil Huff presented the subgroup report on day 2. They are looking at functional impact. For example in terms of generation — what does it mean for cyber system to impact generation at a h/m/l. What does it mean to affect situational awareness? Short of detrimental, moderate, no impact.

Joe Doetzl presented the subgroups ideas on Target of Protection noting they are proposing to expand the scope of what needs to be protected, e.g. collateral system. The hope is that if we are able to apply the appropriate controls, it may take care of target of protection.

Frank Kim presented on requirements for external cyber systems and presented the issues for consideration. Most External Cyber Systems or Third Party Data Connection NERC CIP-related compliance areas are not thoroughly covered in the existing version of the Standards. Therefore further clarification is required. Amplifying External Third Party system, user, and agreement security considerations are further detailed in other industry security standards such as ISO 27002 and NIST 800-53 that could be leveraged for future iterations of the NERC CIP Standards that pertain to external third party system security. On External Cyber systems, if 2 registered entities with cyber connections then some arbitration agreement should be in place to define the assurance. Assurance is provided by NERC. Putting that over to security controls not in CIP 2 version 3.

Keith Stouffer presented the Definition and Selection of Controls Subgroup's work since Vancouver noting that he had hoped to have a set of controls for the SDT to review but hasn't had a chance to do that yet. On day two Keith Stouffer presented the review of ISA 99 Work.

They looked at controls in draft — voluntary standard. Some controls watered down and may not be useful. Looking at 800 53 controls as they may be more applicable to current environment. Proposing to keep same general CIP-003-009. Should 5 and 7 combined? Contained ½ or 2/3s of all requirements. Decided to propose keeping CIP-005 and make it electronic asset controls. The subgroup is fleshing out new CIP-005 to serve as a model for what the SDT will ultimately do with the rest of standards. Starting with 1 requirement from 800-53, R1 Account Management, they came up with low medium and high.

The chair reviewed with the SDT the schedule for the next couple of meetings reminding members that at the conclusion of the October meeting in Kansas City we hope to have a single text of CIP-002 which we can refine in November and December. She thanked the members for their hard work together and in the subgroups and encouraged them to continue working to make headway on each of their charges. She noted she would forward to the chair of the Standards Committee a statement on behalf of the SDT relating to TFE and the urgent action process. The SDT adjourned at 2:45 p.m. on August 21.

I. INTRODUCTIONS, AGENDA, AND SDT WORK PLAN REVIEW

The Chair, Jeri Domingo-Brewer and Vice Chair, Kevin Perry welcomed the members and Joe Bucciero conducted a roll call of members and participants in the room and on the conference call *(See appendix #2*). The Chair reviewed the meeting objectives and Bob Jones, facilitator, reviewed the proposed meeting agenda *(See appendix #1*). The SDT adopted the July 13–14 meeting summary without comment or objection on Friday morning.

Mr. Bucciero reviewed the need to comply with NERC's Antitrust Guidelines *(See Appendix #3).* He urged the team and other participants in the process to carefully review the guidelines as they would cover all participants and observers. He urged all to avoid behaviors or appearance that would be anti-competitive nature and also reminded the group of the sensitive nature of the information under discussion.

Vice Chair Kevin Perry announced, effective at end of October meeting, he will be stepping away from the SDT due to his responsibilities with his new job. He noted he will miss working with the team which has been a superb group to work with. Following the meeting, Mr. Perry asked that the following additional comments be shared with the SDT and placed in the meeting summary: "I believe there are four principles to bear in mind as we develop the new standards requirements: Remove variability; Remove arbitrary decision making; Criteria (requirements/controls) must be clearly understandable; and Criteria performance must be auditable - the entity must be able to demonstrate compliance. As we go through this process, step back and ask yourself two questions: 1) as an entity, how would I comply with the requirement and demonstrate my compliance? 2) As an auditor, how would I confirm compliance?"

Mr. Langton reviewed the CIP-002 work plan between August and December 2009 which the SDT adopted at its meeting in Vancouver, setting up subgroups and some ground rules for their work and coordination with each other. The monthly agenda planning meetings with the chair and vice chair have been expanded to include a leadership coordination meeting with the leads from each of the five subgroups. He noted the five subgroups have about four months to finish work of developing the CIP-002 draft to be released for industry comment in December 2009. He noted by the conclusion of the October 2009 SDT meeting, the goal is to have a single draft CIP-002 that can be debated and refined in November and adopted in December.

Jeri Domingo-Brewer briefed the SDT on the chair and vice chair's presentation to the Standards Committee on a conference call earlier in August. They noted the SDT's appreciation for the ongoing significant support for their work. When the Committee members indicated concerns with the length of the schedule, the chair indicated the SDT's plan is to have the bulk of their work done by the end of 2010. The chair and vice chair agreed with the Standards Committee that the SDT needs to make significant and visible progress or its effort will be overtaken by events and efforts outside the industry. Finally the Committee asked the SDT leadership to provide them with a "heads up" if there are any issues that might affect the SDT's ability to get the job done in a timely fashion.

II. UPDATES

A. Technical Feasibility Exception (TFE) NERC Rules of Procedure Posting

1. Introduction

Kevin Perry made the presentation and Scott Mix, NERC offered additional information. Mr. Perry noted the work of the NERC "Tiger Team" led by Mike Assante, NERC Chief Security Officer, with regional entity representatives to address a number of issues that have been raised in the industry comments received to date. Scott noted that the plan is to submit to NERC Board of Trustees for review and adoption at the October meeting following its consultation with the regional entity representatives. NERC BOT hopes to adopt a final TFE process sometime next year to submit to FERC.

2. Review of Initial Proposals for Addressing TFEs.

On the first day the SDT discussed the current situation with the TFE process and whether the SDT should support efforts to find a standards solution approach to the challenge presented by TFE interim process in advance of the adoption of CIP Standards Version 3. Mr. Perry noted that NERC's current view is that explicit or implicit "enabling language" references in the CIP standards will be required for an entity to request and receive a TFE. NERC came out July 1 with interim guidance. The ROP put out for comment has received significant comments and concerns. There is currently no program and process in place to support the guidance. Regional Entities are asking the industry entities to hold off submitting their TFEs until this is sorted out. Regional Entities have proposed to take over the processing of TFEs and final touches on a joint NERC Region proposal ("Plan C") are being made. It will call for TFE requests submitted to regions in 2 parts. Part A: identification type of equipment and issue and why the TFE is needed. Part B. will require a "deep dive" into how the mitigation plan will appropriately protect grid in absence of strict compliance. The current TFE proposal today would limit the applicable requirements to 14 requirements and sub requirements in CIP-005, CIP-006, and CIP-007.

If you have a compliance issue other than those requirements where a TFE is available, there is a 90-day schedule. Regions have 60-days to triage the TFE requests and determine whether to conditionally accept them: 1. Saying yes and give an exception or 2. Telling the entity to try again, and why they are being rejected. The entity will have one opportunity to revise and resubmit the TFE request in 30-60 days. If provisionally accepted they will be granted safe harbor from compliance action. If you fail to do anything promised you may lose safe harbor, e.g. not maintaining the mitigation plan — and it goes back to initial request date for compliance. Regional Entities are not currently staffed to do this. The TFE Process is supposed to hit the streets next week for an abbreviated comment period. Mr. Mix noted that the initial 60 days is extendable subject to approval by NERC. Also it was clarified that there could be multiple rounds if done within 30 days.

Kevin Perry presented a proposal that the SDT consider a relatively focused and narrow effort to propose standards changes undertaken by a small team of SDT members to build upon the

"Technical Feasibility Exceptions Matrix of Applicable Requirements" (see Appendix # 6**)** that he and other in the industry have been developing. It would propose a broader interim TFE process that will allow for a safe harbor for technical feasibility exceptions granted in the interim. An alternative proposal, presented by Gerry Freese, would propose creating a broader effort that would address the TFE and other interpretation issues raised by CIP Version 1 and Version 2.

The SDT then identified the following pros and cons related to the TFE proposals:

Pros	Cons
It addresses an urgent issue confronting the industry that may undermine the effectiveness of the SDT in producing a CIP Version 3 the industry will adopt.	It will divert and dilute SDT time and resources and time to getting the CIP 002-009 version 3 done ASAP
The SDT is best positioned currently to get this job done	The SDT may have to adjust and lengthen its Version 3 CIP schedule to respond to industry comments and engage in the ballot process.
Shows FERC and congress the industry is doing something in the interim before Version 3 adopted and approved by FERC.	The Standards Committee has asked the SDT to move as expeditiously as possible to complete its charge
	The SDT will address and seek to minimize the need for invoking TFEs in the CIP Version 3 conceptual approach and should focus on that.
	May result in further confusion about the relationships among the NERC ROP, Version 3 SDT standards development process, the Version 2 guidelines and the TFE Interim Guidance and the permanent process.
	May appear to Congress, FERC and others that SDT resources are being redirected to deal with TFEs
	Expanding the TFE process to address other issues will be difficult to fend off industry members who will want to see the rational for not addressing others.

Member Discussion Comments on Proposals Day One

- There is confusion on the status and the development of the TFEs. The initial draft ROP Scott Mix worked with the SDT on. Lawyers got involved. Regions didn't like the approach to the process. Concerned about entities and audits. Struggling how to deal with practical things. What are entities allowed to do with the TFEs?

- NERC needs to make this simpler — for asset owners and members so they can get their jobs done and spend more time thinking about good security in grid. Good security on grid is possible.
- Should there be any limitations for when you ask for a TFE? Why not provide that TFEs can be requested for all requirements. Let each be reviewed and stand on the merits. If it will mean more work for NERC and the regions, so be it.
- Is the position that the TFE exception, unless explicitly authorized, is not allowed supported by FERC staff?
- Concerned about Congress' perception of the industry diverting resources/efforts away from the reform of the 002-009 from Order 706.
- Mr. Perry sent matrix around seeking input from TFE tiger team and the CIP auditors in other regions. The current draft reflects consensus of opinion across the regions as to areas one should be able to take a TFE. NERC however has not accepted it. FERC did not state in Order 706 that TFEs only could be taken where explicitly set forth in the standards. In fact in May, FERC staff suggested they envisioned broadening the ability of TFEs. However FERC legal and NERC legal have developed a different opinion leaving the industry stuck between a rock and hard place.
- Industry folks are increasingly asking SDT members to explain the rules. Hard to describe where the process is: first had a SDT proposal, then a NERC proposal, then a regional proposal. Don't know what the rules are. Bottom line- people in industry will do everything they can, but are concerned about getting caught in the confused mess. Risk is great with this much confusion.
- Other things in the original proposal. Issues of criteria on safety for e.g. If you have a safety issue it is valid? But only applies to certain requirements. Go ahead because don't care about the safety issue?
- Question from 1 region — making security policy reasonably available to everyone. E.g. Janitor — give him the entire policy. Translation. Supervisors do this. Laudable to put clarity into the standards. Keep in mind. Take hard look from entity's perspectives how to comply — look at auditors' perspective — how to verify compliance without an onerous.
- Distressed if CCWG focusing on this? Have regional compliance entities lost focus?

The Chair and facilitators suggested that this proposal be tabled to review on day 2 when the facilitators could summarize the pros/cons and work with the chair to develop a potential way forward for consideration by the SDT.

3. TFE Urgent Action Proposal

On Day 2 the chair mentioned that she and the vice chair reflected on the TFE day 1discussion over dinner last night and offered an alternative proposal for the SDT consideration. Mr. Perry noted he was withdrawing his proposal from day 1 and proposed an "urgent action" path for TFE changes to the CIP standards. He included the following points:

- The SDT should express support for the use of the NERC Urgent Action process to address the current TFE dilemma as was done with the 1200 standard.

- In the Urgent Action process: someone drafts both a SAR and a modified standard that SAR covers and submits to the Standards Committee for their consideration. It differs from regular procedure in several respects. If the Standards Committee concurs, they will appoint a team and post the urgent action standard language for pre-ballot review followed by ballot and pre ballot.
- The Team will respond to comments from first ballot. If adopted by industry it goes to NERC BOT and to FERC.
- The urgent action standard will remain applicable for a set period of time but can be extended annually. A permanent standard must be placed in development to replace the urgent action standard.
- A major advantage to this approach is it doesn't distract the SDT from pursuing its charge.
- The Standards Committee might form another team, perhaps it is handed off to Larry Bugh chair of the original Version 1 SDT who has now completed the work with VSLs.
- It addresses the timeliness issue since the team is asked to do this it would respond only to comments following the first ballot. It does bypass collaborative nature of normal standards process.
- Mr. Perry briefly summarize scope for urgent action contained in the matrix *(see Appendix 6)*

Member Discussion of the Urgent Action Proposal and Matrix

- Did SDT have in mind covering the non-technical reasons in FERC order, safety etc. or strictly the technical?
- Mr. Perry spoke with NERC and urged them to figure this out. Non-technical exceptions treatment is inconsistent. NERC's paper currently has it both ways.
- How much time would it save if we took matrix and go and file without going through urgent action. Doesn't think it will take much time to draft? The mandate for posting for comment, accept, respond to comments, go out for pre-ballot review, respond to 1st ballot comments. We would have to follow all normal action process and it would take many more months and effort if there are significant comments.
- Why won't NERC accept the matrix? Standards Committee may say this is rewriting the standards outside the standards process.
- With the December compliance deadlines for generation folks, how long will this take?
- It will depend. Standards Committee must appoint team to handle the balloting process and they must respond to balloting comments. Post for pre ballot review. Best of all possible worlds. 10 day initial ballot period. 10 business days- only comment response. Not proposing difficult to understand issues. Industry won't be concerned where we are not making. 30 day posting, 30 day balloting. BOT review. Expedited board action. 30 days. Filing submitted to FERC.
- Upon board approval- standards are mandatory but not sanctionable.
- The generation folks will join the pool of entities that already are out there that in absence of TFE, will not be in compliance. That's why the urgency.

- Original intent of the Urgent Action process was to address situations that had an immediate impact to bulk power. Not to provide relief to standards however poorly written. Technical, operations and safety called out in the FERC Order 706. Is this the right use of the urgent action process. I don't believe it is.
- Scott Mix quoted the Urgent Action opening paragraph indicating intent for the SDT: "Under certain conditions, the Standards Committee may designate a proposed standard or revision to a standard as requiring urgent action. Urgent action may be appropriate when a delay in implementing a proposed standard or revision can materially impact the reliability or security of the bulk power systems or be inconsistent with statutory or regulatory requirements for reliability standards, such as by causing adverse impacts on markets or undue discrimination. The Standards Committee must use its judgment carefully to ensure an urgent action is truly necessary and not simply an expedient way to change or implement a standard." Pg 26 of http://www.nerc.com/fileUploads/File/Standards/RSDP_V6_1_12Mar07.pdf
- We shouldn't worry about the industry approval for this. It should be presented as a valid reliability issue. What will entity do with equipment they might have to replace because of TFE can't get. Submit SARs with standards.
- The expectation will be that when an entity is found out of compliance they will go through investigation, confirmation, plan, self-report and take steps to becoming compliant. Will have some form of reliability impacts. Standards Committee understands the issue.
- What's the alternative? The industry needs to do this. Even if helping a smaller group than all. I would vote to head in this direction. The TFE process is important to fix.
- This will help all entities. RC, Vas and TOPs are in need now. But others will be affected going forward. TFE needed? Spoke with head of his compliance. ERCOT would probably be very supportive and other ISOs would be support.
- The SDT needs to be careful and aware of the "optics" that may be seen as way of avoiding the process.
- The SDT could decline the opportunity to take this on because interferes with our mission and charge but support any efforts to take an Urgent Action approach.
- We are looking at the very best April 1 of 2010 of effective date of Version 2. Assumes FERC issues an order by end of September. Urgent action would not become effective until April 1 2010.
- This could mean that the requirements are enforceable but not sanctionable? Regions would take TFE requests for new requirements.

The facilitators noted this was an important issue and there seemed to be support for the SDT to help in some way to facilitate a solution. They presented for SDT consideration the following draft SDT Resolution:

The SDT supports the streamlined treatment of the interim TFE standards issues through the NERC Urgent Action Process utilizing the "Technical Feasibility Exceptions Matrix of

Applicable Requirements" (see Appendix # 6) as a basis for developing a discrete set of proposed modifications to CIP Version 2 standards.

Following some discussion of the resolution language, the Chair suggested that instead she draft a statement to the Chair of the Standards Committee which should note that the SDT has identified an urgent challenge for the industry and that the Standards Committee should consider how to address the gaps that have been identified in terms of Version 2 of CIP Standards and the proposed TFE procedure. The statement would note the SDT looked at trying to help with a solution given the skills, abilities and experience on the Team, but the time needed would take away from the SDT's main charge and ability to complete the current work plan in a timely fashion. It could be sent to Scott Henry Chair of Security Committee, copying Dave Taylor and Gerry Adamski at NERC. This would be consistent with the Committee's request that the SDT give them a heads up on challenges. The Vice Chair offered separately to bring SDT concerns to the NERC TFE group that was meeting by conference call later in the day.

The team agreed by common consent that the chair should prepare and send a statement consistent with the spirit of the SDT's review and discussion.

B. VSLs and VRFs
Scott Mix reported on Dave Taylor's behalf that Version 1 is complete with a 92 percent quorum and 84 percent approval rate. This has been submitted to FERC on July 30. It will be adopted by FERC rule or by NOPR. Version 2 VSLs and VRFs is in the 30-day pre ballot review period. The expectation is for the second ballot to conclude in early October.

NERC anticipates that FERC will take action on the CIP version 2 standards in September/October 2009 as an Order or a NOPR.

C. Update on other Related Cyber Security Initiatives
The SDT Webinar is scheduled for next week. Phil Huff described the presentation 20–30 minutes leaving 1 hour for questions and discussion. It will introduce the industry to the concept paper. As of today over 240 have registered. Phil agreed to send slides to SDT members. There will be a "dress rehearsal" before the webinar.

SDT Member Comments

- Confusion of concept paper with the Critical asset identification guidelines which a working group has out for wide industry comments.
- Part of CIPC package for its September meeting. Will include a redline and comments and response. Working group working on companion critical cyber asset identification.
- Confusion in the industry is running rampant. Mixed up between the two- follow concept paper for audit. Transmittal letters.
- Went back through the document — couldn't find where this is roadmap for CIP-002 for version 3. May need a disclaimer on there.

III. CIP 002 SUBGROUP REPORTS TO THE SDT

A. Overall

Scott Mix noted that the SDT should begin focusing on both the content and format of a NERC standard. He mentioned he had discussed with Dave Taylor to possibility of a short set of clear requirements backed up by more detailed appendices or attachments. He noted that this would be a departure from how NERC normally does standards and that the sooner the SDT can get some samples to NERC to review format and structure the better.

Member Comments

- Do other standards have attachments associated with them? Scott reported that is precedent in that there are 8-10 standards that have attachments, e.g. EOP 2 (EEA Attachment) and IRO 6 (TLR procedures as an attachment).
- The functions group may have a proposed format to present to the SDT for their section by the end of the meeting.
- It will also be important to be able to show the flow and linkages from one requirement and any supporting appendix to the next

The Chair reviewed with the SDT the subgroups and their members and observers.

Subgroup Name	Members and Observers
Reliability Functions	John Varnell (1), Jim Brenton (1), Dave Norton, Rich Kinas, Doug Johnson, James Bassett
List of BES Subsystems and/or BES Cyber Systems	Jackie Collett, Scott Rosenberger, Jay Cribb, and Gerry Freese.
BES Mapping	John Lim (1), Jeri D. Brewer (1), Dave Revill (2) Sharon Edwards and Kevin Sherlin
Cyber Analysis	Chris Peters, Phil Huff, Rob Antonishen, Frank Kim and Joe Doetzl. Sam Merrell and Mike Toecker
Definition and Selection of Controls	Kevin Perry, Bill Winters, Jon Stanford, Keith Stouffer. Peter Schneider

B. CIP 002 Subgroup Reports and Discussion

1. Reliability Functions Subgroup Report

a. 8-20 Progress Report

John Varnell reviewed a draft list of assets the Subgroup was developing. He noted they haven't added any more functions but did combine some functions and expand on what was meant by each. He noted they hope to have a complete list by the end of the meeting.

Member comments

- Not sure we are all is clear on what each subgroup is to do and produce. Our group has come up with wording for a strawman for requirements would be worded and how functions would be used in the wording of the requirements.
- This subgroup will come up with list of functions. E.g. Requirement 1 in CIP 002 is to come up with list of BES subsystems. Need to list the functions and use list to come up with inventory of relevant subsystems. This might result in a list of minimum types of sub systems that must be used.
- Requirement 2 is the categorization itself and then onward.
- This subgroup will need to work with and help the BES Subsystems/BES Cyber systems Subgroup to come up with list of subsystems.

b. 8-21 Progress Report

John Varnell presented the following proposed functions critical to the reliable operation of the BES:

Defining Functions critical to reliable operation of the BES

The following functions must be evaluated by each Register Entity (RE) for all functions that the RE is responsible for as identified by the NERC Functional Model. The RE must identify ALL equipment required to perform the function, not just the RE owned equipment!

1. Dynamic response
2. Balancing Load and Generation
3. Controlling Frequency (real power)
4. Controlling Voltage (reactive power)
5. Managing Constraints
6. Control & Operation
7. Restoration of BES
8. Situational awareness
9. Inter-Entity coordination and communication

1. Dynamic Response

1.1. Spinning reserve (contingency reserves)

1.2. Governor response
1.3. Protection System (transmission & generation)
1.4. Special Protection System
1.5. Under frequency relay protection
1.6. Under voltage relay protection
1.7. Power System Stabilizers

2. Balancing Load and Generation

2.1. Load management
2.2. Demand Response
2.3. Load shedding
2.4. Unit commitment
2.5. Non-spinning reserve(contingency reserve)
2.6. Calculation of ACE

3. Controlling Frequency (real power)

3.1. Regulation (regulating reserves)
3.2. Generation Control (such as AGC)

4. Controlling Voltage (reactive power)

4.1. AVR (Automatic Voltage Regulation)
4.2. Capacitive and Inductive resources
4.3. SVC (Static VAR Compensators)
4.4. Synchronous Condensers

5. Managing Constraints

5.1. Interchange schedules
5.2. Generation re-dispatch and unit commit
5.3. Identify and monitor SOL's and IROL's
5.4. Identify and monitor Flowgates

6. Control & Operation

6.1. All methods of operating breakers and switches (such as SCADA)

7. Restoration of BES

7.1. Blackstart restoration including planned cranking path (nuke?)

8. Situational Awareness

8.1. Monitoring and alerting (such as EMS alarms)
8.2. Change management
8.3. Current Day & Next Day planning
8.4. Contingency Analysis
8.5. Frequency monitoring

9. Inter-Entity coordination and communication

9.1. Scheduled interchange
9.2. Facility status
9.3. Operational directives

He noted that there are no preconceived notions of regions as these don't exactly match current reliability standard requirements. The subgroup also changed some names so as not to confuse with other terms.

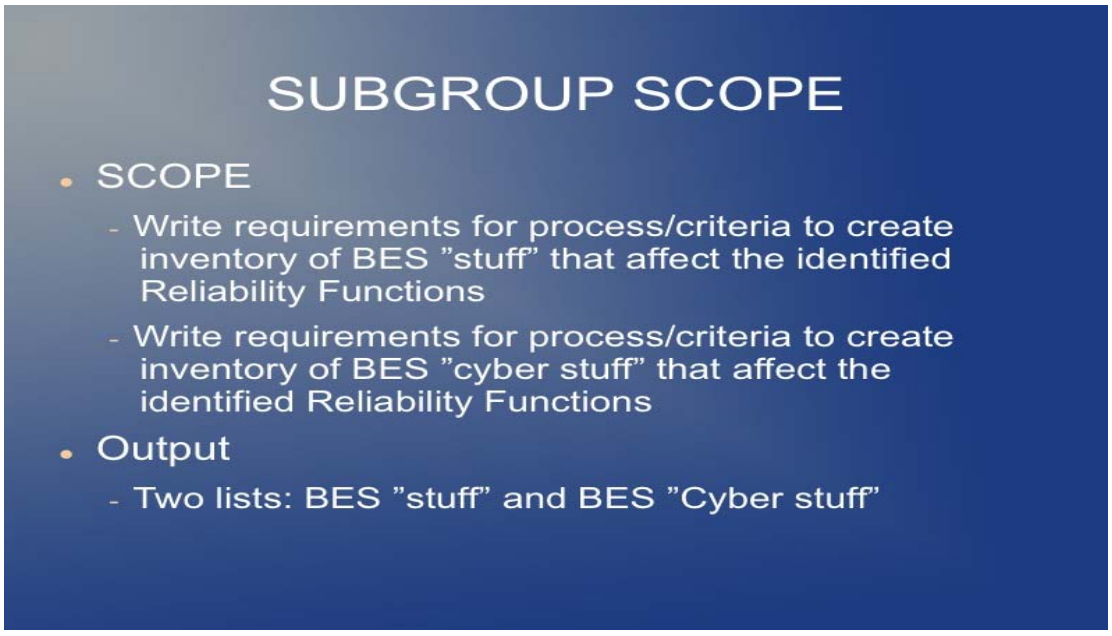
Member Comments

- It is a good idea to put numbers on everything to be able to follow this as we add detail, if necessary. Use numbers to refer to specific functions. Attachments to standards- will be consistent across all entities.
- Why the calculation of ace and not ACE and load balancing? 4. Synchronous condensers here? Yes.
- ACE is specifically laid out in the standards. It is a piece of balancing load and generation.
- Looking at functions based on impact on BES. Thought it might be clearest way to identify the functions.
- The subgroup will develop the real thing and get the requirements. These are the categories the subgroup wanted to get out to other subgroups and their leaders so they can start out their pieces with some idea of the functions.
- Jason Mason offered to run by the Assist Team- OC meeting in September pass by them. The subgroup agreed this would be helpful.

2. List of BES Subsystems/BES Cyber systems Subgroup Report

a. 8-20 Progress Report

Jay Cribbs presented an overview of the work done since the Vancouver meeting. Jackie Collett was on vacation but the group met once in the interim. He described the subgroup scope and expected output.



He noted the subgroup has identified a list of issues and questions ("in this phase the subgroup is coming up with all questions and no answers") that will guide their efforts to develop draft requirements:

- We're step 2. What is step 1's output? Meet with Reliability Functions team to see what their output consists of.
- How do we handle system that cross functional model entities or is owned/controlled by different entities? Whose list does it go on? What if different entities assess things differently?
- What is the definition of "system"? What is the proper granularity of system identification? Must provide clarity not confusion Focus on "stuff" for now then we'll determine the right terminology that considers the NERC Glossary.
- Will there be minimum criteria to be on the lists? This is not an asset management system how do we insure complete list without requiring everything?
- What is the methodology for identifying BES and cyber assets? How do we write a methodology in a requirement?
- Are assets in "connections" to be included in the lists, or do these come in later in the TOP?
- How to handle the dynamic nature of the grid?

SDT Member Comments

- The interface requirements underscore the coordination effort that is critical re output and input.
- This subgroup is the first requirement.
- What is definition of "system"? What level of granularity is needed to define /identify system. Provide clarity not confusion.
- Minimum criteria- to be on list? This isn't an asset management system. Don't want to require everything but where is the line?
- Will there be things like generation at some level or higher?
- What will be the methodology for identifying BES? How to write a methodology in a requirement will be challenging.
- Assets in connection to be included? Target of Protection team will handle.
- One of the things the functions group has discussed. Will have some problems with not having said anything about the overview of the area/region and not being the regional coordinator. This will be challenging all the way through.
- The OC/Planning Committee nominees are now organized and up to speed. They have been given them the list of contacts of the subgroup chairs. The first 3 subgroups groups will be most applicable.
- Can't meet external reviews in the FERC order.
- We hope to be looking at established or establishing thresholds for classification in order to eliminate need for external reviews. Conflicts with RCs. Wrong guesses= liability. This may no longer applicable given new approach. What they ordered was tweaking the existing standards not a rewrite.

- This doesn't mean the RCs are completely out of picture. Criteria may be based on criteria set by RCs. E.g. Contingency reserves set by RCs? That is a BA function or an RSU function? RC can provide insight and information which is different from oversight and review.
- You don't need to know what kind of control system, just know what things required to make the system work reliability.

b. 8-21 Progress Report

Jay Cribb presented the Subgroups report on day two offering the following points:

- We will not outline the process for "how" to create the lists. The white paper gives flexibility in the creation of the lists and allows entities to take a primarily cyber systems oriented view if they wish.
- Assets and systems that are below the mapping team's "Low" thresholds could be included as minimum criteria in our requirements. This should address the concern over having a "negligible" ranking without requiring us to have an explicit 'negligible' impact category.
- Are the 'R' statements at the right level? In the current CIP-002, each asset category has its own 'R' statement but we think this is unnecessary.

In terms of next steps he noted the subgroup would:

1) Convene the remainder of our team to gather input and wordsmith our requirements.
2) Obtain and incorporate the work of the Reliability Functions team into our requirements.
3) Work with the Mapping team to determine minimum requirements for our lists.

3. BES Mapping Subgroup Report, Q & A

a. 8-20 Progress Report

John Lim, the Subgroup leader noted they met twice since Vancouver on August 5 and on August 19. They have reviewed and used/borrowed concepts from three key documents: a set of critical asset guidelines; the NERC DHS proposal for tiering BES assets (3 tiers) depending on impact on reliability of BES; and a classification of events. The resulting first draft of Requirement #2 will address how responsible entities will apply set of criteria to map list from requirement to high/medium and low tiers. The Subgroup has sorted and put the requirements in 3 buckets as an initial exercise. The Subgroup is Still debating this but it appears that there is a fundamental problem with hard thresholds. E.g. 2000 mw, doesn't make sense unless you have an analysis backing that up in terms of impact on reliability. Key need is an analysis to support or not for a bright line threshold. In general, they are trying to get away from hard thresholds. Will be probably qualifying requirements based on this analysis. While there is more work to be done, it appears that High impact is the most important to be clear on, then Moderate impact. And then all else remaining may be in Low.

SDT Member Q & A/ Comments

- How were the levels arrived at? SGWG critical guidelines? Took from 3 documents.
- What is status of the NERC/DHS document process?
- Other criteria were taken from the guideline at the time it was published. Will recheck with final document submitted.
- Members comments on the work. Rod joined from the SIS with good input.
- Subgroup gather together these documents as some of ways to look at criticality. Only begun to vet. Member companies have vetted. Next steps on vetting.
- While there were initially 19 measures for assessing criticality, the subgroup hopes to condense them down to a handful.
- Vetting with SDT- seems to be a resistance to a numerical thresholds. All but 5 members expressed concerns/problems with numerical thresholds.
- 1st requirement. 2000 mw? Is there a way to determine that is universal, and standardize that so that it is not up to a company to figure out?
- Dilemma is you need clear criteria to allow entities to make the correct determination of level (e.g. high). Haven't yet got to the point of how to handle this. This is a threshold, unless you can demonstrate through engineering analysis etc. that it is not. Is it "high unless demonstrate it is not high?"
- Congress won't believe that 2000 mw is not critical. If this were the threshold it wouldn't fly.
- The issue shouldn't be is 2000 the right number , but are big generators critical? Then focus on what "big" is in different interconnections, regions. Sound engineering based on what "big" is and document it in an attachment. It will have to be persuasive. Note that it may make sense in eastern connection and irrelevant everywhere else.
- Big transmission stations- how much is lots of stuff, and what is stuff? John Lim's group will have this job.
- Sharon questioned whether thresholds good. Want to know what the impact is on the BES. Don't care for e.g. lose generation in sharing event exceeding contingency reserve level. Focus on how does it impact the BES. Not thrilled with the tiers. Need to keep in mind the on potential for cascading. There is fear about what "misuse" means. E.g. Aurora turned off a bunch of protections to use this.
- It is important we cover not just the loss of but also misuse of an asset. Operators don't have a long history this.
- How big is big is going to be different in different areas. RCs are going to be the ones understanding this. Not just for oversight but for definition before oversight. Need to discuss this sooner than later.
- To extent you can define common mode contingencies, RCs can provide that guidance.
- Any threshold is wrong. Being big is not the right question. Transmission planner for 11 years. Size of substation or generator. Has to be room evaluation and rational decision that would avoid inconsistent answers in different regions.

- Differences between different regions are presently handled by event analysis. Do other standards have differentiation among the regions?
- Keep in mind "small guys" in the low impact category. Any thing will be weighed against NIST menu of controls.
- Do we need to look at a "non applicable" or negligible category?
- All cyber assets need some level of protection. Thresholds may not be the way to go. Address the different thresholds among interconnections. Those are going to be dynamic and change on a temporal basis and thresholds will be affected by that.
- Mike Assante's- protect control systems in general, large, medium and small.
- Even a small asset with connection needs to be protected. Be careful about what we say should and should not be protected.
- Perception out there may be driving this- if you have a big piece it has to be critical or high impact. If freedom given to reach those determinations then we have the materials to address them.
- VRF team- tendency to call "high" because it is part of standard. This is similar. Don't rush to categorize as high impact as there will be implications down the line.
- Appreciate the SDT feedback- importance of being able to assess the impact to the BES as they are the driving focus of what we are trying to do. If anyone has any across the board strategies we are all ears. What is the best approach to do this? John Lim's approach was valid as a starting point. When you look at these individually they are very flawed.
- Recognize system dynamics causes daily changes. Got to remove variability aspect from any criteria we have. Shouldn't change way we view impact on BES.
- Remove arbitrary decision process that we have today, understandable, repeatable and makes sense. Get away from entity gets to make that choice.
- What ever performance criteria developed- can demonstrate compliance.
- Hard limit on generator output as a threshold related to BES reliability? Balancing generation and load when they get out of whack, they can become a real problem overtime.
- How you can address control systems of neighbors. RC can't really do this. This is a hole in our concept.
- Inadvertent interchange- can be a good thing, not necessarily a bad thing.
- BES Asset and associated cyber stuff. High, medium low. Concerned about time needed to come up with thresholds vs. set of controls applied to everything.
- Focus of NERC and FERC has been on documentation. We potentially have a system with sanctions for something that is not important to reliability.
- The schedule proposed to implement a security control may be different/ (shorter or longer) if it is a high, medium or low impact. E.g. 2 years for high, medium 5, lows 10. 10 year plan. Prioritize work. Keith Stouffer and the Controls subgroup work may help.
- Assign VSF/VSL differently to high medium low?
- References entities criteria be arbitrary? Variable maybe. Not as arbitrary as a threshold standards. N-1 methodology- look at extreme events not N-1- TPL standard

studies include more than N-1. Include contingency events in terms of terrorist actions. Concerned about global national thresholds.
- Differences in controls in the baselines. Some are same, some different. Access control suite of family. Low has 11 requirements; moderate 34 requirement/enhancements; high 39 requirements.
- Awareness and training- same across the board.

b. 8-21 Progress Report

John Lim presented the Subgroups report noting they have lively discussions in the last few days. Changed the format to a matrix for a number of assets in 3 sections: Control Centers and Back up Control Centers; Transmission; and Generation. The subgroup discussed what are control centers, discussed thresholds whether they should be yes/no or performance based. There was a general aversion to thresholds. If we have to use thresholds, provide the way for entities to say if I meet the threshold with engineering analysis. The common thread is that this will require a lot of use of engineering analysis What is it? Will be a challenge to formulate this to put in a standards requirement that is auditable. John will take last 2 days of discussion; redraft the standard requirement format previously to reflect the discussion. He noted the following issues as outstanding: coordinating with the first 2 groups: functions and BES subsystems. Have a session with PH- to ensure consistency with analysis in both groups. Call scheduled in early September- functions group invited to join.

SDT Members Q & A
- High. Medium and low for each category. Specific to another layer- table with 50 rows of h/m/l impact?
- Purpose of functions will be different. Higher level of granularity. Lower level functions useful in providing guidance to entities to identify who is doing what. Keep functions in mind when looking at criteria.
- If this will be auditable, you have a reliability function, go to table to find h/m/l and that is what you would share with the auditor.
- Single subsystem performing a high and lower function, will be placed in the higher.
- Need to be clear so there is no question as to how someone arrived at the rankings.

4. Cyber Analysis Subgroup Report, Q & A

a. 8-20 Progress Report

Phil Huff presented a report on the Subgroup's work since Vancouver. He reviewed the 3 teams the Subgroup has formed: Cyber impact categorization; target of protection team; and external cyber systems. He outlined some issues and assumptions including:

- Cyber analysis- impact assessment on the BES cyber system reliability function
- What impact do reliability functions have on the BES?

- Impact levels: perfect process with impact level the weak point in terms of verifiability.
- Impact levels for each reliability function. High impact to situational awareness, generation control.
- Most BES cyber system will likely have high impact on the function.
- Impact of information disclosure (CEII).

Phil reviewed the inputs and outputs of the Cyber System Categorization Process objectives as:

- To ensure the Responsible Entity categorizes all of its BES Cyber Systems according to the impact a violation in the Cyber System security requirements would have on the BES.
  - To correlate BES reliability functions directly to the BES Cyber System.
  - To correlate the objectives of protecting the confidentiality, integrity, and availability of the Cyber System directly to its BES impact categorization.
- The cyber impact categorization takes the high water mark of impact on each of the supported functions.
- State explicit criteria for the Cyber Impact Assessment (including the misuse of Cyber Systems) [*from the SDT Points of Consensus*].
- Include a methodology to merge the BES and Cyber Impact assessments [*from the SDT Points of Consensus*].

He noted the following issues the subgroup has identified for consideration:

- Impact levels or Cyber categorization are difficult to audit. The alternative to having generic impact descriptions would be to have specific descriptions for each reliability function.
- Assumption: Almost all BES Cyber Systems are *High* impact to the function they provide. If this is the case, then the Cyber Impact Assessment is trivial. This is equivalent to the BES Subsystem impact mapping determining the final categorization.
- In the paper, the cyber impact categorization ties to the final categorization through a matrix. The purpose of having a matrix is to provide some control in how an entity categorizes Cyber Systems. So the cyber impact categorization limits the view of impact only to the reliability functions it supports without considering the importance of those reliability functions to the BES. However, we define a BES Cyber System as one which directly supports reliability functions of the BES. One could argue that, by definition, all BES Cyber Systems have a high impact on the reliability functions they support.

- Instead of a matrix, we might consider using the BES Subsystem mapping as an upper bound which results in the following:

Asset Impact -->	High	Medium	Low
Cyber Impact:			
High	H	M	L
Medium	M	M	L
Low	L	L	L

- Cyber impact would have an upper bound of the function(s) it supports. Using this methodology, it would not be necessary to include the matrix within the Standard.

- We assume the BES Subsystem mapping will have (high/medium/low) criteria. If this is the case, then the Cyber Impact Assessment would look to the criteria for the loss of confidentiality, integrity and availability.
  - The BES Subsystem mapping provides input by mapping the worst case.
  - When assessing the impact of a Cyber System, the organization would first map all of the BES Subsystems which the Cyber System can impact.
  - The organization would look at the loss of confidentiality to a BES Subsystem, as an example. It should not have greater impact to the BES than the BES Subsystem impact mapping. However, justifying a lower impact category would be on the basis of the functional mapping criteria.
- Need to work with *Reliability Functions* team to ensure information such as CEII fits into the proposed assessment model.

He then noted the following steps:

Step 1 — BES subsystem mapping, e.g. SCADA system.
Step 2 — Assess the potential functional impact. E.g. what impact does SCADA have for every reliability function (blackstart etc.) E.g. Situational awareness.
Step 3 — Combine in categorization look up table. Have BES mapping for functions.
Step 4 — Final categorization. High water mark approach.

SDT Member Q & A

- How are you handling the aggregation issue? Mapping to BES sub systems. When multiple, taking a high water mark? Yes.

Joe Doetzl presented the subgroups ideas on Target of Protection noting the are proposing to expand the scope of what needs to be protected, e.g. collateral system. The hope is that if we are able to apply the appropriate controls, it may take care of target of protection.

Frank Kim presented on requirements for external cyber systems noting the following objective:

- Identify and manage risk associated with External Cyber Systems or Third Party Data Connections operating within the Target of Protection

He then presented the following issues for consideration:

- Most External Cyber Systems or Third Party Data Connection NERC CIP-related compliance areas are not thoroughly covered in the existing version of the Standards. Therefore; further clarification is required. In addition, industry security practices and controls such as modifying existing entity contractual agreements and processes to meet applicable NERC CIP requirements should be addressed.
- Amplifying External Third Party system, user, and agreement security considerations are further detailed in other industry security standards such as ISO 27002 and NIST 800-53 that could be leveraged for future iterations of the NERC CIP Standards that pertain to external third party system security. These are not necessarily germane to this requirement but several examples include:

    - **Security Assessment and Authorization (CA-3) Cyber System Connections**
        - Control: The Responsible Entity:
        - Authorizes connections from the Cyber System to other Cyber Systems outside of the Target of Protection through the use of Interconnection Security Agreements;
        - Documents, for each connection, the interface characteristics, security requirements, and the nature of the information communicated; and
        - Monitors the Cyber System connections on an ongoing basis verifying enforcement of security requirements.
    - **Personnel Security (PS-7) Third-Party Personnel Security**: policies and procedures for personnel position categorization, screening, transfer, penalty, and termination; also addresses third-party personnel security.
        - The Responsible Entity:
        - Establishes personnel security requirements including security roles and responsibilities for third-party providers;
        - Documents personnel security requirements; and
        - Monitors provider compliance.
    - **Supplemental Guidance:** Third-party providers include, for example, service bureaus, contractors, and other organizations providing Cyber System development, information technology services, outsourced applications, and network and security management. The Responsible Entity explicitly includes personnel security requirements in acquisition-related documents.
    - **System and Services Acquisition (SA-9) External Cyber System Services**
        - Control: The Responsible Entity:
        - Requires that providers of external Cyber System services comply with Responsible Entity Cyber System security requirements and employ

appropriate security controls in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance;
  - Defines and documents government oversight and user roles and responsibilities with regard to external Cyber Systems services; and
  - Monitors security control compliance by external service providers.
- **System and Communications Protection (SC-7): Boundary Protection**
  - Control: The Cyber System:
  - Monitors and controls communications at the external boundary of the Cyber System and at key internal boundaries within the Cyber System; and Connects to external networks or Cyber Systems only through managed interfaces consisting of boundary protection devices arranged in accordance with an organizational security architecture.

SDT Comments Q & A

- 3rd party connections not covered in the standards. Will ultimately require
- Borrowed from IS0 27 002, NIST 853.
- 2 types of external cyber systems- those under realm subject to NERC. Others not under NERC regulations but have some impact.
- Mix of 3rd parties: vendors, consultants.
- How far to go in 3rd party cyber systems? Should we go for a more narrow focus?

b. 8-21 Progress Report

Phil Huff presented the subgroup report on day 2. They are looking at functional impact. For example in terms of generation what does it mean for cyber system to impact generation at a h/m/l. What does it mean to affect situational awareness? Short of detrimental, moderate, no impact.

SDT Member Q &A

- However we make these decisions, important to capture the thought process. This is what we used to determine high, medium or low.
- Is the impact specific to the function and not the cyber?
- Aren't we looking to the reach of each cyber asset with the reach determining high/med/low
- What is the relationship of cyber asset to functions or sub-functions? The functions themselves dictate what the impact is.
- EMS e.g. impact is high water marking. If it touches 40 of 50, it is high, don't need to look at the other 39. Make sure as soon as you hit the high, you are done. This has to be clear to auditors.
- Target of Protection- security controls- not a requirement that goes in CIP 2 for this. Working hard on definitions in terms of consistency and intent in terms of BES and cyber systems you want to protect.

- On External Cyber systems, if 2 registered entities with cyber connections then some arbitration agreement should be in place to define the assurance. Assurance is provided by NERC. Don't need more.
- Issues with external cyber systems. Putting that over to security controls not in CIP 2 version 3.

5. Definition and Selection of Controls Subgroup Report, Q & A

a. 8-20 Progress Report

Keith Stouffer presented the subgroup's work since Vancouver noting that he had hoped to have a set of controls for the SDT to review but hasn't had a chance to do that yet. He hopes to start working on that soon and bring to the next session. The Subgroup needs help from the SDT on which requirements have the highest priorities that controls are needed for? The Subgroup will need guidance on which to do first and on to last. They have looked at ISA 99- 4 baselines (security assurance levels, and DHS Catalogue of Control System Security just a catalogue NIST 800-53, ISA 99

SDT Member Q & A

- Shows the connection with the ISA and NIST work as well as
- Mike Assante's Congressional testimony training and awareness, incidence response addressed at an organizational level.
- Pull out of catalogue controls and look at general requirements.
- In the Federal system can take care of some of these at organizational level
- From Policy at high org level down to specific controls, vary by installation or by system.
- SDT need to get arms around the consistent use of terminology. Lets refer to these as a "Catalogue of security controls" vs. the familiar process controls.

b. 8-21 Progress Report

Keith Stouffer presented the review of ISA 99 Work. They looked at controls in draft-voluntary standard. Some controls watered down and may not be useful. Looking at 800 53 controls as they may be more applicable to current environment. Proposing to keep same general CIP 003-009. Should 5 and 7 combined? Contained ½ or 2/3s of all requirements. Decided to propose keeping CIP 5 and make it electronic asset controls. The Subroup is fleshing out new CIP 5 to serve as a model for what the SDT will ultimately do with the rest of standards. Starting with 1 requirement from 800-53, R1 Account Management, they came up with low medium and high R1 Account management e.g.

SDT Member Comments

- a and b used in making your documents. Why struck? Seemed odd. Will sort out.
- Exclusion #2 don't agree. Default accounts need to be authorized. Aware they are there. Should remove as well. Requirement for reviewing, for approving.

- The Subroup had the same discussion among themselves.
- Changing the name of account is not changing the account. System id. Can't be changed. Name vs. the function/role.
- On the low 11 controls apply? On this one requirement of one standard. If there are no minimum then every asset is at least a low. Everything- with a chip in it. Is there no "lower than low"?
- I.e. a negligible category? Other piece trying to match requirement to the characteristics of the device and says you don't have to . Malware on an old relay.
- Already have 2 standards- as developing controls- document that says this is why we are not applying this.
- Minimum- utilizing exclusions to manage the "negligible"? 800-53 more extensive, and more guidance. Will be developing a guidance to go along with standard.
- Look at version 1 experience, following 2nd draft, had to take out word "exclusion"
- We should talk in version 3- 200-300 controls? Think about some formal presentation different variations. Formulate a way for dealing with exceptions. Consider controls
- R 1.5.3 remove access to the role, therefore can't perform in the role. Timeline needed here. Cover the entire populations of individual transferred. When someone leaves, remove access and then grant access again.
- Would you consider applying different levels- for high it will be removed. For a low we may not need to do.
- 1 hour termination- how audited?
- Implement system- termination person- within 24 hours. Need to provide documentation. Multi-million access control by profiles. Lots of resources to do this.
- Deletion of temporary-R1.2 f. striken.
- 1.5 sections - 10k switzer relays. 24 hours to change passwords- no inheritance of higher level controls.
- Have to look at environment has to be recognized in drafting controls and requirements.
- Current sub standards don't address this. Users that have access but are not authorized, e.g. system administrators. Need to clearly address.
- Timeline on transferred users etc. can't tell entity that in 1 week to something. "Removing unneeded access" simplifies.
- Technical merits- discussion is good.
- Concerned about this requirement- looks different from everything we've done as part of a standard.
- Get format in front of dt, ga, Maureen, compliance, legal.
- As soon we figure out what it will look like. How will it work? Can it be an acceptable NERC reliability standard.
- Had discussion. Will do what they want and then hear from NERC on whether or not it is possible. Get it down for one requirement. See if it is acceptable.
- NERC no longer putting Rs on sub requirements.
- Applicability and exclusions?

- Need to get Maureen in with this team ASAP.
- If applicability was at beginning- that would flow better than at end.
- Embed applicability in requirement language. Figure out how to draft the structure of the requirements.
- If requirement has sub requirement. Roll up requirements. E.g. the Entity shall do the following
- Some requirements have more than 1 within the requirement itself.
- If roll up function why does it have a VRFs? Have to have a VSL with the main requirements.
- We need to get a hold of filing- and look at Version 2. Such as—bullets. Kept sub requirement.
- Information "Filing" attach to the minutes. Jason will send.
- Need to encourage Maureen to produce a style guide. Scott will follow up.
- This requirement, consolidates all or parts several of CIP 4 R4, CIP 5 2.4.1 2.1.3,
- Is this drafting team going to develop VSLs for version 3? Yes.
- Encouraged by approach- getting all related to a functional area in one place vs. the spaghetti approach.
- Shouldn't have to do all standards at one time.
- Any areas identified where need communication coordination?
- 1 area- make sure opportunity for someone analyzing a function needs to i.d. all hardware used to perform that function whether they own it or not. Assets that do not belong to them.
- John Lim talked about that in criteria. E.g. generation and transmission owner context. Requirement for generator to notify your transmission owner and operators of impact level of facility.

VI. NEXT STEPS AND CLOSING

The Chair reviewed with the SDT the schedule for the next couple of meetings reminding members that at the conclusion of the October meeting in Kansas City we hope to have a single text of CIP 002 which we can refine in November and December. She thanked the members for their hard work together and in the Subroups and encouraged them to continue working to make headway on each of their charges.

She noted that she would draft up the letter to the Standards Committee Chair based on the SDT's discussion of the TFE and Urgent Action approach.

Members completed an onsite meeting evaluation form *(See, Appendix #3).*

The SDT adjourned at 2:45 p.m. on August 21.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

APPENDICES TABLE OF CONTENTS

Appendix # 1— Meeting Agenda

Proposed Meeting Objectives and Outcomes

- Review the work plan going forward;
- Receive update on the MRC presentation and Leaders Coordination call;
- Receive updates on TFE, VSL/VRF and related cyber security efforts;
- Receive and discuss reports from CIP 002 Subgroups;
- Convene CIP 002 Subgroup meetings;
- Subgroup reports back to SDT; and
- Agree on work plan, next steps and assignments.

Thursday August 20, 2009
8:00 a.m. – 12:45 p.m.

1. **Review of CIP 002 Work plan and Subgroup Process including pros – cons of a possible TFE Exception "Version 2.5" — Kevin Perry and Jerry Freese' Version 2.5 Proposal**

2. **Update on Technical Feasibility Exception (TFE) NERC Rules of Procedure and VSLs – VRFs**

3. **Subgroup Reports to the SDT**
   - Reliability Functions Subgroup Report
   - List of BES Subsystems/BES Cyber systems Subgroup Report
   - BES Mapping Subgroup Report
   - Cyber Analysis Subgroup Report
   - Definition and Selection of Controls Subgroup Report

4. **Subgroup Meetings (at various locations)**

5. **Adjourn**

Friday August 21, 2009

1. **Subgroup Meetings**

2. **Subgroup Reports — Plenary Session**
   - Reliability Functions Subgroup Report, Q & A
   - List of BES Subsystems/BES Cyber systems Subgroup Report, Q & A
   - BES Mapping Subgroup Report, Q & A
   - Cyber Analysis Subgroup Report, Q & A

- Definition and Selection of Controls Subgroup Report, Q & A

3. Review and Decide on Work Plan – Review Proposed 2010 Meeting Schedule

4. Adjourn

Appendix # 2
Attendees List
August 20–21, 2009 Charlotte NC

Attending in Person — SDT Members

1. Jeri Domingo-Brewer, Chr.	U.S. Bureau of Reclamation
2. Jim Breton	ERCOT
3. Jay S. Cribb	Information Security Analyst, Southern Company Services
4. Joe Doetzl	Manager, Information Security, Kansas City Pwr. & Light Co.
5. Sharon Edwards	Duke Energy
6. Gerald S. Freese	Director, Enterprise Info. Security America Electric Pwr.
7. Phillip Huff	Arkansas Electric Coop Corporation
8. John Lim	CISSP, Department Manager, Consolidated Edison Co. NY
9. Frank Kim	Ontario Hydro
10. Rich Kinas	Orlando Utilities Commission
11. Sharon Edwards	Duke Energy
12. Kevin B. Perry, Vice Ch.	Director Critical Infrastructure Protection, Southwest Power Pool
12. David S. Revill	Georgia Transmission Corporation
13. Kevin Sherlin	Sacramento Municipal Utility District
14.Keith Stouffer	National Institute of Standards & Technology
15. John D. Varnell	Technology Director, Tenaska Power Services Co.
16.William Winters	Arizona Public Service, Inc.
1. Roger Lampilla	NERC
3. Joe Bucciero	NERC/Bucciero Assoc.
6. Robert Jones	FSU/FCRC Consensus Center (Wed. & Thursday)
7. Stuart Langton	FSU/FCRC Consensus Center

SDT Members Attending via WebEx and Phone

1. Rob Antonishen	Ontario Power Generation (Friday)
2. Jonathan Stanford	Bonneville Power Administration

SDT Members Unable to Attend

1. Jackie Collett	Manitoba Hydro
2. David Norton	Entergy
3. Christopher A. Peters	ICF International
4. Scott Rosenberger	Luminant Energy

Others Attending in Person

Sam Merrill	CERT/SEI
Michael Toecker	BMcD
Peter Schneider	Subnet Solutions

Others Attending via WebEx and Phone

James Bassett	Lafayette
Mike Fischette	Lancing BWI

Matt Greek	
Rob Hardiman	
Doug Johnson	ConEd
Kim Long	Duke
Mike Mertz	SCE
Hoang Ngo	RI Eng
Nitin Patel	
Brian Smith	EnerNex
Robin Siewart	EON
Peter Schneider	

Appendix # 3 — Meeting Evaluation Feedback Summary
August 20–21, 2009, Charlotte, NC
Meeting Evaluation Feedback for Inclusion in Facilitator's Report

Members used the following 0 to 10 scale in evaluating the meeting: 0 means totally disagree and 10 means totally agree.

1. Please assess the overall meeting.

7.78 The agenda packet was very useful.
6.83 The WebEx document display and the audio were effective
8.50 The quality of the meeting facility was good.
7.40 The objectives for the meeting were stated at the outset.
8.30 Overall, the objectives of the meeting were fully achieved.

Was each of the following meeting objectives fully achieved:
7.90 Review the work plan going forward and assess "Version 2.5" possibilities.
8.10 Receive MRC presentation and Leadership Coordination Meeting summary.
7.13 Receive updates on TFE, VSL/VRF and related cyber security efforts;
8.50 Receive and discuss reports from CIP 002 Subroups identifying key issues and coordination points;
9.00 Convene CIP 002 Subroup meetings;
9.20 Receive and discuss Subroup reports on progress made; and
8.80 Agree on Work plan, next steps and assignments

2. Please tell us how well you believe the Team engaged in the meeting.
8.70 The Chair and Vice Chair provided leadership and direction to Team and Facilitators
9.20 The Facilitators made sure the concerns of all members were heard.
8.30 The Facilitators helped clarify and summarize issues.
7.63 The Facilitators helped members build consensus.
9.10 The Facilitators made sure the concerns of all participants were heard.
8.10 The Facilitators helped us arrange our time well.

3. What is your level of satisfaction with what was achieved at the meeting?

8.11 Overall, I am very satisfied with the results of the meeting.
8.13 Overall, the design of the meeting agenda was effective.
8.22 I was very satisfied with the services provided by the Facilitators.
7.89 I am satisfied with the outcome of the meeting.
7.25 I am satisfied with the progress we are making as a Team.
8.75 I know what the next steps following this meeting will be.
8.75 I know who is responsible for the next steps.

See other side

4. Other comments (use other side)

- Small groups good!
- I'd like the sub-teams to do most work offline rather than taking most of our time in sub-team meetings. We need more time together as a group reviewing each other's work and integrating it.
- The inclusion of additional personnel with operating experience was helpful.
- No space on the other side! Until everyone sees responses from the paper we are doing make-work. I believe our over all direction will change when we see the replays. I am a lemming running over the cliff because the facilitators don't know the subject and history. Jerry, Kevin, Jon D, Philip only know normal IT processes.

What did we achieve?

- Make work
- Concrete work on CIP 002

What are our biggest challenges going forward?

- Finishing the amount of work within time parameters.
- Teaching history.
- A coherent/consistent and clear CIP 002.

What suggestions do you have for making our group more productive?

- Sub-team meetings are difficult without projectors.
- Much work is being done in sub-team Silos. This approach created some of the issues with CIP v1. More coordination is required among the various teams to ensure all issues are addressed but NOT addressed by multiple teams.

Appendix # 4 — NERC Antitrust Compliance Guidelines

I. General

It is NERC's policy and practice to obey the antitrust laws and to avoid all conduct that unreasonably restrains competition. This policy requires the avoidance of any conduct that violates, or that might appear to violate, the antitrust laws. Among other things, the antitrust laws forbid any agreement between or among competitors regarding prices, availability of service, product design, terms of sale, division of markets, allocation of customers or any other activity that unreasonably restrains competition.

It is the responsibility of every NERC participant and employee who may in any way affect NERC's compliance with the antitrust laws to carry out this commitment.

Antitrust laws are complex and subject to court interpretation that can vary over time and from one court to another. The purpose of these guidelines is to alert NERC participants and employees to potential antitrust problems and to set forth policies to be followed with respect to activities that may involve antitrust considerations. In some instances, the NERC policy contained in these guidelines is stricter than the applicable antitrust laws. Any NERC participant or employee who is uncertain about the legal ramifications of a particular course of conduct or who has doubts or concerns about whether NERC's antitrust compliance policy is implicated in any situation should consult NERC's General Counsel immediately.

II. Prohibited Activities

Participants in NERC activities (including those of its committees and Subroups) should refrain from the following when acting in their capacity as participants in NERC activities (e.g., at NERC meetings, conference calls and in informal discussions):

- Discussions involving pricing information, especially margin (profit) and internal cost
- information and participants' expectations as to their future prices or internal costs.
- Discussions of a participant's marketing strategies.
- Discussions regarding how customers and geographical areas are to be divided among competitors.
- Discussions concerning the exclusion of competitors from markets.
- Discussions concerning boycotting or group refusals to deal with competitors, vendors or suppliers.

III. Activities That Are Permitted

From time to time decisions or actions of NERC (including those of its committees and Subroups) may have a negative impact on particular entities and thus in that sense adversely impact competition. Decisions and actions by NERC (including its committees and Subroups)

should only be undertaken for the purpose of promoting and maintaining the reliability and adequacy of the bulk power system. If you do not have a legitimate purpose consistent with this objective for discussing a matter, please refrain from discussing the matter during NERC meetings and in other NERC-related communications.

You should also ensure that NERC procedures, including those set forth in NERC's Certificate of Incorporation and Bylaws are followed in conducting NERC business. Other NERC procedures that may be applicable to a particular NERC activity include the following:

- Reliability Standards Process Manual
- Organization and Procedures Manual for the NERC Standing Committees
- System Operator Certification Program

In addition, all discussions in NERC meetings and other NERC-related communications should be within the scope of the mandate for or assignment to the particular NERC committee or Subroup, as well as within the scope of the published agenda for the meeting.

No decisions should be made nor any actions taken in NERC activities for the purpose of giving an industry participant or group of participants a competitive advantage over other participants. In particular, decisions with respect to setting, revising, or assessing compliance with NERC reliability standards should not be influenced by anti-competitive motivations.

Subject to the foregoing restrictions, participants in NERC activities may discuss:

- Reliability matters relating to the bulk power system, including operation and planning matters such as establishing or revising reliability standards, special operating procedures, operating transfer capabilities, and plans for new facilities.
- Matters relating to the impact of reliability standards for the bulk power system on
- electricity markets, and the impact of electricity market operations on the reliability of the bulk power system.
- Proposed filings or other communications with state or federal regulatory authorities or other governmental entities.
- Matters relating to the internal governance, management and operation of NERC, such as nominations for vacant committee positions, budgeting and assessments, and
- employment matters; and procedural matters such as planning and scheduling meetings.

Any other matters that do not clearly fall within these guidelines should be reviewed with NERC's General Counsel before being discussed.

APPENDIX # 5
Meeting Schedule
October 2008–December 2010

Development of CIP Version 2 and Version 3 Framework
October 2008–July 2009

1. October 6–7, 2008 — Gaithersburg, MD Reviewed CIP-002-CIP-009, Agreed on Version 2 approach.
2. October 20–21 —Sacramento, CA CIP-002-CIP-009 Version 2 development
3. November 12–14, 2008 — Little Rock, AR CIP-002-CIP-009 Version 2 adoption for comment and balloting; CIP-002-CIP-009 Version 3 process reviewed.
4. December 4–5, 2008 — Washington D.C. CIP-002-CIP-009 Version 3 reviewed and debated, SDT member white papers assigned.
5. January 7–9 — Phoenix, AZ, Reviewed Technical Feasibility Exceptions white paper**,** reviewed industry comments on CIP-002-CIP-009 Version 2 products — established small groups to draft responses, reviewed Version 3 white papers.
January 15 — WebEx meeting(s) Small group drafted responses to industry Version 2 comments.
January 21 — WebEx meeting(s) Small group drafted responses to industry Version 2 comments.
6. February 2–4, 2009 — Phoenix, AZ Update on NERC Technical Feasibility Exceptions process**,** VSL process and SDT role**,** review of Version 3 White papers, strawman and principles**,** reviewed and adopted SDT responses to industry comments on Version 2 and Version 2 Product Revisions.
7. February 18–19, 2009 — Fairfax, VA Update on Version 2 process**,** NERC TFE process and VSL Team process; reviewed, discussed and refined Version 3 CIP-002 White papers, strawman, and principles.
8. March 10–11, 2009 — Orlando, FL Update on NERC TFE and VSL and VRF Team process and review and refine Version 3 CIP-002 Strawman Proposals
March 2–April 1, 2009 — 30-day Pre Ballot
Mid-March — NERC posts TFE draft Rules of Procedure for industry comment
March 30, 2009 — WebEx meeting(s) White Paper Drafting Team
April 1–10 — NERC Balloting on Version 2 Products
April 6, 2009 — WebEx meeting — White Paper Drafting Team
April 8, 2009 — WebEx meeting(s) — White Paper Preview- Full SDT Conference Call
April 11, 2009 — Version 2 Ballot Results (Quorum: 91.90% Approval: 84.06%) and Industry Comments-
9. April 14–16, 2009 — Charlotte NC Update on NERC TFE process, VSL Team process and NERC Critical Assets Survey; agreed and adopted responses for Version 2 industry comments for recirculation ballot; reviewed and refined Version 3 whitepaper and consensus points and progress report to NERC Member Representative Committee (MRC) May meeting.
April 28 and May 6, 2009 — White Paper Drafting Team Meetings and WebEx
April 17–27, 2009 — Recirculation Results: Quorum: 94.37% Approval: 88.32%
May 5, 2009 — NERC MRC Meeting, Arlington, VA- SDT progress report.
10. May 13–14, 2009 — Boulder City NV Reviewed MRC presentation and further SDT refinement and discussion of the Version 3 White Paper.
June 8 and June 15, 2009 — Working Paper Drafting Team Meetings and WebEx
11. June 17–18, 2009 — Portland OR Further SDT refinement of the draft CIP Version 3 Working Paper(s), reviewed SDT development process for June-December 2009; discussed potential SDT subcommittee structure and deliverables.
June — WebEx meeting(s)

- Working Paper drafting group sessions including inputs from selected industry personnel to help establish BES categorization criteria

CIP-002 Development of Requirements, Measures, Etc. July-December 2009

12. July 13–14, 2009 in Vancouver, B.C., Canada

- SDT plenary session to review, refine, and adopt SDT Working Paper
- Adopt SDT response to NERC for Interpretation of CIP-006-1
- Review and adopt proposal for CIP-002 Subroups and Deliverables
- Convene Subroup organizational meetings to develop work plans
- Adopt 2010 Meeting Schedule

July–August Interim WebEx meeting(s)

- CIP-002 Subroup meetings (as needed)
- CIP-002 Coordination Team meeting (as needed)

August 3–5, 2009 in Winnipeg, Manitoba **NERC Member Representative Committee**
Progress Report and presentation on new CIP Version 3 Working Paper-Concept- Reliability Standards on Cyber Security for MRC input.

13. August 20–21, 2009 in Charlotte, NC

- SDT Plenary session to review and respond to MRC input on Working Paper/CIP-002 Concepts
- SDT Subroup and plenary meetings to develop CIP-002 requirements and "proof of concept" control (s).

July–September — 45-day Industry Comment Period on CIP-002 Concept Working Paper
NERC Webinar
August–September Interim WebEx meeting(s)

- CIP-002 Subroup meetings (as needed)
- CIP-002 Coordination Team meeting

14. September 9–10, 2009 in Folsom, CA

- SDT plenary session to review and respond to any additional industry comments on Working Paper and CIP-002 Concepts
- SDT Subroup drafting meetings- consider industry comments, draft requirements and "proof of concept" control (s).
- SDT plenary session(s) Subroup reports on requirements
- Review of CIP-002 Standards, Requirements, Measures, and Outline
- Address coordinating issues.
- Establish SDT meeting dates and proposed locations for January–December 2010

September–October Interim WebEx meeting(s)

- CIP-002 Subroup meetings (as needed)
- CIP-002 Coordination Team meeting

15. October 20–22, 2009 in Kansas City, MI

- SDT Subroup drafting meetings — day one
- SDT Plenary Session(s) — day two Subroup reports on CIP-002 requirements
- Review and refine initial draft of CIP-002 single text

October–November Interim WebEx meeting(s)

- CIP-002 Coordination Team meeting

16. November 17–19, 2009 in Orlando, FL

- SDT plenary session(s) — to review and refine CIP-002 standard, requirements, measures and controls.

November–December Interim WebEx meeting(s)
- Drafting teams as needed to finalize drafts
- CIP-002 Coordination Team meeting

17. December 15–16, 2009 in Little Rock AK
- SDT plenary session(s) to review, refine, and agree on and adopt CIP-002 standard, requirements, measures and controls.
- Agree on initial posting of draft CIP-002 for industry review and comment.

Refinement of CIP-002 and Development of Other CIP Standards
January–December 2010
(12 SDT monthly meetings and Subroup WebEx meetings as needed)

- SDT responds to industry comments on initial and subsequent postings of CIP-002, Version 3 (may be multiple comment periods, as required)
- Refine the CIP-002 through the comment period and submit new CIP-002 Version 3 Standard for Balloting along with the catalogue of controls (i.e. CIP-003-CIP-009 or its successor) OR
- Ballot CIP-002 while permitting industry to rely on CIP 003-CIP-009 until the full suite of controls (i.e. CIP-003-CIP-009 or its successor) is reviewed and presented for balloting.
- Submit the full suite of CIP Reliability Standards on Cyber Security for Industry Comment
- Refine and Submit the full suite of CIP standards for industry ballot
- NERC Board of Trustees adoption of the full suite of standards
- FERC approves and NERC Implements the full suite of CIP standards

Proposed 2010 Meeting Schedule

18. January 20–21 — Wednesday–Thursday, Atlanta GA	24. July 14–15, Wednesday–Thursday
19. February 18–19 —Thursday –Friday, Austin TX	25. August 11–12, Wednesday–Thursday
20. March 9–11 — Tuesday–Thursday, Phoenix, AZ	26. September 8–9, Wednesday–Thursday
21. April 14–15 — Wednesday–Thursday, Atlanta GA	27. Oct. 13–14, Wednesday–Thursday or Oct.12–14
22. May 12–13 — Wednesday–Thursday, Dallas TX	28. November 17–18, Wednesday–Thursday
23. June 9–10 — Wednesday–Thursday, Sacramento CA	29. December 15–16, Wednesday–Thursday

Appendix # 6

Technical Feasibility Exceptions
Matrix of Applicable Requirements

CIP-002-1/R1	Critical Asset Identification Method — The Responsible Entity shall identify and document a risk-based assessment methodology to use to identify its Critical Assets.	No exceptions
CIP-002-1/R1.1	The Responsible Entity shall maintain documentation describing its risk-based assessment methodology that includes procedures and evaluation criteria.	No exceptions
CIP-002-1/R1.2	The risk-based assessment shall consider the following assets: • Control centers and backup control centers performing the functions of the entities listed in the Applicability section of this standard. • Transmission substations that support the reliable operation of the Bulk Electric System. • Generation resources that support the reliable operation of the Bulk Electric System. • Systems and facilities critical to system restoration, including blackstart generators and substations in the electrical path of transmission lines used for initial system restoration. • Systems and facilities critical to automatic load shedding under a common control system capable of shedding 300 MW or more. • Special Protection Systems that support the reliable operation of the Bulk Electric System. • Any additional assets that support the reliable operation of the Bulk Electric System that the Responsible Entity deems appropriate to include in its assessment.	No exceptions
CIP-002-1/R2	Critical Asset Identification — The Responsible Entity shall develop a list of its identified Critical Assets determined through an annual application of the risk-based assessment methodology required in R1. The Responsible Entity shall review this list at least annually, and update it as necessary.	No exceptions
CIP-002-1/R3	Critical Cyber Asset Identification — Using the list of Critical Assets developed pursuant to Requirement R2, the Responsible Entity shall develop a list of associated Critical Cyber Assets essential to the operation of the Critical Asset. Examples at control centers and backup control centers include systems and facilities at master and remote sites that provide monitoring and control, automatic generation control, real-time power system modeling, and real-time inter-utility data exchange. The Responsible Entity shall review this list at least annually, and update it as necessary. For the purpose of Standard CIP-002, Critical Cyber Assets are further qualified to be those having at least one of the following characteristics: • The Cyber Asset uses a routable protocol to communicate outside the Electronic Security Perimeter; or, • The Cyber Asset uses a routable protocol within a control center; or, • The Cyber Asset is dial-up accessible.	No exceptions

CIP-002-1/R4	Annual Approval — A senior manager or delegate(s) shall approve annually the list of Critical Assets and the list of Critical Cyber Assets. Based on Requirements R1, R2, and R3 the Responsible Entity may determine that it has no Critical Assets or Critical Cyber Assets. The Responsible Entity shall keep a signed and dated record of the senior manager or delegate(s)'s approval of the list of Critical Assets and the list of Critical Cyber Assets (even if such lists are null.)	No exceptions
CIP-003-1/R1	Cyber Security Policy — The Responsible Entity shall document and implement a cyber security policy that represents management's commitment and ability to secure its Critical Cyber Assets. The Responsible Entity shall, at minimum, ensure the following:	No exceptions
CIP-003-1/R1.1	The cyber security policy addresses the requirements in Standards CIP-002 through CIP-009, including provision for emergency situations.	No exceptions
CIP-003-1/R1.2	The cyber security policy is readily available to all personnel who have access to, or are responsible for, Critical Cyber Assets.	No exceptions
CIP-003-1/R1.3	Annual review and approval of the cyber security policy by the senior manager assigned pursuant to R2.	No exceptions
CIP-003-1/R2	Leadership — The Responsible Entity shall assign a senior manager with overall responsibility for leading and managing the entity's implementation of, and adherence to, Standards CIP-002 through CIP-009.	No exceptions
CIP-003-1/R2.1	The senior manager shall be identified by name, title, business phone, business address, and date of designation.	No exceptions
CIP-003-1/R2.2	Changes to the senior manager must be documented within thirty calendar days of the effective date.	No exceptions
CIP-003-1/R2.3	The senior manager or delegate(s), shall authorize and document any exception from the requirements of the cyber security policy.	No exceptions
CIP-003-1/R3	Exceptions — Instances where the Responsible Entity cannot conform to its cyber security policy must be documented as exceptions and authorized by the senior manager or delegate(s).	No exceptions
CIP-003-1/R3.1	Exceptions to the Responsible Entity's cyber security policy must be documented within thirty days of being approved by the senior manager or delegate(s).	No exceptions
CIP-003-1/R3.2	Documented exceptions to the cyber security policy must include an explanation as to why the exception is necessary and any compensating measures, or a statement accepting risk.	No exceptions
CIP-003-1/R3.3	Authorized exceptions to the cyber security policy must be reviewed and approved annually by the senior manager or delegate(s) to ensure the exceptions are still required and valid. Such review and approval shall be documented.	No exceptions
CIP-003-1/R4	Information Protection — The Responsible Entity shall implement and document a program to identify, classify, and protect information associated with Critical Cyber Assets.	No exceptions
CIP-003-1/R4.1	The Critical Cyber Asset information to be protected shall include, at a minimum and regardless of media type, operational procedures, lists as required in Standard CIP-002, network topology or similar diagrams, floor plans of computing centers that contain Critical Cyber Assets, equipment layouts of Critical Cyber Assets, disaster recovery plans, incident response plans, and	No exceptions

	security configuration information.	
CIP-003-1/R4.2	The Responsible Entity shall classify information to be protected under this program based on the sensitivity of the Critical Cyber Asset information.	No exceptions
CIP-003-1/R4.3	The Responsible Entity shall, at least annually, assess adherence to its Critical Cyber Asset information protection program, document the assessment results, and implement an action plan to remediate deficiencies identified during the assessment.	No exceptions
CIP-003-1/R5	Access Control — The Responsible Entity shall document and implement a program for managing access to protected Critical Cyber Asset information.	No exceptions
CIP-003-1/R5.1	Responsible Entity shall maintain a list of designated personnel who are responsible for authorizing logical or physical access to protected information.	No exceptions
CIP-003-1/R5.1.1	Personnel shall be identified by name, title, business phone and the information for which they are responsible for authorizing access.	No exceptions
CIP-003-1/R5.1.2	The list of personnel responsible for authorizing access to protected information shall be verified at least annually.	No exceptions
CIP-003-1/R5.2	The Responsible Entity shall review at least annually the access privileges to protected information to confirm that access privileges are correct and that they correspond with the Responsible Entity's needs and appropriate personnel roles and responsibilities.	No exceptions
CIP-003-1/R5.3	The Responsible Entity shall assess and document at least annually the processes for controlling access privileges to protected information.	No exceptions
CIP-003-1/R6	Change Control and Configuration Management — The Responsible Entity shall establish and document a process of change control and configuration management for adding, modifying, replacing, or removing Critical Cyber Asset hardware or software, and implement supporting configuration management activities to identify, control and document all entity or vendor-related changes to hardware and software components of Critical Cyber Assets pursuant to the change control process.	No exceptions
CIP-004-1/R1	Awareness — The Responsible Entity shall establish, maintain, and document a security awareness program to ensure personnel having authorized cyber or authorized unescorted physical access receive on-going reinforcement in sound security practices. The program shall include security awareness reinforcement on at least a quarterly basis using mechanisms such as: • Direct communications (e.g., emails, memos, computer based training, etc.); • Indirect communications (e.g., posters, intranet, brochures, etc.); • Management support and reinforcement (e.g., presentations, meetings, etc.).	No exceptions
CIP-004-1/R2	Training — The Responsible Entity shall establish, maintain, and document an annual cyber security training program for personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets, and review the program annually and update as necessary.	No exceptions
CIP-004-1/R2.1	This program will ensure that all personnel having such access to Critical Cyber Assets, including contractors and service vendors, are trained within ninety calendar days of such authorization.	No exceptions

CIP-004-1/R2.2	Training shall cover the policies, access controls, and procedures as developed for the Critical Cyber Assets covered by CIP-004, and include, at a minimum, the following required items appropriate to personnel roles and responsibilities: • The proper use of Critical Cyber Assets; • Physical and electronic access controls to Critical Cyber Assets; • The proper handling of Critical Cyber Asset information; and, • Action plans and procedures to recover or re-establish Critical Cyber Assets and access thereto following a Cyber Security Incident.	No exceptions
CIP-004-1/R2.3	Responsible Entity shall maintain documentation that training is conducted at least annually, including the date the training was completed and attendance records.	No exceptions
CIP-004-1/R3	Personnel Risk Assessment —The Responsible Entity shall have a documented personnel risk assessment program, in accordance with federal, state, provincial, and local laws, and subject to existing collective bargaining unit agreements, for personnel having authorized cyber or authorized unescorted physical access. A personnel risk assessment shall be conducted pursuant to that program within thirty days of such personnel being granted such access. Such program shall at a minimum include:	Exception permitted for statutory restrictions. Exception permitted for collective bargaining agreement if entity can demonstrate good faith effort to negotiate this requirement into the contract.
CIP-004-1/R3.1	The Responsible Entity shall ensure that each assessment conducted include, at least, identity verification (e.g., Social Security Number verification in the U.S.) and seven-year criminal check. The Responsible Entity may conduct more detailed reviews, as permitted by law and subject to existing collective bargaining unit agreements, depending upon the criticality of the position.	Exception inherited from CIP-004-1/R3 criteria. No exception required for more detailed background check – optional component of the requirement.
CIP-004-1/R3.2	The Responsible Entity shall update each personnel risk assessment at least every seven years after the initial personnel risk assessment or for cause.	Exception inherited from CIP-004-1/R3 criteria.
CIP-004-1/R3.3	Responsible Entity shall document the results of personnel risk assessments of its personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets, and that personnel risk assessments of contractor and service vendor personnel with such access are conducted pursuant to Standard CIP-004.	Exception inherited from CIP-004-1/R3 criteria.
CIP-004-1/R4	Access — The Responsible Entity shall maintain list(s) of personnel with authorized cyber or authorized unescorted physical access to Critical Cyber Assets, including their specific electronic and physical access rights to Critical Cyber Assets.	No exceptions
CIP-004-1/R4.1	The Responsible Entity shall review the list(s) of its personnel who have such access to Critical Cyber Assets quarterly, and update the list(s) within seven calendar days of any change of personnel with such access to Critical Cyber	No exceptions.

	Assets, or any change in the access rights of such personnel. The Responsible Entity shall ensure access list(s) for contractors and service vendors are properly maintained.	
CIP-004-1/R4.2	The Responsible Entity shall revoke such access to Critical Cyber Assets within 24 hours for personnel terminated for cause and within seven calendar days for personnel who no longer require such access to Critical Cyber Assets.	No exceptions.
CIP-005-1/R1	Electronic Security Perimeter — The Responsible Entity shall ensure that every Critical Cyber Asset resides within an Electronic Security Perimeter. The Responsible Entity shall identify and document the Electronic Security Perimeter(s) and all access points to the perimeter(s).	Exceptions inherited from CIP-005-1/R1.5 criteria. Note exemption (see CIP-005-1/R1.2 and explanatory information in the FAQ) for a Critical Cyber Asset that does not use a routable protocol and is only dial-up accessible.
CIP-005-1/R1.1	Access points to the Electronic Security Perimeter(s) shall include any externally connected communication end point (for example, dial-up modems) terminating at any device within the Electronic Security Perimeter(s).	No exceptions.
CIP-005-1/R1.2	For a dial-up accessible Critical Cyber Asset that uses a non-routable protocol, the Responsible Entity shall define an Electronic Security Perimeter for that single access point at the dial-up device.	No exceptions.
CIP-005-1/R1.3	Communication links connecting discrete Electronic Security Perimeters shall not be considered part of the Electronic Security Perimeter. However, end points of these communication links within the Electronic Security Perimeter(s) shall be considered access points to the Electronic Security Perimeter(s).	No exceptions.
CIP-005-1/R1.4	Any non-critical Cyber Asset within a defined Electronic Security Perimeter shall be identified and protected pursuant to the requirements of Standard CIP-005.	No exceptions.
CIP-005-1/R1.5	Cyber Assets used in the access control and monitoring of the Electronic Security Perimeter(s) shall be afforded the protective measures as a specified in Standard CIP-003, Standard CIP-004 Requirement R3, Standard CIP-005 Requirements R2 and R3, Standard CIP-006 Requirements R2 and R3, Standard CIP-007, Requirements R1 and R3 through R9, Standard CIP-008, and Standard CIP-009.	Exception criteria inherited from the referenced requirements that the applicable Cyber Assets are subject to.
CIP-005-1/R1.6	The Responsible Entity shall maintain documentation of Electronic Security Perimeter(s), all interconnected Critical and non-critical Cyber Assets within the Electronic Security Perimeter(s), all electronic access points to the Electronic Security Perimeter(s) and the Cyber Assets deployed for the access control and monitoring of these access points.	No exceptions.
CIP-005-1/R2	Electronic Access Controls — The Responsible Entity shall implement and document the organizational processes and technical and procedural mechanisms for control of electronic access at all electronic access points to the Electronic Security Perimeter(s).	No exceptions.
CIP-005-1/R2.1	These processes and mechanisms shall use an access control model that denies	Exception permitted where access control

	access by default, such that explicit access permissions must be specified.	rule set does not provide for "deny by default."
CIP-005-1/R2.2	At all access points to the Electronic Security Perimeter(s), the Responsible Entity shall enable only ports and services required for operations and for monitoring Cyber Assets within the Electronic Security Perimeter, and shall document, individually or by specified grouping, the configuration of those ports and services.	Exception permitted where ports and services cannot be configured.
CIP-005-1/R2.3	The Responsible Entity shall maintain a procedure for securing dial-up access to the Electronic Security Perimeter(s).	No exceptions.
CIP-005-1/R2.4	Where external interactive access into the Electronic Security Perimeter has been enabled, the Responsible Entity shall implement strong procedural or technical controls at the access points to ensure authenticity of the accessing party, where technically feasible.	Exception permitted for technical infeasibility.
CIP-005-1/R2.5	The required documentation shall, at least, identify and describe: • The processes for access request and authorization. • The authentication methods. • The review process for authorization rights, in accordance with Standard CIP-004 Requirement R4. • The controls used to secure dial-up accessible connections.	No exceptions.
CIP-005-1/R2.6	Appropriate Use Banner — Where technically feasible, electronic access control devices shall display an appropriate use banner on the user screen upon all interactive access attempts. The Responsible Entity shall maintain a document identifying the content of the banner.	Exception permitted for technical infeasibility.
CIP-005-1/R3	Monitoring Electronic Access — The Responsible Entity shall implement and document an electronic or manual process(es) for monitoring and logging access at access points to the Electronic Security Perimeter(s) twenty-four hours a day, seven days a week.	Exceptions permitted for technical infeasibility of sub requirements R3.1 and/or R3.2 only.
CIP-005-1/R3.1	For dial-up accessible Critical Cyber Assets that use non-routable protocols, the Responsible Entity shall implement and document monitoring process(es) at each access point to the dial-up device, where technically feasible.	Exception permitted for technical infeasibility.
CIP-005-1/R3.2	Where technically feasible, the security monitoring process(es) shall detect and alert for attempts at or actual unauthorized accesses. These alerts shall provide for appropriate notification to designated response personnel. Where alerting is not technically feasible, the Responsible Entity shall review or otherwise assess access logs for attempts at or actual unauthorized accesses at least every ninety calendar days.	Exception permitted for technical infeasibility.
CIP-005-1/R4	Cyber Vulnerability Assessment — The Responsible Entity shall perform a cyber vulnerability assessment of the electronic access points to the Electronic Security Perimeter(s) at least annually. The vulnerability assessment shall include, at a minimum, the following:	Exceptions inherited from CIP-005-1/R4.2 and R4.3 criteria.
CIP-005-1/R4.1	A document identifying the vulnerability assessment process;	No exceptions.
CIP-005-1/R4.2	A review to verify that only ports and services required for operations at these access points are enabled;	Exception inherited from CIP-005-1/R2.2.

CIP-005-1/R4.3	The discovery of all access points to the Electronic Security Perimeter;	Exception permitted if the only means to discover all ESP access points is an active scan of the network segment and such a scan would put the Critical Cyber Assets at risk.
CIP-005-1/R4.4	A review of controls for default accounts, passwords, and network management community strings; and,	No exceptions.
CIP-005-1/R4.5	Documentation of the results of the assessment, the action plan to remediate or mitigate vulnerabilities identified in the assessment, and the execution status of that action plan.	No exceptions.
CIP-005-1/R5	Documentation Review and Maintenance — The Responsible Entity shall review, update, and maintain all documentation to support compliance with the requirements of Standard CIP-005.	No exceptions.
CIP-005-1/R5.1	The Responsible Entity shall ensure that all documentation required by Standard CIP-005 reflect current configurations and processes and shall review the documents and procedures referenced in Standard CIP-005 at least annually.	No exceptions.
CIP-005-1/R5.2	The Responsible Entity shall update the documentation to reflect the modification of the network or controls within ninety calendar days of the change.	No exceptions.
CIP-005-1/R5.3	The Responsible Entity shall retain electronic access logs for at least ninety calendar days. Logs related to reportable incidents shall be kept in accordance with the requirements of Standard CIP-008.	Exception permitted if logs cannot be offloaded from the logging device, there is no alternative to the logging device, and the device cannot retain logs for the prescribed period of time.
CIP-006-1/R1	Physical Security Plan — The Responsible Entity shall create and maintain a physical security plan, approved by a senior manager or delegate(s) that shall address, at a minimum, the following:	Exceptions inherited from CIP-006-1/R1.1 and R1.8 criteria.
CIP-006-1/R1.1	Processes to ensure and document that all Cyber Assets within an Electronic Security Perimeter also reside within an identified Physical Security Perimeter. Where a completely enclosed (“six-wall”) border cannot be established, the Responsible Entity shall deploy and document alternative measures to control physical access to the Critical Cyber Assets.	Exception permitted when completely enclosed (“six wall”) border cannot be established and alternative protective measures are implemented. Complete exception from the requirement is not permitted.
CIP-006-1/R1.2	Processes to identify all access points through each Physical Security Perimeter	No exceptions.

	and measures to control entry at those access points.	
CIP-006-1/R1.3	Processes, tools, and procedures to monitor physical access to the perimeter(s).	No exceptions.
CIP-006-1/R1.4	Procedures for the appropriate use of physical access controls as described in Requirement R3 including visitor pass management, response to loss, and prohibition of inappropriate use of physical access controls.	No exceptions.
CIP-006-1/R1.5	Procedures for reviewing access authorization requests and revocation of access authorization, in accordance with CIP-004 Requirement R4.	No exceptions.
CIP-006-1/R1.6	Procedures for escorted access within the physical security perimeter of personnel not authorized for unescorted access.	No exceptions.
CIP-006-1/R1.7	Process for updating the physical security plan within ninety calendar days of any physical security system redesign or reconfiguration, including, but not limited to, addition or removal of access points through the physical security perimeter, physical access controls, monitoring controls, or logging controls.	No exceptions.
CIP-006-1/R1.8	Cyber Assets used in the access control and monitoring of the Physical Security Perimeter(s) shall be afforded the protective measures specified in Standard CIP-003, Standard CIP-004 Requirement R3, Standard CIP-005 Requirements R2 and R3, Standard CIP-006 Requirement R2 and R3, Standard CIP-007, Standard CIP-008 and Standard CIP-009.	Exception criteria inherited from the referenced requirements that the applicable Cyber Assets are subject to.
CIP-006-1/R1.9	Process for ensuring that the physical security plan is reviewed at least annually.	No exceptions.
CIP-006-1/R2	Physical Access Controls — The Responsible Entity shall document and implement the operational and procedural controls to manage physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week. The Responsible Entity shall implement one or more of the following physical access methods: • Card Key: A means of electronic access where the access rights of the card holder are predefined in a computer database. Access rights may differ from one perimeter to another. • Special Locks: These include, but are not limited to, locks with "restricted key" systems, magnetic locks that can be operated remotely, and "man-trap" systems. • Security Personnel: Personnel responsible for controlling physical access who may reside on-site or at a monitoring station. • Other Authentication Devices: Biometric, keypad, token, or other equivalent devices that control physical access to the Critical Cyber Assets.	No exceptions.
CIP-006-1/R3	Monitoring Physical Access — The Responsible Entity shall document and implement the technical and procedural controls for monitoring physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week. Unauthorized access attempts shall be reviewed immediately and handled in accordance with the procedures specified in Requirement CIP-008. One or more of the following monitoring methods shall be used: • Alarm Systems: Systems that alarm to indicate a door, gate or window has been opened without authorization. These alarms must provide for immediate notification to personnel responsible for response. • Human Observation of Access Points: Monitoring of physical access	No exceptions.

	points by authorized personnel as specified in Requirement R2.3.	
CIP-006-1/R4	Logging Physical Access — Logging shall record sufficient information to uniquely identify individuals and the time of access twenty-four hours a day, seven days a week. The Responsible Entity shall implement and document the technical and procedural mechanisms for logging physical entry at all access points to the Physical Security Perimeter(s) using one or more of the following logging methods or their equivalent: • Computerized Logging: Electronic logs produced by the Responsible Entity's selected access control and monitoring method. • Video Recording: Electronic capture of video images of sufficient quality to determine identity. • Manual Logging: A log book or sign-in sheet, or other record of physical access maintained by security or other personnel authorized to control and monitor physical access as specified in Requirement R2.3.	No exceptions.
CIP-006-1/R5	Access Log Retention — The responsible entity shall retain physical access logs for at least ninety calendar days. Logs related to reportable incidents shall be kept in accordance with the requirements of Standard CIP-008.	No exceptions.
CIP-006-1/R6	Maintenance and Testing — The Responsible Entity shall implement a maintenance and testing program to ensure that all physical security systems under Requirements R2, R3, and R4 function properly. The program must include, at a minimum, the following:	No exceptions.
CIP-006-1/R6.1	Testing and maintenance of all physical security mechanisms on a cycle no longer than three years.	No exceptions.
CIP-006-1/R6.2	Retention of testing and maintenance records for the cycle determined by the Responsible Entity in Requirement R6.1.	No exceptions.
CIP-006-1/R6.3	Retention of outage records regarding access controls, logging, and monitoring for a minimum of one calendar year.	No exceptions.
CIP-007-1/R1	Test Procedures — The Responsible Entity shall ensure that new Cyber Assets and significant changes to existing Cyber Assets within the Electronic Security Perimeter do not adversely affect existing cyber security controls. For purposes of Standard CIP-007, a significant change shall, at a minimum, include implementation of security patches, cumulative service packs, vendor releases, and version upgrades of operating systems, applications, database platforms, or other third-party software or firmware.	Exception permitted for technical infeasibility if no offline testing environment can be established. Offline test environments can include stand-by production and DR systems as well as more traditional test environments. Typically, the permitted exception will be limited to plant and possibly substation control systems. Network management environments (switches, firewalls, domain controllers)

		might also qualify for an exception.
CIP-007-1/R1.1	The Responsible Entity shall create, implement, and maintain cyber security test procedures in a manner that minimizes adverse effects on the production system or its operation.	No exceptions.
CIP-007-1/R1.2	The Responsible Entity shall document that testing is performed in a manner that reflects the production environment.	Exception permitted to the extent the production environment cannot be replicated. See CIP-007-1/R1 exception comments.
CIP-007-1/R1.3	The Responsible Entity shall document test results.	No exceptions.
CIP-007-1/R2	Ports and Services — The Responsible Entity shall establish and document a process to ensure that only those ports and services required for normal and emergency operations are enabled.	Exception permitted where ports and services cannot be configured.
CIP-007-1/R2.1	The Responsible Entity shall enable only those ports and services required for normal and emergency operations.	Exception permitted where ports and services cannot be configured.
CIP-007-1/R2.2	The Responsible Entity shall disable other ports and services, including those used for testing purposes, prior to production use of all Cyber Assets inside the Electronic Security Perimeter(s).	Exception permitted where ports and services cannot be configured.
CIP-007-1/R2.3	In the case where unused ports and services cannot be disabled due to technical limitations, the Responsible Entity shall document compensating measure(s) applied to mitigate risk exposure or an acceptance of risk.	No exceptions.
CIP-007-1/R3	Security Patch Management — The Responsible Entity, either separately or as a component of the documented configuration management process specified in CIP-003 Requirement R6, shall establish and document a security patch management program for tracking, evaluating, testing, and installing applicable cyber security software patches for all Cyber Assets within the Electronic Security Perimeter(s).	No exception
CIP-007-1/R3.1	The Responsible Entity shall document the assessment of security patches and security upgrades for applicability within thirty calendar days of availability of the patches or upgrades.	No exceptions.
CIP-007-1/R3.2	The Responsible Entity shall document the implementation of security patches. In any case where the patch is not installed, the Responsible Entity shall document compensating measure(s) applied to mitigate risk exposure or an acceptance of risk.	Exception permitted when security patch cannot be implemented for technical reasons. Compensating measures MUST be applied per the requirement. The exception only applies to the inability to apply

		the security patch itself. Note, need to consider the case where the system vendor declines to support the system if unapproved patches are installed. Is this a valid reason for a TFE?
CIP-007-1/R4	Malicious Software Prevention — The Responsible Entity shall use anti-virus software and other malicious software ("malware") prevention tools, where technically feasible, to detect, prevent, deter, and mitigate the introduction, exposure, and propagation of malware on all Cyber Assets within the Electronic Security Perimeter(s).	Exception permitted for technical infeasibility.
CIP-007-1/R4.1	The Responsible Entity shall document and implement anti-virus and malware prevention tools. In the case where anti-virus software and malware prevention tools are not installed, the Responsible Entity shall document compensating measure(s) applied to mitigate risk exposure or an acceptance of risk.	Exception permitted for technical infeasibility.
CIP-007-1/R4.2	The Responsible Entity shall document and implement a process for the update of anti-virus and malware prevention "signatures." The process must address testing and installing the signatures.	Exceptions inherited from CIP-007-1/R4.1 criteria.
CIP-007-1/R5	Account Management — The Responsible Entity shall establish, implement, and document technical and procedural controls that enforce access authentication of, and accountability for, all user activity, and that minimize the risk of unauthorized system access.	No exception.
CIP-007-1/R5.1	The Responsible Entity shall ensure that individual and shared system accounts and authorized access permissions are consistent with the concept of "need to know" with respect to work functions performed.	No exception.
CIP-007-1/R5.1.1	The Responsible Entity shall ensure that user accounts are implemented as approved by designated personnel. Refer to Standard CIP-003 Requirement R5.	No exception.
CIP-007-1/R5.1.2	The Responsible Entity shall establish methods, processes, and procedures that generate logs of sufficient detail to create historical audit trails of individual user account access activity for a minimum of ninety days.	No exceptions.
CIP-007-1/R5.1.3	The Responsible Entity shall review, at least annually, user accounts to verify access privileges are in accordance with Standard CIP-003 Requirement R5 and Standard CIP-004 Requirement R4.	No exceptions.
CIP-007-1/R5.2	The Responsible Entity shall implement a policy to minimize and manage the scope and acceptable use of administrator, shared, and other generic account privileges including factory default accounts.	No exceptions.
CIP-007-1/R5.2.1	The policy shall include the removal, disabling, or renaming of such accounts where possible. For such accounts that must remain enabled, passwords shall be changed prior to putting any system into service.	No exceptions.
CIP-007-1/R5.2.2	The Responsible Entity shall identify those individuals with access to shared accounts.	No exceptions.
CIP-007-1/R5.2.3	Where such accounts must be shared, the Responsible Entity shall have a policy	No exceptions.

	for managing the use of such accounts that limits access to only those with authorization, an audit trail of the account use (automated or manual), and steps for securing the account in the event of personnel changes (for example, change in assignment or termination).	
CIP-007-1/R5.3	At a minimum, the Responsible Entity shall require and use passwords, subject to the following, as technically feasible:	Exceptions inherited from CIP-007-1/R5.3.1 and R5.3.2 criteria.
CIP-007-1/R5.3.1	Each password shall be a minimum of six characters.	Exception permitted for technical infeasibility.
CIP-007-1/R5.3.2	Each password shall consist of a combination of alpha, numeric, and "special" characters.	Exception permitted for technical infeasibility.
CIP-007-1/R5.3.3	Each password shall be changed at least annually, or more frequently based on risk.	No exception.
CIP-007-1/R6	Security Status Monitoring — The Responsible Entity shall ensure that all Cyber Assets within the Electronic Security Perimeter, as technically feasible, implement automated tools or organizational process controls to monitor system events that are related to cyber security.	Exceptions inherited from CIP-007-1/R6.3 and R6.4 criteria.
CIP-007-1/R6.1	The Responsible Entity shall implement and document the organizational processes and technical and procedural mechanisms for monitoring for security events on all Cyber Assets within the Electronic Security Perimeter.	No exceptions.
CIP-007-1/R6.2	The security monitoring controls shall issue automated or manual alerts for detected Cyber Security Incidents.	No exception.
CIP-007-1/R6.3	The Responsible Entity shall maintain logs of system events related to cyber security, where technically feasible, to support incident response as required in Standard CIP-008.	Exception permitted for technical infeasibility.
CIP-007-1/R6.4	The Responsible Entity shall retain all logs specified in Requirement R6 for ninety calendar days.	Exception inherited from CIP-007-1/R6.3 criteria.
CIP-007-1/R6.5	The Responsible Entity shall review logs of system events related to cyber security and maintain records documenting review of logs.	No exceptions.
CIP-007-1/R7	Disposal or Redeployment — The Responsible Entity shall establish formal methods, processes, and procedures for disposal or redeployment of Cyber Assets within the Electronic Security Perimeter(s) as identified and documented in Standard CIP-005.	No exceptions.
CIP-007-1/R7.1	Prior to the disposal of such assets, the Responsible Entity shall destroy or erase the data storage media to prevent unauthorized retrieval of sensitive cyber security or reliability data.	No exceptions.
CIP-007-1/R7.2	Prior to redeployment of such assets, the Responsible Entity shall, at a minimum, erase the data storage media to prevent unauthorized retrieval of sensitive cyber security or reliability data.	No exceptions.
CIP-007-1/R7.3	The Responsible Entity shall maintain records that such assets were disposed of or redeployed in accordance with documented procedures.	No exceptions.

CIP-007-1/R8	Cyber Vulnerability Assessment — The Responsible Entity shall perform a cyber vulnerability assessment of all Cyber Assets within the Electronic Security Perimeter at least annually. The vulnerability assessment shall include, at a minimum, the following:	Exception inherited from CIP-007-1/R8.2 criteria.
CIP-007-1/R8.1	A document identifying the vulnerability assessment process;	No exceptions.
CIP-007-1/R8.2	A review to verify that only ports and services required for operation of the Cyber Assets within the Electronic Security Perimeter are enabled;	Exception inherited from CIP-005-1/R2.2 and CIP-007-1/R2, R2.1, and R2.2.
CIP-007-1/R8.3	A review of controls for default accounts; and,	No exceptions.
CIP-007-1/R8.4	Documentation of the results of the assessment, the action plan to remediate or mitigate vulnerabilities identified in the assessment, and the execution status of that action plan.	No exceptions.
CIP-007-1/R9	Documentation Review and Maintenance — The Responsible Entity shall review and update the documentation specified in Standard CIP-007 at least annually. Changes resulting from modifications to the systems or controls shall be documented within ninety calendar days of the change.	No exceptions.
CIP-008-1/R1	Cyber Security Incident Response Plan — The Responsible Entity shall develop and maintain a Cyber Security Incident response plan. The Cyber Security Incident Response plan shall address, at a minimum, the following:	No exceptions.
CIP-008-1/R1.1	Procedures to characterize and classify events as reportable Cyber Security Incidents.	No exceptions.
CIP-008-1/R1.2	Response actions, including roles and responsibilities of incident response teams, incident handling procedures, and communication plans.	No exceptions.
CIP-008-1/R1.3	Process for reporting Cyber Security Incidents to the Electricity Sector Information Sharing and Analysis Center (ES ISAC). The Responsible Entity must ensure that all reportable Cyber Security Incidents are reported to the ES ISAC either directly or through an intermediary.	No exceptions.
CIP-008-1/R1.4	Process for updating the Cyber Security Incident response plan within ninety calendar days of any changes.	No exceptions.
CIP-008-1/R1.5	Process for ensuring that the Cyber Security Incident response plan is reviewed at least annually.	No exceptions.
CIP-008-1/R1.6	Process for ensuring the Cyber Security Incident response plan is tested at least annually. A test of the incident response plan can range from a paper drill, to a full operational exercise, to the response to an actual incident.	No exceptions.
CIP-008-1/R2	Cyber Security Incident Documentation — The Responsible Entity shall keep relevant documentation related to Cyber Security Incidents reportable per Requirement R1.1 for three calendar years.	No exceptions.
CIP-009-1/R1	Recovery Plans — The Responsible Entity shall create and annually review recovery plan(s) for Critical Cyber Assets. The recovery plan(s) shall address at a minimum the following:	No exceptions.
CIP-009-1/R1.1	Specify the required actions in response to events or conditions of varying duration and severity that would activate the recovery plan(s).	No exceptions.

CIP-009-1/R1.2	Define the roles and responsibilities of responders.	No exceptions.
CIP-009-1/R2	Exercises — The recovery plan(s) shall be exercised at least annually. An exercise of the recovery plan(s) can range from a paper drill, to a full operational exercise, to recovery from an actual incident.	No exceptions.
CIP-009-1/R3	Change Control — Recovery plan(s) shall be updated to reflect any changes or lessons learned as a result of an exercise or the recovery from an actual incident. Updates shall be communicated to personnel responsible for the activation and implementation of the recovery plan(s) within ninety calendar days of the change.	No exceptions.
CIP-009-1/R4	Backup and Restore — The recovery plan(s) shall include processes and procedures for the backup and storage of information required to successfully restore Critical Cyber Assets. For example, backups may include spare electronic components or equipment, written documentation of configuration settings, tape backup, etc.	No exceptions.
CIP-009-1/R5	Testing Backup Media — Information essential to recovery that is stored on backup media shall be tested at least annually to ensure that the information is available. Testing can be completed off site.	Exception permitted for technical infeasibility when there is no ability to create a suitable test environment to restore the backup information to.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Meeting Agenda

Cyber Security Order 706 SDT — Project 2008-06

Thursday, August 20, 2009 | 8:00 a.m. – 5:00 p.m. EDT
Friday, August 21, 2009 | 8:00 a.m. – 3:30 p.m. EDT
Charlotte, North Carolina

Proposed Meeting Objectives and Outcomes

- Review the work plan going forward;
- Receive update on the MRC presentation and Leaders Coordination call;
- Receive updates on TFE, VSL/VRF and related cyber security efforts;
- Receive and discuss reports from CIP 002 Subgroups;
- Convene CIP 002 Subgroup meetings;
- Subgroup reports back to SDT; and
- Agree on work plan, next steps and assignments.

Thursday August 20, 2009
8:00 a.m. – 12:45 p.m.

1. **Review of CIP 002 Workplan and Subgroup Process including pros – cons of a possible TFE Exception "Version 2.5" — Kevin Perry and Jerry Freese' Version 2.5 Proposal**

2. **Update on Technical Feasibility Exception (TFE) NERC Rules of Procedure and VSLs – VRFs**

3. **Subgroup Reports to the SDT**
   - Reliability Functions Subgroup Report
   - List of BES Subsystems/BES Cyber systems Subgroup Report
   - BES Mapping Subgroup Report
   - Cyber Analysis Subgroup Report
   - Definition and Selection of Controls Subgroup Report

1:15 p.m. – 5:00 p.m.

1. **Subgroup Meetings *(at various locations)***
2. **Adjourn**

116-390 Village Blvd.
Princeton, NJ 08540
609.452.8060 | www.nerc.com

Friday August 21, 2009
8:00 a.m. – 12:30 p.m.

1. **Subgroup Meetings**

12:30 p.m. – 3:00 p.m.

1. **Subgroup Reports – Plenary Session**
    - Reliability Functions Subgroup Report, Q & A
    - List of BES Subsystems/BES Cyber systems Subgroup Report, Q & A
    - BES Mapping Subgroup Report, Q & A
    - Cyber Analysis Subgroup Report, Q & A
    - Definition and Selection of Controls Subgroup Report, Q & A

3:00 p.m. – 3:30 pm

1. **Review and Decide on Work Plan – Review Proposed 2010 Meeting Schedule**

3:30 p.m.

1. **Adjourn**

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Meeting Notes
CS706SDT Leadership Team

September 1, 2009

Coordination with Subgroup Leaders

Comments on the Concept paper are due by September 4, 2009. Scott Mix will attempt to put the comments together quickly in ways that each of the subgroups can use.

The proposed meeting agenda for next week includes a brief overview of the industry comments up front, and if the subgroups have had a chance to review the comments in advance, they can offer any initial reflections as part of their initial progress report. The agenda includes 45 minutes for each subgroup report on day one. The subgroups will review these inputs when they break out in the afternoon of day one and the morning of day 2.

Subgroup Leaders Roll Call:

- Scott Mix
- Kevin Perry
- Joe Bucciero
- Hal Beardal
- Phil Huff
- John Lim
- Joe Doetzl
- Jay Cribb
- Jim Breton

1. Reliability Functions Subgroup Update and Coordination Issues — Jim Breton (for John Varnell)

The Subgroup is meeting Thursday morning and trying to set up a meeting with Jackie Collett's BES Subsystems and BES Cyber systems subgroup on Thursday at 11:00 a.m. CST to talk about transition. How to turn our work over to that group is the key. What would this look like in terms of applicability and how to evaluate which functions do you perform?

Participant Comments

- This gets more complex as we move forward. One server can be on four components with different high or low values.

- Everything will have security on it. It will be a huge job to evaluate everything.

2. List of BES Subsystems and BES Cyber systems Subgroup Update and Coordination Issues — Jay Cribb (for Jackie Collett)

The team was unaware of the Functions subgroup trying to set up a joint meeting. They have base requirements but need reliability functions to complete their task. The concept paper is very loose regarding lists. There is a remaining concern about possibly requiring compliance on every nut and bolt on the system.

Participant Comments

- Documentation for compliance taking time away from and attention to security? Focus on high and medium for audits and not audit low unless there is an event that must be documented.
- Acknowledge that that is the NIST model and the Rockefeller/Snowe Bill.
- Lot of work but industry will probably vote it down
- The current politics, waiting for a negative vote. What is the alternative?
- Cannot demonstrate everything on every system. I would love for the SDT to step through the process on each system from start to finish. No one has gone through to make sure it will work.
- Other participants thought this was a good idea
- Internally within the SDT? Yes
- Get requirements first then walk through demonstration.
- Need to make the whole process as simple as possible and limit discretionary decision making. What do I need to do to be in compliance?
- Looking at systems impacting reliability
- What are we auditing against?
- Review with Jeri, Keith and others in terms of how NIST works now
- Should be looking at compliance not management
- Take a look at risk based methodology now

3. BES Mapping Subgroup Update and Coordination Issues — John Lim

The team is scheduled to meet this Wednesday to clean up the document. If we have performance based criteria will not applicable to all cases. What if thresholds don't work?

For generation, transmission, etc. looking to group in related systems. They will need a full list of functions

4. Cyber Analysis Subgroup Update and Coordination Issues — Phil Huff

The Subgroup is working to determine the final categorizations to present next week. The team is not sure they have the experts they need to finish the list. Even if you have all the BES functions, what does high mean in certain power generation situations? The team may need more input from John or Jackie's teams. Detailed thresholds would be a serious bottleneck. Jay's suggestion is that the SDT needs to walk through examples to illustrate application and

identify implications make sense. Perhaps in California the team could go through some real life examples.

Participant Comments

- We will need to understand how evaluation will be applied and implications. Apply to digital pressure gauge on a steam line?

Definition and Selection of Controls Subgroup Update and Coordination Issues — Keith Stouffer

Kevin Perry reported that there have been no meetings of Keith's group since Charlotte.

Summary and Next Steps

- Each group will review with others key issues in reports on day one
- Small group work will follow that
- Thursday morning small groups can look at and work on the "seams"
- Possibly end with a concept outline to integrate drafts on Thursday afternoon
- Can we work out guidelines?
- Auditors can only audit to standards/requirements, not to guidelines. Auditors assess compliance.
- Phil, Scott and Kevin (with other minor contributions) got into discussing an example to illustrate possible application of high/medium/low categorization on a BES – low production transformer. Assess function, not the asset? Asset may serve different functions
- Jay Cribb ended the conversation by noting this was a good discussion and illustrated why they need to walk through example(s) as a full group

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Meeting Agenda

Cyber Security Order 706 SDT — Project 2008-06

September 9, 2009 | 8 a.m.–5 p.m. PDT
September 10, 2009 | 8 a.m.–5 p.m. PDT
Western Area Power Administration, Sierra Nevada Regional Office
114 Parkshore Drive
Folsom, California
(916-353-4416)
NOTE: Subgroup Meetings May Not Have Access to Telephones and WebEx

Proposed Meeting Objectives and Outcomes

- Review the CIP-002 Work plan going forward
- Receive updates on TFE, VSL, VRF, and related cyber security efforts
- Receive an overview of industry comments on the SDT concept paper
- Receive and discuss reports from CIP-002 Subgroups identifying key issues and coordination points
- Convene CIP-002 Subgroup meetings
- Receive and discuss Subgroup reports on progress made and responses to industry comments
- Agree on Work plan, next steps, and assignments

Wednesday September 9, 2009

1. **Welcome and Opening Remarks — Jeri Domingo-Brewer**
   a. Roll Call and NERC Antitrust Compliance Guidelines
   b. Facilitator review of August 20–21 Charlotte meeting summary and adoption
2. **Review of Meeting Objectives, Agenda, and Meeting Guidelines — Jeri Domingo Brewer and Bob Jones**
3. **Review of CIP-002 Work plan and CIP-002 Subgroup Process — Stu Langton**
4. **Webinar Report — Jackie Collett, Phil Huff, and Jeri Domingo Brewer**
5. **Update on Technical Feasibility Exception (TFE) NERC Rules of Procedure — Jeri Domingo Brewer and Scott Mix**
6. **Update on VSLs and VRFs — David Taylor or Scott Mix**

7. **Update on other Related Cyber Security Initiatives — SDT Members**
8. **Overview of the Industry Comments on the Concept Paper — Scott Mix**
9. **Subgroup Reports to the SDT**
    a. Reliability Functions Subgroup Report and Reflections on Industry Comments, John Varnell
10. **List of BES Subsystems, BES Cyber Systems Subgroup Report and Reflections on Industry Comments — Jackie Collett**
11. **BES Mapping Subgroup Report and Reflections on Industry Comments — John Lim**
12. **Cyber Analysis Subgroup Report, and Reflections on Industry Comments — Joe Doetzl**
13. **Definition and Selection of Controls Subgroup Report and Reflections on Industry Comments — Keith Stouffer**
14. **Coordination Discussions and Plans among Sub Groups**
    a. Subgroup Meetings (at various locations)
15. **Recess**

Thursday September 10, 2009

1. **Subgroup Meetings**
2. **Welcome and Agenda Review — Jeri Domingo-Brewer**
3. **Subgroup Reports — Plenary Session**
    a. Reliability Functions Subgroup Report and Reflection on Industry Comments
    b. List of BES Subsystems and BES Cyber Systems Subgroup Report and Reflection on Industry Comments,
    c. BES Mapping Subgroup Report and Reflection on Industry Comments
    d. Cyber Analysis Subgroup Report and Reflection on Industry Comments
    e. Definition and Selection of Controls Subgroup Report
4. **Discussion of and Agreement on Subgroup Coordination Strategies**
5. **Review Work Plan**
    a. Review Next Steps for Subgroups and SDT and the creation of a single CIP 002 text

6. **Review Proposed 2010 Meeting Schedule**
7. **Review October Kansas City, Missouri Meeting Objectives**
8. **Meeting Evaluation**
9. **Adjourn**

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Project 2008-06 Cyber Security Order 706 SDT Members

1. Rob Antonishen	Ontario Power Generation
2. **Jeri Domingo-Brewer, Chr**.	U.S. Bureau of Reclamation
3. Jim Breton	ERCOT
4. Jackie Collett	Manitoba Hydro
5. Jay S. Cribb	Information Security Analyst, Southern Company Services
6. Joe Doetzl	Manager, Information Security, Kansas City Pwr. & Light Co.
7. Sharon Edwards	Duke Energy
8. Gerald S. Freese	Director, Enterprise Info. Security America Electric Pwr.
9. Phillip Huff	Arkansas Electric Coop Corporation
10. John Lim	CISSP, Department Manager, Consolidated Edison Co. NY
11. Frank Kim	Ontario Hydro
12. Rich Kinas	Orlando Utilities Commission
13. David Norton	Entergy
14. Kevin B. Perry, Vice Ch.	Director Critical Infrastructure Protection, Southwest Power Pool
15. Christopher A. Peters	ICF International
16. David S. Revill	Georgia Transmission Corporation
17. Scott Rosenberger	Luminant Energy
18. Kevin Sherlin	Sacramento Municipal Utility District
19. Jonathan Stanford	Bonneville Power Administration
20.Keith Stouffer	National Institute of Standards & Technology
21. John D. Varnell	Technology Director, Tenaska Power Services Co.
22.William Winters	Arizona Public Service, Inc.
Roger Lampilla	NERC
Scott Mix	NERC
Dave Taylor	NERC
Joe Bucciero	NERC/Bucciero Assoc.
Robert Jones	FSU/FCRC Consensus Center
Hal Beardal	FSU/FCRC Consensus Center
Stuart Langton	FSU/FCRC Consensus Center

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Meeting Schedule — October 2008–December 2010

Development of CIP Version 2 and Version 3 Framework
October 2008–July 2009

1. October 6–7, 2008 — Gaithersburg, MD Reviewed CIP-002-CIP-009, Agreed on Version 2 approach.

2. October 20–21 —Sacramento, CA CIP-002-CIP-009 Version 2 development

3. November 12–14, 2008 — Little Rock, AR CIP-002-CIP-009 Version 2 adoption for comment and balloting; CIP-002-CIP-009 Version 3 process reviewed.

4. December 4–5, 2008 — Washington D.C. CIP-002-CIP-009 Version 3 reviewed and debated, SDT member white papers assigned.

5. January 7–9 — Phoenix, AZ, Reviewed Technical Feasibility Exceptions white paper**,** reviewed industry comments on CIP-002-CIP-009 Version 2 products — established small groups to draft responses, reviewed Version 3 white papers.

January 15 — WebEx meeting(s) Small group drafted responses to industry Version 2 comments.

January 21 — WebEx meeting(s) Small group drafted responses to industry Version 2 comments.

6. February 2–4, 2009 — Phoenix, AZ Update on NERC Technical Feasibility Exceptions process**,** VSL process and SDT role**,** review of Version 3 White papers, strawman and principles**,** reviewed and adopted SDT responses to industry comments on Version 2 and Version 2 Product Revisions.

7. February 18–19, 2009 — Fairfax, VA Update on Version 2 process**,** NERC TFE process and VSL Team process; reviewed, discussed and refined Version 3 CIP-002 White papers, strawman, and principles.

8. March 10–11, 2009 — Orlando, FL Update on NERC TFE and VSL and VRF Team process and review and refine Version 3 CIP-002 Strawman Proposals

March 2–April 1, 2009 — 30-day Pre Ballot

Mid-March — NERC posts TFE draft Rules of Procedure for industry comment

March 30, 2009 — WebEx meeting(s) White Paper Drafting Team

April 1–10 — NERC Balloting on Version 2 Products

April 6, 2009 — WebEx meeting — White Paper Drafting Team

April 8, 2009 — WebEx meeting(s) — White Paper Preview- Full SDT Conference Call

April 11, 2009 — Version 2 Ballot Results (Quorum: 91.90% Approval: 84.06%) and Industry Comments-

9. April 14–16, 2009 — Charlotte NC Update on NERC TFE process, VSL Team process and NERC Critical Assets Survey; agreed and adopted responses for Version 2 industry comments for recirculation ballot; reviewed and refined Version 3 whitepaper and consensus points and progress report to NERC Member Representative Committee (MRC) May meeting.

April 28 and May 6, 2009 — White Paper Drafting Team Meetings and WebEx

April 17–27, 2009 — Recirculation Results: Quorum: 94.37% Approval: 88.32%

May 5, 2009 **—** NERC MRC Meeting, Arlington, VA- SDT progress report.

10. May 13–14, 2009 — Boulder City NV Reviewed MRC presentation and further SDT refinement and discussion of the Version 3 White Paper.

June 8 and June 15, 2009 **—** Working Paper Drafting Team Meetings and WebEx

11. June 17–18, 2009 — Portland OR Further SDT refinement of the draft CIP Version 3 Working Paper(s), reviewed SDT development process for June-December 2009; discussed potential SDT subcommittee structure and deliverables.

June **—** WebEx meeting(s)

- Working Paper drafting group sessions including inputs from selected industry personnel to help establish BES categorization criteria

CIP-002 Development of Requirements, Measures, Etc. July-December 2009

12. July 13–14, 2009 in Vancouver, B.C., Canada

- SDT plenary session to review, refine, and adopt SDT Working Paper
- Adopt SDT response to NERC for Interpretation of CIP-006-1
- Review and adopt proposal for CIP-002 Subgroups and Deliverables
- Convene Subgroup organizational meetings to develop work plans
- Adopt 2010 Meeting Schedule

July–August Interim WebEx meeting(s)

- CIP-002 Subgroup meetings (as needed)
- CIP-002 Coordination Team meeting (as needed)

August 3**–**5, 2009 in Winnipeg, Manitoba **NERC Member Representative Committee**
Progress Report and presentation on new CIP Version 3 Working Paper-Concept- Reliability Standards on Cyber Security for MRC input.

13. August 20–21, 2009 in Charlotte, NC

- SDT Plenary session to review and respond to MRC input on Working Paper/CIP-002 Concepts
- SDT Subgroup and plenary meetings to develop CIP-002 requirements and "proof of concept" control (s).

July–September — 45-day Industry Comment Period on CIP-002 Concept Working Paper
NERC Webinar
August–September Interim WebEx meeting(s)

- CIP-002 Subgroup meetings (as needed)
- CIP-002 Coordination Team meeting

14. September 9–10, 2009 in Folsom, CA

- SDT plenary session to review and respond to any additional industry comments on Working Paper and CIP-002 Concepts
- SDT Subgroup drafting meetings- consider industry comments, draft requirements and "proof of concept" control (s).
- SDT plenary session(s) Subgroup reports on requirements
- Review of CIP-002 Standards, Requirements, Measures, and Outline
- Address coordinating issues.
- Establish SDT meeting dates and proposed locations for January–December 2010

September–October Interim WebEx meeting(s)

- CIP-002 Subgroup meetings (as needed)

- CIP-002 Coordination Team meeting

15. October 20–22, 2009 in Kansas City, MI
- SDT Subgroup drafting meetings — day one
- SDT Plenary Session(s) — day two Subgroup reports on CIP-002 requirements
- Review and refine initial draft of CIP-002 single text

October–November Interim WebEx meeting(s)
- CIP-002 Coordination Team meeting

16. November 17–19, 2009 in Orlando, FL
- SDT plenary session(s) — to review and refine CIP-002 standard, requirements, measures and controls.

November–December Interim WebEx meeting(s)
- Drafting teams as needed to finalize drafts
- CIP-002 Coordination Team meeting

17. December 15–16, 2009 in Little Rock AK
- SDT plenary session(s) to review, refine, and agree on and adopt CIP-002 standard, requirements, measures and controls.
- Agree on initial posting of draft CIP-002 for industry review and comment.

Refinement of CIP-002 and Development of Other CIP Standards
January–December 2010
(12 SDT monthly meetings and Subgroup WebEx meetings as needed)

- SDT responds to industry comments on initial and subsequent postings of CIP-002, Version 3 (may be multiple comment periods, as required)
- Refine the CIP-002 through the comment period and submit new CIP-002 Version 3 Standard for Balloting along with the catalogue of controls (i.e. CIP-003-CIP-009 or its successor) OR
- Ballot CIP-002 while permitting industry to rely on CIP 003-CIP-009 until the full suite of controls (i.e. CIP-003-CIP-009 or its successor) is reviewed and presented for balloting.
- Submit the full suite of CIP Reliability Standards on Cyber Security for Industry Comment
- Refine and Submit the full suite of CIP standards for industry ballot
- NERC Board of Trustees adoption of the full suite of standards
- FERC approves and NERC Implements the full suite of CIP standards

Proposed 2010 Meeting Schedule

18. January 20–21 — Wednesday–Thursday, Atlanta GA	24. July 14–15, Wednesday–Thursday
19. February 18–19 —Thursday –Friday, Austin TX	25. August 11–12, Wednesday–Thursday
20. March 9–11 — Tuesday–Thursday, Phoenix, AZ	26. September 8–9, Wednesday–Thursday
21. April 14–15 — Wednesday–Thursday, Atlanta GA	27. Oct. 13–14, Wednesday–Thursday or Oct.12–14
22. May 12–13 — Wednesday–Thursday, Dallas TX	28. November 17–18, Wednesday–Thursday
23. June 9–10 — Wednesday–Thursday, Sacramento CA	29. December 15–16, Wednesday–Thursday

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Meeting Notes
Cyber Security Order 706 SDT — Project 2008-06

September 9, 2009 | 8 a.m. – 5 p.m. PST
September 10, 2009 | 8 a.m. – 4:30 p.m. PST
Folsom, CA

Robert Jones, Stuart Langton, and Hal Beardall
Facilitation and Meeting Design
FCRC Consensus Center, Florida State University

Joe Bucciero, Bucciero Consulting, LLC

http://www.nerc.com/filez/standards/Project_2008-06_Cyber_Security.html

116-390 Village Blvd.
Princeton, NJ 08540
609.452.8060 | www.nerc.com

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

SDT 706 September 9-10, 2009 Meeting Summary Contents

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

SDT 706 SEPTEMBER 9-10, 2009 MEETING

EXECUTIVE SUMMARY

The Chair, Jeri Domingo-Brewer welcomed the members to Folsom California and Joe Bucciero conducted a roll call of members and participants in the room and on the conference call *(See appendix #2*). The Chair reviewed the meeting objectives and Bob Jones, facilitator, reviewed the proposed meeting agenda *(See appendix #1*). On day two the SDT accepted the August 20-21 meeting summary without comment or objection.

Mr. Bucciero reviewed the need to comply with NERC's Antitrust Guidelines *(See Appendix #3).* He urged the team and other participants in the process to carefully review the guidelines as they would cover all participants and observers. He urged all to avoid behaviors or appearance that would be anti-competitive nature and also reminded the group of the sensitive nature of the information under discussion.

Mr. Langton reviewed the CIP 002 work plan between August and December 2009 which the SDT adopted at its meeting in Vancouver, setting up subgroups and some ground rules for their work and coordination with each other. The monthly agenda planning meetings with the Chair and Vice Chair have been expanded to include a leadership coordination meeting with the leads from each of the five subgroups. Mr. Langton reminded the five subgroups that they have about two more months to finish their work of developing proposed draft language for the new CIP-002 Version 4 standard, and the full SDT will then work to finalize the new draft CIP-002-4 standard for posting to the industry for comment in December 2009. He noted by the conclusion of the October 2009 SDT meeting, the goal is to have a single draft CIP 002-4 that can be debated and refined in November and adopted in December.

Jackie Collett & Phil Huff & Jeri Domingo Brewer provided the SDT with a review of the August 25th Industry Webinar on the concept paper. The Webinar participation was estimated to be over 650 participants with more than 800 registered.

Jeri Domingo Brewer and Scott Mix jointly presented an update on the TFE process. The Chair noted that at the conclusion of the August meeting, she had agreed to follow up with the Standards Committee regarding the SDT support for addressing TFE issues as an urgent matter. She indicated she will be presenting these to the Committee soon. Scott Mix noted that on the Rules of Procedure side the NERC 2nd draft posting is in comment process now and the Comment period has been extended to Sept 11.

Scott Mix provided a brief update on Version 2 VRF and VSLs noting that the pre-ballot comment period will close September 10 with a 10-day ballot period immediately following the comment period. A recirculation ballot is a high probability, since there is likely to be a comment from an entity voting no. He noted that in the future, the SDT 706 will be responsible for Version 3 VSLs and VRFs and will need to accomplish this in its 2010 workplan.

The following related industry initiatives update was provided:

- In the past week an industry meeting was convened to update the DOE Control Systems Security Roadmap which was initially developed 3 years ago.
- There is a NIST working group, Cyber Security Coordination Task Group (CSCTG), that is focused on smart grid cyber security issues that has been holding weekly conference calls, and its current face-to-face meeting is being held at the same time as this SDT meeting. The CSCTG is in the process of defining cyber security requirements for the various application and functional interfaces that exist among the various computer systems that are utilized by utilities. They are organizing their work to address FERC's four priority policy areas for the smart grid (Demand Response, Electric Storage, Electric Vehicles, and Wide Area Situational Awareness), plus two additional areas of AMI/AMR and Distribution Grid Management. They will be consolidating their inputs into a Smart Grid Framework and Roadmap document, as well as providing a NIST Interagency Report (NISTIR) on Cyber Security. For each interface, they will propose security controls. The NIST site has documents posted, and they should be released shortly for industry comment and feedback.
- The NERC Planning Committee has established a small working group and is soliciting applications for membership in the working group that will focus on cyber security of smart grid components.

Scott Mix presented an overview of the industry comments received on the draft concept paper, noting that 49 comments were submitted by the deadline (Sept. 4) with three additional sets being received following the deadline for a total of 52 comments consisting of over 140 pages. Scott suggested the comments were "all over the map." Few of the commenters, if any, expressed general agreement with the approach. Many struggled to understand of the process and either didn't understand or didn't agree with process.

The SDT reviewed the draft concept paper comments and discussed what the SDT's vision for success is in putting these pieces together from the feedback and comments. Below are the elements of the vision of success suggested by SDT members:

- Standards that will assure the reliability of the BES.
- Multiple groups of people running through the process with same inputs/requirements will reach the same conclusion.
- The end result passes the "smell test"- engineering analysis would agree with the results.
- Industry recognition that reliability functions are important and understanding why protection is needed and beneficial. Focus on reliability functions can demonstrate reliability of BES.
- A clear enforceable standard that doesn't create an unnecessary hardship on entities.
- Get requirements on paper that are simple for entities to follow but may be complex in their development.

The SDT identified the following themes in the industry comments:

- Clarify the SDT philosophy and approach in terms of the degree of flexibility vs. prescription provided in the standards.
- Seek simplification in the final standard but engage in complex hard issues in getting there. Achieve some simplification: workable, clear and doable.
- Engineering analysis needs to support any thresholds. SDT should do this as part of setting the standard.

The SDT identified the following issues from industry comments:

- Complexity.
- CIP-002 Not Yet Tested.
- Augment existing CIP requirements with elements of SDT concept paper.
- Should the SDT take on CIP 003-009 sooner than 2010?
- Value of a walk through example for the SDT and industry.
- Role of Adequate Level of Reliability (ALR) in Concept.
- Pilot the Concept Paper approach.
- CIP 002 as Cornerstone.
- Concern about scope.
- Thresholds and Engineering Analysis needed to support standard.

Scott Mix brought a request from Mike Assante at NERC to the SDT. He asked whether the SDT could confirm that the existing exemption for non-routable protocols will not be carried forward into Version 3? Or in the alternative, can the SDT confirm it will be considering the removal of the non-routable exception for future systems and any modifications to current systems? He noted that the impact of a device is not a function of communication protocols-which are better covered in the list of requirements on how to secure the device.

In light of the SDT discussion, Mr. Mix brought the following statement to the SDT for its consideration, and it indicated a 3.6 out of 4 point consensus scale indicating support for the following statement:

Concerning the elimination of the blanket exemption for non-routable protocol connected serial devices, as is being considered for inclusion in the scope of the CIP Cyber Security Standards, assume the following:

1. The removal of the exemption will not be applicable to the existing approved Version 1 or Version 2, but will be considered in future versions of the standards.
2. The specific security requirements for serially connected devices will be contained in the “catalog of security requirements” (currently CIP-003 through CIP-009), properly accounting for the threat and vulnerability components to the risk to the device.
3. An appropriate implementation plan will need to be adopted recognizing the number of devices brought into scope by this change

The SDT will recommend that the blanket exemption not continue into Version 3, such that communications to a device will not be a consideration for the impact to reliability of the

device. Mr. Mix agreed to provide Mr. Assante with a sense of the team's position on this issue.

Jackie Collett, SDT member, agreed to conduct an informal concept walk-through the proposed conceptual approach to CIP 002 for the SDT with an example that starts with identification of the functions. She started by noting that the SDT needs to develop a vision of what this is going to look like comparing it to designing a vehicle when you are not sure if it's a bike, truck, car, or van.

Using restoration as a function, she suggested that a list of generating units, transformers, station busses, transmission lines, and associated loads for balancing as the BES subsystems supporting this function.

Members identified the following key questions in the course of the Functional Walk-Through:

- One of the industry's questions was how much flexibility should be given to the entities in determining the applicable BES subsystems. If no flexibility in identification and categorizing is given, then you don't need to put a methodology in the standard.
- Do the supporting pieces together create the BES subsystem?
- Will there be consistent outcomes going through the restoration functional analysis first or going through the cyber analysis first?
- If same generator does both restoration and other reliability functions, how to address aggregation in terms of its categorization?
- How to deal with multiple reliability functions from multiple entities?
- Do you need reliability functions mentioned in the standards? This might be part of the development of the standards but would reduce complexity if functions not included in the standards.
- Should there be a "none" or "no impact" category for the functions included in the BES list?
- For which subsystems do we need to do BES mapping?
- Is redundancy protection aimed at failure vs. compromise?
- Should we apply controls at cyber system level, or a methodology to a device level?
- What do we apply controls to: system or components of the system?
- How can we address interconnected systems and systems we are dependent?
- What about interconnectivity with other systems that are ranked differently?
- What is the SDT philosophy and approach- i.e. degree of flexibility vs. prescriptive, guide or impose? How to go about this? What is our strategy?
- Who can determine impact to the reliability of BES? Owner of asset has to even if they have no way to. Is this the right way to go. Who has wide enough view and capable of doing this?

On day two, Joe Doetzl reminded the SDT that the concept paper offered entities the choice of an alternative approach that started with the cyber systems and map those. The concept suggested that the different starting points should result in the same ending point. The

complexity comes from the BES mapping and reliability functions and different levels of impacts on each of those systems. The question is whether if you start with the cyber system it will be a simpler approach to cyber security than starting with the reliability functions.

Members identified the following key questions in the course of the Cyber Analysis Walk-Through:

- What would a responsible entity do in determining what should be in the scope to protect?
- On cyber side, if the cyber is deemed impactful does it inherit the impact level of the function supporting the BES assets? Is anything not impactful not in scope?
- For the assessment of functions or on asset supporting reliability function, do you need an intermediate step?
- Do we agree we want to have multiple levels of impacts on function so we can connect the controls to those?
- Can the assets mapping be capable of translation to a systems approach?
- Any way to diminish the impact of the audit process on low impact sites?
- What does it mean for a BES cyber system to support a reliability function? Is it info for situational awareness, control to generation, etc?
- Are there systems we unequivocally expect to be protected? Basic SCADA systems shouldn't have a minimum set of auditable controls. Even isolated generation. This might take some complexity out.

SDT members discussed what was learned through the walk through of the functional and cyber approaches including:

- The two walk-throughs indicated there is a similarity in complexity in both approaches.
- The issue is how do we eliminate complexity regardless of which side we start the analysis. For example in the cyber approach the complexity is contained in Step 3 whereas in the functional approach it appeared in Step 2.
- Neither is more complex that the other as it will depend on the environment and context. Large number of BES and small number assets may start on cyber side. Small number BES and lots of cyber may want to start on the BES functional side. Neither is wrong.

On the first day of the meeting, the SDT heard and discussed reports from each of the subgroups. The subgroups then met on the second day to review and respond to the comments and suggestions of the SDT.

On the first day Rich Kinas reported, on behalf of John Varnell, on the Reliability Functions Subgroup's work. He noted the subgroup has redistributed its members into other subgroups. The subgroup will continue to try to put more definitions around what was meant by different functions including a brief paragraph on each and what is meant for benefit of and guidance to the other subgroups.

Jackie Collett noted the BES Subsystems subgroup had no further meetings since the August Charlotte meeting. She noted that Jim Case and Matt Greek from the NERC Operating Committee are now participating on the subgroup. On day two, she reported that the subgroup still needs to put time and effort into defining what these BES subsystems are and move into drafting requirements.

John Lim noted the BES Mapping Subgroup met to continue its work in developing the BES Mapping draft markup and was joined by members from the Functions subgroup. Two major issues the subgroup is dealing with include: how do we validate an engineering study? Approval by regional reliability assurer? TFE type process? Need to look at this more. Note that no entities currently are performing the role of reliability assurer. Also, what is meant by "Misuse"- need to describe this term.
John Lim reported following the BES Mapping Subgroup's meeting on day two. The Subgroup is drafting a set of requirements for High, Medium, and Low. There are still questions on how to handle industry studies. In terms of generation subsystems, he noted they are using terms that are not very well defined (e.g., subsystems in generating stations). The terminology they are using must be precise and consistent and coordinated with Jackie Collett's subgroup.

Phil Huff delivered the initial Cyber Analysis Subgroup report noting his confusion about how the subgroup should go forward. BES impact categorization as the black box is a flawed assumption. The subgroup could reduce some of the complexity in the process. We assumed each function mapped would have an impact categorization so we could combine through a "look-up table." On day two, Mr. Huff noted that his subgroup would huddle when the SDT breaks. He noted that there may not be as much confusion as was stated yesterday. Impact criteria that are involved in John Lim's one-to-one mapping will be considered. The subteam needs to develop a strategy on the cyber analysis side.

Keith Stouffer presented the Definition and Selection of Controls subgroup's report. He noted that during the Charlotte meeting the subgroup developed and presented an example based on access control. We pulled together into one location the access control referenced in many places. Keith mentioned that the format is new and the subgroup doesn't know if this is acceptable. Need to nail down as soon as possible what is an acceptable format. The Subgroup on day two noted they will seek to nail the format decision down with NERC. Joe Bucciero will send latest work in progress of the Subgroup to all group leaders.

The SDT agreed that a brief statement should be drafted for publication in NERC's newsletter. Gerry Freese agreed to draft the summary. The Chair reviewed with the SDT the schedule for the next couple of meetings, reminding members that at the conclusion of the October meeting in Kansas City we hope to have a single text of CIP 002 which we can refine in November and approve for posting in December. She thanked the members for their hard work together and in the Subgroups and encouraged them to continue working to make headway on each of their charges. Members completed an onsite meeting evaluation form.

The SDT adjourned at 3:45 p.m. on September 10.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

SDT 706 SEPTEMBER 9-10, 2009 MEETING SUMMARY

I. INTRODUCTIONS, AGENDA AND SDT WORK PLAN REVIEW

The Chair, Jeri Domingo-Brewer welcomed the members and Joe Bucciero conducted a roll call of members and participants in the room and on the conference call *(See appendix #2*). The Chair reviewed the meeting objectives and Bob Jones, facilitator, reviewed the proposed meeting agenda *(See appendix #1*). The SDT adopted the August 10-11 meeting summary without comment or objection on Thursday morning.

Mr. Bucciero reviewed the need to comply with NERC's Antitrust Guidelines *(See Appendix #3).* He urged the team and other participants in the process to carefully review the guidelines as they would cover all participants and observers. He urged all to avoid behaviors or appearance that would be anti-competitive nature and also reminded the group of the sensitive nature of the information under discussion.

Mr. Langton reviewed the CIP 002 work plan between August and December, 2009 which the SDT adopted at its meeting in Vancouver, setting up subgroups and some ground rules for their work and coordination with each other. The monthly agenda planning meetings with the Chair and Vice Chair have been expanded to include a leadership coordination meeting with the leads from each of the five subgroups. He noted the five subgroups have about two months to finish their work of developing the CIP 002 draft to be finalized by the SDT in November and December, and released for posting and industry comment in December 2009. He noted by the conclusion of the October 2009 SDT meeting, the goal is to have a single draft CIP 002 that can be debated and refined in November and adopted in December.

Member Comments on SDT Workplan

- Due to increased workload in terms of response to CIP-002 industry comments and the development of CIP-003-009 requirements in 2010, the SDT will be convening 3-day meetings
- The SDT will continue to use phone and telephone conference calls to enhance effectiveness.
- As an alternative, NERC staff brought up the possibility of meeting 1 to 2 weeks at a time to improve schedule effectiveness.
- The current proposed game plan- is to set SDT meetings using 3-day schedules with a back-up strategy of spending a 1-week chunk somewhere, if needed.
- At first blush this appears shocking. However, when you factor in the day traveling/to and from it might not be more onerous than the current meeting schedule.
- The hosts for the remaining 2009 SDT meetings are checking to see if they can add a 3rd day to each of their meetings.

Jackie Collett & Phil Huff & Jeri Domingo Brewer provided the SDT with a review of the recent Webinar (held on August 25) on the working concept paper that was posted to promote information exchange with the industry. The Webinar participation was estimated at over 650 with more than 800 registered. The SDT leaders indicated the session went well and Joe Bucciero agreed to get the Webinar summary notes out to the Team. Questions were raised surrounding the security controls which underlined the importance of work ahead. There were process questions of what version would be implemented when? NERC staff didn't jump in to answer questions as this was designed as an SDT Webinar. Those questions were referred to NERC for responses.

Member comments on the Webinar Presentation

- In terms of questions dealing with process and NERC standards, communications with the industry is needed. We need to do a better job of telling the industry what they should be doing. There is significant confusion currently.
- The Chair proposed and the SDT agreed to do another Webinar in the December time frame with the Subgroup leaders participating. NERC will need to flesh out with the industry the process area questions.

II. UPDATES

A. Update on Technical Feasibility Exception (TFE) NERC Rules of Procedure

Jeri Domingo Brewer and Scott Mix jointly presented an update on the TFE process. The Chair noted that at the conclusion of the August meeting, she had agreed to follow up with the Standards Committee regarding the SDT support for addressing TFE issues as an urgent matter. She indicated she will be presenting these to the Committee soon. The Chair noted that Kevin Perry is prepared to move forward with an urgent action SAR that was reviewed and discussed at the August SDT meeting and is looking for a proxy to submit.

Scott Mix noted that on the Rules of Procedure side the NERC 2nd draft posting is in comment process now and the Comment period has been extended to Sept 11. They have received 5 sets of comments which NERC staff is reviewing.

In the context of interim guidance issues for those entities in compliant phase, regions are in process of figuring out how to handle these. NERC is trying to get the interim process running ASAP while the formality of approving the final process takes place.

Member Comments on SDT

- Has a decision been made on the matrix for the SAR? In August Mr. Perry noted it was "vetted" it with regional group representatives on the CCWG group and the chair of the Version 1 CIP.
- Where do we go to get guidance for entities coming up on an audit and the status of TFEs? The interim guidance document on NERC website--which NERC drafted and regions have

agreed to. Updated interim guidance is under development to make interim more consistent with final if approved.

- What if a region has no facility for accepting TFEs? Rely on your own legal council.
- Last posting of TOP is one we should expect to be implemented. Section A- by September 17, 2009. The assumption is that the implementation proposed is best we know right now.
- In July 2008 there were 13 requirements compliance by July 2009, there were 41 requirements. The regions are hanging in the wind on this. One entity represented on the SDT is 5 weeks from a NERC audit. Members are confused. Need to make things easier.
- The MPCC in discussing the ROP has pointed out FERC hasn't approved version 2 yet. Version 1 of standard only? Will we have to change again?

B. Update on VSLs/VRFs

Scott Mix provided a brief update on Version 2 VRF and VSLs noting that the pre-ballot comment period will close September 10 with a 10-day ballot period following with recirculation a high probability if there is a single comment from an entity voting no. In the future, the SDT 706 will be responsible for Version 3 VSLs and VRFs and will need to accomplish this in its 2010 workplan.

C. Update on other related cyber security initiatives- *SDT Members*

Keith Stouffer noted that in the past week a meeting was convened of over 100 experts in La Jolla, California to update DOE Control Systems Security Roadmap which was initially developed 3 years ago. They addressed activities and initiatives over 3 years, e.g. smart grid and SDT 706. Energetics provided facilitators to manage a number of break-outs. They are under contract to produce an update to the road map in the next few months. The website is: http://www.PublicIERoadmap.com

There is a NIST working Control Center ETG focused on smart grid issues that is meeting today and tomorrow. They are collecting interface security requirements and are looking at FERC's four areas of focus. They will be consolidating inputs into 1 document. For each interface, they will propose security controls. The NIST site has documents posted.

The NERC Planning Committee has established a small working group and is soliciting applications for membership in the working group that will focus on cyber security of smart grid components. They understand they need enough of a cyber security perspective on the working group and the Planning and Operating committees don't typically have that perspective. They are looking at the electric grid reliability impacts of smart grid(s). You can't do smart grid without high speed communication. A fundamental tenet of this is requiring good cyber security.

III. REVIEW OF INDUSTRY COMMENTS ON THE CONCEPT PAPER

A. Overview of Industry Comments

Scott Mix presented an overview of the industry comments noting that 49 comments were submitted by the deadline with three additional sets following the deadline for a total of 52 comments consisting of over 140 pages. He suggested the comments were "all over the map." Few of the commenters, if any, expressed general agreement with the approach. Many struggled to understand of the process and either didn't understand or didn't agree with process. Some took exception to the breadth and scope of the concept suggesting it may exceed the authority of 215 Fed Power Act. Responses to Question 5 are typical of the diversity of perspectives: some believed 3 levels is the right number, others suggested higher and lower numbers, including 2 levels of critical and non critical and others suggested leaving it as it is currently.

B. Overview of Member Comments

1. Overall Themes of SDT Reflections on Industry Comments

- Clarify the SDT philosophy and approach in terms of the degree of flexibility vs. prescription provided in the standards. Trying to get away from the current wide latitude and flexibility. How much less latitude? How much room for judgment? If give latitude. If entity can provide an alternative approach through an analysis, this will increase the complexity of the standard if you have to outline what will be an acceptable analysis.
- Seek simplification in the final standard but engage in complex hard issues in getting there. Achieve some simplification: workable, clear and doable. Engineering analysis needs to support any thresholds. SDT should do this as part of setting the standard.

2. Vision of SDT Success

The SDT reviewed the comments and discussed what the SDT's vision for success in putting these pieces together to do? Below are elements of the vision of success suggested by members:

- Standards that will assure the reliability of the BES.
- Multiple groups of people running through the process with same inputs/requirements will reach the same conclusion.
- The end result passes the "smell test"- engineering analysis would agree with the results.
- Industry recognition that reliability functions are important and understanding why protection is needed and beneficial. Focus on reliability functions can demonstrate reliability of BES.
- A clear enforceable standard that doesn't create an unnecessary hardship on entities.
- Get requirements on paper that are simple for entities to follow but may be complex in their development.

3. SDT Identification of Issues from Industry Comments on Concept Paper

   a. Complexity. Is the concept too complex as presented?

b. CIP OO2 Not Yet Tested. Haven't run with existing CIP 002 long enough- consider staying with it longer?
c. Augment existing CIP with elements of SDT concept paper. Recommend to take valuable elements of new approach to augment legacy CIP 002-009 framework.
d. Should the SDT take on CIP 003-009 sooner? Is there another way to deal with "dodgers"- can we take another look at what we need to deal with CIP 003-009. E.g. grading high medium and low. Significant concurrence with moving in direction with identifying controls. Should we look at how to improve 3-9 and then back to 002? Hunt down dodgers.
e. Value of a walk through example for the SDT and industry. Help the SDT and the industry to walk through process CIP 002 start to finish with some mythical power plant, control center or sub station. How to go from defining system, to applying controls to assets. "Systems" is the new concept and how to help the industry make this leap. Walk through as a team. We would better tell our story and let people understand it. Haven't stepped all the way through this process.
f. Role of ALR in Concept. What was missed in responses is that the concept of ALR is not going to appear in the CIP 002 standard. It is a framework for deriving the functions. The functions will be included, not the ALR. They only served as a guide for drafting team to derive functions that are relevant. They served as principles for getting at the scope for 002. If you ignore principle 6, the other 5 principles are in line with Federal Power Act at a high level. ALR defines adequate levels of reliability.
g. Pilot the Concept Paper approach. May need a pilot for the concept similar to how this is done in the nuclear side to test how it works in practice.
h. CIP 002 as Cornerstone. The SDT made a strategic decision to develop CIP 002 as the cornerstone. It is ugly and difficult work. We can't drop this, we have to finish it even though it is hard.
i. Concern about Scope. Industry concern is that no one knows how big this will be—there is a "paranoia about scope". Concern also of the possible loss of invested effort (time and $$). Is there a way of taking what has been done and map it to the CIP Version 1 and 2 to see what happens to the critical cyber assets. Industry is asking how much more will we have to do than what we do now. If the under Verion 1 and 2 represents 10% of critical assets. Will I have to spend 10 times as much under version 3?
j. Thresholds and Engineering Analysis to Support. If this drafting team puts out hard threshold numbers it need solid engineering analysis behind it.

4. Member Review of Industry Input on Concept Paper

a. Wednesday Member Discussion Notes
   - Some suggested we didn't provide enough detail for them to respond, even though this was presented as a concept paper. A few entities didn't understand the concept.

- Overall, it appears many didn't understand what the rationale was for changing the existing process changes believing the existing didn't have a chance to prove itself.
- Lots of discussions among drafting team over last 6 months. Going forward, we need to lay out more clearly why we are moving in this direction. Set forth why this sea-change is being proposed in identifying and categorizing?
- Industry may be upset because we are perceived as a moving away from compliance and trying to address security. What we do currently is compliance oriented.
- If the SDT and industry do this right, both security and compliance can be achieved. This is a new way of looking at security that is trying to do just that.
- My take is different. I believe we should take the critique of concept complexity seriously. It is mentioned 40 times in the comments. Confusing is mentioned 31 times and complicated is referenced 12 times.
- SDT has to be aware of and trying to not making this more complicated than is needed.
- Some are suggesting we should not start with ALR- which is suggested to be too broad a starting point. Instead consider starting with Federal Power Act definition of reliability and build on basic approach.
- The concern with ALR may be directed at principle 6. The other 5 are more in support of the Federal Power Act reliability definition. Enough generation to serve load.
- Written by Operation and Planning Committees- wrote this on reliability. Is this service reliability vs. bulk electric reliability.
- Yes it is a complex process- we started with 3 levels. Created a complex process that overloaded the front-end analysis. Entities not sure of how to implement. Hard #s would make it easier and simpler. Higher impact- easy to understand. Push back is that engineering analysis may find that is quite right. Are we painting the house with a small brush in order to keep the paint off?
- We may have gotten so few comments because of the complexity and the other things out there.
- Compliance vs. security discussions- compliance is overwhelmed with evidence they must provide. Reluctant to introduce additional documentation/evidence requirements.
- Should we focus on 003-009 where we have problems and come back to 002? FERC order 706 had many issues with 003-009.
- If we provided some relief and flexibility in that area? Easier to expand later.
- There is a concern with putting out 002 in a vacuum- CIP 003-009 most concerned with. What do I have to do? We need to post a sample with 002.
- In the current paperwork drill and compliance we are forgetting security. Is there a possibility of a quick hit on something helpful in 003-009? If this is another paperwork nightmare, could get voted down. How are we going to get

there from here? Don't have a vision for success that we can articulate to the industry.

- Is the concept too far reaching on CIP 002 aspect? One comment suggested it is too complex and should run with existing CIP 002 long enough to judge its effectiveness.
- Another way to deal with "dodgers"- can we take another look at what we need to deal with CIP 003-009. E.g. grading high medium and low. Significant concurrence with moving in direction with identifying control.
- Should we look at how to improve 3-9 and then come back to 002? Hunt down dodgers.
- We need to help industry to walk through process CIP 002 from start to finish with some mythical power plant, control center or sub station. How will this go from defining the system to applying controls to assets?
- "Systems"- how to make this leap. Walk through as a team. We would better tell our story and let people understand it. Haven't stepped all the way through this process.
- Paper work drill. Can't repeat with new standards. Seeing future audits of standards being more operational vs. paper work. If we are going to get this security- test operations to see if secure. Operational audit only way to do this in a hands on way. Don't know how this will happen. Need to think about. Pie in the sky? E.g. "Penetration test"
- Audits will do more of this in the future.
- Agree with today's SDT comments. We still have a focus on paperwork for audits.
- The industry is hesitant to walk away from the compliance investment.
- Recommend valuable elements of new approach that can augment the legacy framework of CIP 002-009.
- Should ALR be the beginning point? Does ALR need to be removed?
- ALRs- if we ignore principle 6 right now, the other 5 principles are in line with the Federal Power Act at a high level. Back up protection schemes were presented in Phoenix. Where in the system are these systems required? How to determine this? ALR defines adequate levels of reliability. Maybe we should have 2 levels. High impact and low impact? Low impact- difference with Version 1 or 2- got to do something more than the current model requires. E.g. issues with password managing, patching. Different levels of e.g. patch management. Comes into requirements section is where that belongs.
- Support for using the current CIP as basis and augmenting with new things.
- What was missed in the industry responses is that the concept of ALR is not going to appear in the standard. It is a framework for deriving the functions. The functions will be included not the ALR. It serves as a guide for the drafting team to derive functions that are relevant. They are just principles for getting at scope.

- If we stick with a multi level approach in 003-009, we will need to know what we are devising requirements for. OO2 does this. Put out an example. Categorizing system. Medium or high system show applying security controls. Show that not every single asset will have a requirement. Will be more complicated as a compliance exercise.
- The regions seemed to be suggesting that the concept appears good but there is a suggestion that what may be needed now is a pilot. Similar things done on nuclear side to see how it works. We don't know how it is working but we invested lots of $$. Audits- going on now. Think right now of a case study or pilot.
- Critical assets, non-critical assets and de-minimus assets?
- The concept seeks to provide strategic decision- CIP 002 is the cornerstone, albeit, ugly and difficult for the SDT. We can't drop it and say this is too hard yet.
- What is desperately needed is what is low is? That's why getting this. Everything will be protected. Give both high and low.
- There is a concern that no one knows how big this will be—i.e. a "paranoia about scope". Concern of loss of invested effort (time and $$).
- SDT should consider a way of taking what has been done, providing a mapping of what has been done- a critical asset- critical cyber asset- show that mapping and what happens if you apply the concept paper. Critical assets and critical cyber assets- question is the middle ground. Industry wants to know how much more will we have to do than what we do now?
- If I currently devote 10% to facilitating critical assets, will I have to spend 10 times as much under the concept?
- Routable vs. non-routable- trying to be a physical security standard while calling itself a cyber security standard. Can we address this? CIP 10- physical security. Big disconnect- something important but not protecting.

b. Thursday Member Discussion Notes

At the beginning of the discussion on Thursday of the Industry input, the facilitators summarized several key questions raised in Wednesday's discussion including:

- Are there systems we unequivocally expect to be protected? Basic SCADA systems shouldn't have a minimum set of auditable controls. Even isolated generation. This might take some complexity out
- On the cyber side, if the cyber is impactful, then it inherits the impact level/ function of the BES assets it is supporting. Anything not impactful is not in scope. This could be one way to simplify the process.
- Do we agree we want to have multiple levels of impacts on function so we can connect the controls to those? In end multiple levels of cyber systems impact on function.

- Define what it means for a BES cyber system to support a reliability function. Is it info for situational awareness, control to generation, etc?

Member Comments

- Clarification and simplicity to make this a more manageable change process.
- Didn't hear industry rejection of fundamental assumptions and model.
- Threshold model approach?
- Upon reflection there might not as much confusion as we initially thought.
- Our team need to develop more on the cyber analysis side.
- We haven't decided whether there will be a one-to-one mapping. Can't promise that yet. Lots of overlapping functions. Level of functions we have is higher in the criteria than the functions we have from Subgroup 1.
- Subgroup 1 functions- BES assets list- covered all functions rather than a 1-1 mapping.
- Supporting documentation will be critical to communicate to the industry how we got there.
- Is there existing mapping of any generation sub system? Building on work already done and look for thoroughness.
- Matrix- started in middle of concept. 2 sides of matrix. Decoupled approach then use matrix to combine. Laid out some general thresholds. Supporter of thresholds.
- Generation subsystems
- The 19 criteria John Lim's group identified covering high/medium and low- may not be enough. Raw megawatt output, Constraint mitigation, radial vs. non radial etc.
- The SDT should consider applying watermarking on that generation.
- Based on around 10 generation criteria
- Then Cyber impact- may not have hard number- describing impact of cyber system to the BES subsystem generator. Impact is same whether big or small. Combination of cyber and BES impact accommodated in the final result. Feed into CIP 003-009. Below was is an example to illustrate the concept that Scott Mix shared with the SDT:

	High	*Med.*	*Low*	*Null*
BES impact e.g.	<2001	<1001	<400	Less than 400

	High	*Med.*	*Low*	*Null*
Cyber impact:				

- Is this per unit or per plant? One row for per plant and another row per unit? Need to determine this as well. Per unit on cyber side and per plant on BES side. E.g. a plant wide scope of control?
- Degree of simplification- detailed work. Should this team take this one on?. Assume it should be done. Punt to somebody else?
- Don't know its been done to this level. Is that a scope of work for a cyber security person. If we don't do it, no one else will.

- Subgroup understanding. Making marriage of two impact assessments. Way to move forward to define the cyber impact criteria. What does it mean for BES cyber system to support the reliability functions. May not have H/M/L levels.
- Proposal on evaluation of cyber system- proposing a H/M/L on its impact on the function? Most functions map to BES subsystem.
- Analyze the Impact to the system.
- Impacts to the reliability function are de-coupled. This is not how it impacts the BES systems.
- We may be counting the impact twice on each side.
- In the federal context, the White House defined criteria for defining cyber system impact on a business function level. Marrying top-down and bottoms-up approach. Painful process to begin with. Interpreting top down approach. Has become easier to develop what controls apply.
- E.g., boiler flame control system- what cyber- reliability function of generation. Not counting twice. Make sure clear on what a BES cyber system is. Define it on a functional level—i.e. what it means for cyber system to support at reliability function.
- What happens if the cyber system isn't there. Only defined cyber system as supporting a reliability function.
- High =loss or compromise of confidentiality, integrity and accessibility. Medium= there are effects, not expected to effect.
- The size of a generator does not play into cyber analysis.
- The cyber system inherits the rating of the BES asset. Like to consider a cyber analysis as binary. Cyber systems not associated with "big iron."
- It is an issue of scope of control.
- Now that you know the function- e.g. EMS what cyber systems are and they inherit EMS. E.g. historian functions, offline logging system probably low.
- Assets essential to perform that scope of control are inherited. Bottom out at low.
- Point out that here are the filters that help place these in the buckets.
- The cyber impact doesn't trump the BES impacts.
- We are assuming inputs of categorized reliability functions. We can define them for reliability. Don't have a list of cyber functions.
- The SDT needs to get the requirements down. Take this opportunity to know what we need to do in writing.
- Numbers- is there a threshold number assumed that can be applied? Risk based methodology (guideline 27). "Bright line"- categorization of what constitutes a BES.
- Are we coordinating with other regional entities? SDT represents all the regions. NPCC doing this? Bring to everyone else? NPCC aversion to "bright lines" (A 10 as methodology for id critical assets for CIPs standards)
- NPCC- only region that has used the NERC definition of bulk power. Issued a performance-based methodology to determine what is bulk power with backup studies. Guideline 27 is a regional guideline.

- We may need something talks about constraints- relieve IRLs or SOLs. VAR support and voltage support. We will need a number of yardsticks to determine criticality.
- Control center- simpler map back to transmission and generation? Numbers of links and lines? Relationship to elements underlying that.
- Are there other reliability standards under draft- similar process determining applicability to BES elements. Rationalize with them and make it the same? E.g. disturbance reporting standard.
- NERC attempted to do that in Version 1 but fell short. Criteria for disturbance reporting is an early warning gray area. (warning track).
- Determination of bright lines. Focus on cyber security side. Are we in danger of going down rabbit holes?

C. Exemption for Non-Routable Protocols

Scott Mix brought a request from Mike Assante at NERC to the SDT. He asked whether the SDT could confirm that existing exemption for non-routable protocols will not be carried forward into Version 3? Or in the alternative, can the SDT confirm it will be considering the removal of the non-routable exception for future systems and any modifications to current systems? He noted that the impact of a device not a function of communication protocols- better covered in list of requirements on how to secure the device.

Member Comments on the Request

- Non-routable protocols may be as susceptible to attack as routable, e.g. electronic security perimeters are not feasible, patch management and other things, incidence management. Attach those requirements to other cyber devices.
- What was the logic behind non-routable exception? Why did we do this?
- Primarily around electronic protection- firewall kind of device. Because we cant do ESPS, ended as a blanket exemption.
- Wouldn't have a problem supporting this. However there is no implementation plan under CIP Version 1 yet. Can we allot sufficient time for compliance?
- Newly identified critical assets- Version 1 / 2 may take from 6 to 24 months to implement.
- Under version 1- physical security on nuclear sites? This won't happen. Can we accomplish this within the time limits?
- Intent question= CIP 2 version 1- exclusions were deliberate- initial starting point. Couldn't deal with the serial devices issues and left it out at that time. Too much for industry to start with and swallow. Has anything changed?
- Need to address effective security for those devices. Some measure of physical security.
- Implementation plan- version 2- different implementation plan.

- Michael Assante's request- appropriate for Team to respond with a position- our task is to improve the overall cyber security stance of the industry. We will consider what is appropriate for modern and legacy serial devices and risk/vulnerabilities associated with this.
- Many took prudent measures to provide some level of security for those devices serial in nature.
- The SDT will need to do thorough analysis of the implications before we take a stand on this. We shouldn't address now unless we fix everything else.
- assuming that exclusion is on the table to be lifted in version 3, assuming that we appropriately address requirements for serial devices. Ok with assumptions.
- Assuming you mean the future CIP standards instead of system the Team is considering the need for exceptions to the standards.
- This question has nothing to do with version 3 of the standard.
- Grandfathering the non routable as it is
- He is asking if regardless of version 3 of standards, are we going to do something to stop people from changing or replacing systems.
- There is a difference between exemption and exception. Are we talking about an exemption? We need clarification of what he's asking.

Draft Statement

In light of the discussion above, later in the afternoon Scott Mix brought the following statement to the SDT for its consideration:

> Concerning the elimination of the blanket exemption for non-routable protocol connected serial devices as being considered for inclusion in the scope of the CIP Cyber Security Standards:
>
> Assuming the following:
>
> 1. The removal of the exemption will <u>not</u> be applicable to the ~~next version of the standards (Version 3), but not to the~~ existing approved Version 1 or Version 2), <u>but will be considered in future versions of the standards.</u>
> 2. The specific security requirements for serially connected devices will be contained in the "catalog of security requirements" (currently CIP-003 through CIP-009), properly accounting for the threat and vulnerability components to the risk to the device.
> 3. An appropriate implementation plan will need to be adopted recognizing that the number of devices brought into scope by this change
>
> The SDT will recommend that the blanket exemption not continue into Version 3, such that communications to a device will not be a consideration for the impact to reliability of the device.

	4=acceptable	*3= minor reservations*	*2=major reservations*	*1= not acceptable*
SDT Rating	**7**	**9**	**1**	**1**

Comments before the Rating

- Concerns with stating it will be removed. JDB
- "will be applicable.
- Assumptions imply this is the position of the team as a whole. Discussed exceptions but hadn't concluded that Version 3 will need exceptions.
- We haven't made that conclusion.
- The SDT does not intend to include a similar clause in CIP 002 differentiating between routable and non-routable protocols.
- We haven't walked up and touched the elephant.
- Impatient-consider this reasonable- we will consider it in the future. No objection.
- The issue of non-routable protocols will be addressed in…. implying this in the 002 concept. Target of protection may lead you to communications that are routable.
- The SDT hasn't discussed this. Needs to be vetted.
- We don't know yet whether you keep them in or take them out.
- Yes we will look at this in version 3.
- If version 3 is targeted at something else, want to make sure that any decisions incorporate sufficient time for implementation.
- Keep it simple. Eliminating it? Not for Version 1 or 2.
- This is an apple and oranges issue. "Critical cyber asset" What we are doing has nothing to do with this. Different ball game. No idea how connectivity will play into categorization.
- This doesn't belong in 002 but in the individual controls.
- Appropriate to respond- that impact is not related to communications connectivity.
- We don't know how we are handling connectivity.
- If Mike Assante wants the SDT to consider this further, he should provide a statement in advance of a meeting so the SDT can understand the intent. E.g. was it to prevent routable communications from being ripped out of service and replaced with non routable to not have critical cyber assets to apply security controls?
- Interpretation cannot modify standards.
- Scott Mix will provide Mr. Assante with a sense of the team's position on this issue.

IV. SDT CONCEPT PAPER WALK THROUGH

A. Walking CIP 002 Through an Example- Restoration Functional

Jackie Collett, SDT member, agreed to conduct an informal concept walk-through the proposed conceptual approach to CIP 002 with the SDT with an example that starts with identification of the functions. She started by noting that the SDT needs to develop a vision of

what this is going to look like comparing it to designing a vehicle when you are not sure if it's a bike, truck, car, van.

Using restoration as a function, she suggested that a list of generating units, transformers, station busses, transmission lines, and associated loads for balancing as the BES subsystems supporting this function.

Member Walk-Through Key Questions

- One of the industry's question was how much flexibility will we give the entities in determining the applicable BES subsystems. If no flexibility in identification and categorizing, then you don't need to put a methodology in standard.
- Do the supporting pieces together create the BES subsystem?
- How much flexibility should there be for the entity? Should there be pre-determined criteria?
- Will there be consistent outcomes going through the restoration functional analysis first or going through the cyber analysis first.
- If same generator does both restoration and other reliability functions, how to address aggregation in terms of its categorization?
- How to deal with multiple reliability functions from multiple entities?
- Do you need reliability functions mentioned in the standards? This might be part of the development of the standards but would reduce complexity if functions not included in the standards.
- Should there be a "none" under this function as part of the BES list?
- What are the subsystems we need to do BES mapping for?
- Is redundancy protection aimed at failure vs. compromise?
- Should we apply controls at cyber system level, or a methodology to a device level?
- What do we apply controls to: system or components of the system?
- How can we address interconnected systems and systems we are dependent?
- What about interconnectivity with other systems that are ranked differently?
- What is the SDT philosophy and approach- i.e. degree of flexibility vs. prescriptive, guide or impose? How to go about this? What is our strategy?
- Who can determine impact to the reliability of BES? Owner of asset has to even if they have no way to. Is this the right way to go. Who has wide enough view and capable of doing this?

Member Discussion Comments

- One of the industry's question was how much flexibility will we give the entities in determining the applicable BES subsystems.
- There will be an EOP- works for restoration? Assume for this example that there isn't an EOP- assets work together
- Do we expect every registered entity to perform restoration?
- Do these supporting pieces together create the BES subsystem?
- Today it is asset based. Generation as critical asset without transmission being critical?

- List of BES subsystem stuff.
- Do we apply the criteria to BES subsystems or parts?
- Before we apply, do we need to make sure the list of assets is impactful to the BES? If not it shouldn't go into categorization system.
- How much flexibility should there be for the entity? Should there be pre-determined criteria?
- Entities should apply criteria to BES sub system to determine whether the subsystem is in scope.
- Is it the low threshold?
- When we started work of categorization, we assumed that the things have some impact, high, medium and rest is low. Should we define low? And everything else is out of scope.
- 1 for generation and 1 for transmission.
- High impact- part of regional restoration plan.
- Apply the criteria to generation and this is medium.
- High impact- transmission sub system- comprising 2 or more paths.
- When we reference the regional blackstart plan we should acknowledge the potential for gaming.
- Assume that this vehicle has to drive properly. How will this work?
- Is the level a binary evaluation? Are you are either part of it or you are not? You are high or low?
- This may not be in keeping with the way we are trying to look at this as a whole.
- Should transmission and generation be in the same class?
- Compliance- generation operator/owner and transmission owner/operator.
- Consistent outcomes? Go thru restoration functional analysis and have one categorization and through another analysis and come up with another. Does this create extra work? Some pieces will likely do another function. Joe Doetzl agreed to do a walk through the other side of the optional concept approach.
- Once you hit high- you are high.
- Aggregation issue :If same generator does restoration and other functions. Supports multiple reliability functions does that change its categorization?
- Will this introduce too much subjectivity and complexity
- Flexibility=complexity. How much flexibility will entities be provided? If no flexibility in identification and categorizing, then you don't need to put a methodology in standard. Would greatly simplify by giving marching orders.
- Multiple functions from multiple entities. E.g. situational awareness for 2 entities, and control and operations for another. Substation monitored by control center. Another entity with control center does control from station.
- This is part of agreement and oversight. BES subsystem side and the same issue will be there for cyber systems.
- What are the cyber systems associated with "big iron" system that is ranked high? Associated with the big iron system and its function.

- BES subsystem- just supporting the big iron stuff ranked as a high.
- What are the cyber systems associated with big iron?
- Impact categorization. Developing criteria- mentioning the function and the BES subsystem. All within the criteria. Do you need reliability functions mentioned in the standards?
- This would be part of the development of the standards- would reduce complexity if functions not in standards.
- From a compliance point of view this might be an issue. The reason for first list is so you can know they are all categorized.
- BES sub system based on reliability function with no H/M/L criteria- where would that place.
- Will we define the low threshold or will this be done by the development of the list of BES subsystems that are in scope.
- Lows are now a "catch hold." Criteria for high and medium are specified and if it is not in those then it is placed in a low category functioning as a default category.
- If we introduce a "none" category, then we need a low impact. Could be a "none" under this function. Would the "none" be part of the BES list?
- We developed a list of functions and BES mapping. Are all essential functions represented by one of the BES mapping criteria? Do we need to start with functions? Make sure all essential functions are represented in the mapping.
- Need a way to check that all are included in a bucket.
- You would have a restoration criteria? Yes. Ensure all functions are captured in the mapping criteria.
- From impact categorization, it is easier to think of generation, transmission etc. vs. functions.
- If we do the BES mapping of functions into the criteria, we need to make sure we have covered all the functions at appropriate level in the criteria.
- How does BES subsystem fit into this?
- Is the entity going to determine what sub systems are or will a table be provided.
- What they would like to see, if you are a generator and you perform this function and above this many megawatts, you are a high.
- Start with the asset not the function. Risk is you will miss systems supporting functions that are not part of the asset.
- Mapping BES subsystems to reliability functions. Current assumption- impact criteria would reference some finite set of BES subsystems.
- Stayed away from generating stations. Stating the impact criteria in terms of BES sub systems? Yes.
- Would have minimal set of subsystems- if you have these kinds, performing these functions, have to be evaluated as a generation subsystem.
- We need to define the reliability functions in terms the industry can understand.
- Reliability functions- every asset involved in situational awareness or balancing load and generation.

- What are the subsystems we need to do BES mapping for?
- How do we work in those doing engineering studies now to do ranking of assets? Has the universe been covered in these reliability functions?
- Jeff Gillen ATC noted that the industry has done a lot of work already. There may be an industry problem if ALR and existing planning standards aren't tied to this. Things should be done with existing methodologies if possible. Planning criteria for category A, B, C etc. Category C event is looking from a common mode failure of a cyber attack.
- Industry understands the current methodology. Consider building on it. Analysis looking at cascading.
- This is one of the inputs for coming up with the list by the Mapping Group.
- We have identified a major stumbling block on identification of BES sub systems. However an alternative appears available for building on what exists today.
- Categorizing cyber systems. It is not until Step 5 of methodology and finally talk about cyber systems.
- BES subsystems and categorized and now identify BES cyber systems. Look at BES cyber systems (SCADA, control system). Look at all of BES systems/
- Assume we identify BES cyber systems that support reliability functions of the BES.
- Identified- to the asset which supports the functions. Generating stations- remote RTU, SCADA, master, blackstart, local in plant controls. How do you then apply the controls. Do an analysis of your cyber systems.
- Which subgroup is looking at defining or describing a cyber system? Here's its cyber system- in house plant controls. Apply appropriate/adequate controls.
- If compromised cyber system (integrity, confidentiality, reliability) how would it impact reliability of BES.
- None not low. Cyber standard. If no cyber stuff, it doesn't apply.
- Functional impact analysis. What would it mean to impact restoration? E.g. metering in the station provides situational awareness, but not highly required. If start/stop controls rely on meters. Meters then part of a start/stop system.
- What is the basis of being low?
- General criteria h/m/l. If it is compromised can you continue to perform your function.
- Blackstart relying on remote communication. Regional restoration plan is a way-documented.
- Final step is to combine the assessment to the look up table. How many systems are you protecting for?
- Redundancy is another complexity issue. Identify the primary preferred blackstart paths. Three primary blackstart cranking paths. Protect all the same. Need to protect any of them. What are you protecting for.
- Redundancy is protection for failure not for compromise. Issue of redundancy- dealt with at identification of BES subsystem.
- How should we deal with redundant cyber sub-systems? Should redundant equal same?

- Planners might argue that redundancy has an impact- might not solve all but most.
- Standards today- generators- engineered the utility grid so that nothing is critical?
- On the cyber side- even if you have four redundant systems, if one gets the virus, all may have it depending on connectivity. Have to plan that way.
- Issue is if you don't protect those 2 systems, all could be compromised through cyber means. Often don't know when compromised.
- Set of cyber systems, applied an impact category on it. How do we apply our controls? Local control system in a generating plant.
- Can we have a meaningful discussion of controls?
- Is a cyber system a DCS? Targeted protection. What is a DCS? 1000s of cyber systems or one system with an impact rating.
- How much flexibility should there be for the entity?
- If you apply single category to that is is clear what you need to do, but it takes long time to get done.
- Multiple levels of granularity- don't know what to do and we risk spending all your time figuring out what to do.
- Simplicity vs. complexity. You need the analysis so to apply security controls.
- Currently defining down to a CCA level. It may be the DCS and a subcomponent brings along the baggage of the DCS.
- Define target of protection- several controls will be common across
- Risk management- and address TFE.
- How does this work within a FISMA framework. DCS at Hoover. Microprocessor devices. Expectation from NIST?
- The understanding in NIST is that you analyze the security engineering process on your system. Go through and determine if it is a moderate impact system. Here are security controls I need to comply to the system.
- In order meet this requirement, you need to meet this access control by applying to central access control management.
- E.g. measurement of flow on spillway.
- "Scoping and Tailoring"- is the NIST term. Scope it out. Provide rationale as to why not. Oversight on process? As long as you can argue and win with your IGs. Puts lots on the auditor for quality types of assessment.
- Should we apply controls at cyber system level, or a methodology to a device level?
- As a team should we think about a different path?
- You may need to go down to the equipment level not stopping at systems.
- Go further down from DCS system level to the component level to effectively apply the controls.
- Scoping the target of protection- you need to tailor it? Do we further subdivide? TOP-DCS.
- DCS: 1 or 2 primary processors/computers, operating work stations, engineering work stations, HMI, slave components, data acquisition components, interfaces to business system.

- TOP universe of systems you need to protect.
- What do we apply controls to: system or components of the system? It will depends on the control. No cut and dry answer.
- Risk management framework uses compensating controls. You can meet the intent of control on component by doing other things.
- How have the federal agencies implemented 800-53 to field devices. Apply to individual level?
- Use a 'Control inheritance' concept and use the "tailoring and scoping" exercise. Come up with Compensating controls. All of this is documented in the security plan appropriately. Acceptance of risk is not allowed by FERC. How can we develop a hybrid approach?
- Puzzle pieces are fitting together better through this discussion.
- One-to-one mapping between reliability functions and BES subsystem may not be possible.
- How can we address interconnected systems and systems we are dependent?
- Identified cyber system focusing on and components making up system.
- What we haven't done is defining target of protection.
- Determine interconnected cyber systems that support the BES functions. E.g. DCS- in the model is control equipment- interconnected cyber system? It depends. On how you connect workstations to them. Network design is important to note.
- Once BES system is in scope. We need to determine how the system resides in the architecture and what are the components within system.
- Does ranking of components consider the factor of functions or connectivity?
- Connectivity defines controls or high/medium/low.
- Distributed control systems- plant controls- generator.
- What about interconnectivity with other systems that are ranked differently?
- Typical DCS may not communicate off campus.
- Assumption that identified TOP- done the methodology- interconnected systems inherit the rankings. TOP – assumes BES cyber system is a single element? Drawings suggest already part of system.
- E.g. Conflicker worm- hooked up to internet- through dumb workstations.
- Difference in understanding and perception- of a system from an operations side or a data side. This is the old model- look forward to new model.
- Target of protection model value- what is my realm of influence if compromised?
- Access control is key to security- network, operating, application and facility layer.
- TOP- e.g. email server. High impact. TOP control center- Rules and what applies- need to distinguish- unique target areas. TOP- showed how when you got to BES cyber system- interconnected nature- won't know where to place your control. Email server- negligent case of putting on same network at DCS switch.
- Inheritance of levels into collateral systems- apply same analysis on these systems as we apply to other. Impact on mission- each cyber system impact/support mission- calling that reliability functions.

- TOP- apply the same analysis to these. Some may rely on email systems more than others in terms of impact – fulfillment of mission. We learned they needed redundancy of email systems.
- When federal organizations categorize their systems- they consider the potential impact to missions, assets or individuals. Consider potential impact to other organizations they are connected with.
- The lowest level needs some level of security.
- The reason systems outside of BES cyber system. In TOP collateral- could be compromised and could compromise. Required for operation of BES cyber system. Impact on BES cyber- leads to categorization. This is not because of their inherent effect on reliability function itself.
- Concept paper does good job of explaining in TOP- have to secure because they could be a entry point for compromise.
- Identifying Cyber system and TOP. Does TOP just scope how you hare defined your system. Helps you determine what you need to protection.
- Collateral systems- if there are no requirements- won't make it into a standard.
- TOP- 3 in paper- prototypes- 3 environments we built them for. Shouldn't be hard fast rules of what should be where. Auditor should look for this.
- Higher level steps in the process. Concerned about value added.

Concluding Comments- Functional Approach Walk-Through

- What we defined the bicycle- reaction on the whole step through
- First steps- some were confused about the value adding of the step. Think about eliminating and moving on to important steps.
- Last step- TOP passionate about.
- Any candidates for eliminating or simplifying?
- 1st part is more conceptual and complicated. Latter part is more grounded.
- 1st part is new where applying security controls is not new.
- This can be can be simplified. The complexity may be more evident in the development process, where the final standard may be simpler to present.
- TOP- Subgroup 4. Will come out in the controls section. Put a boundary of some sort around the system and protect it.
- We are moving away from perimeter protection and move towards influence control.
- There remain fundamental gaps between 2 groups approaches.
- Need to address how much flexibility. How will we present this to industry? We need a simpler recipe.
- This remains Confusing. How do we expect the industry to understand this? Too complex and confusing. Industry won't buy. Congress will ask whether you have secured the system and they feel that the industry not being forthcoming in their comments regarding money.
- We should seek to integrate the pieces or simplify the entire model.

- It this predicated on the maturity of industry? Cyber security-maturity models are still 3-5 years out.
- What is the SDT's understanding of the maturity level of the industry in terms of security? Don't have a good feel for where the industry is in thinking and acting on this.
- Simplifying CIP 002 is going to be imperative.
- We should develop a strawman set of thresholds to test drive among us. Today's exercise helped show implications of the concept and we learned a lot. What do we need to do to move the level of maturity in the industry along. More proscriptive may be justified today. Not traditional reliability.
- What is the SDT philosophy and approach- i.e. degree of flexibility vs. prescriptive, guide or impose. How to go about this? What is our strategy.
- Give the industry some flexibility to make some of their own decisions? Trying to get away from the current scheme? How much less latitude. If we offer room for judgment, we will give latitude.
- Are we blending the two? Hard limits, low water mark. Entity could provide alternative through analysis. Implication is the complication in the standards?
- Low water mark- opt in and add to it- increase their compliance footprint.
- Engineering analysis needs to support any thresholds. Do this as part of setting the standard.
- Seek simplification with how to go about this. Achieve some simplification: workable, clear and doable.
- Readiness assessment- was eliminated – had some excellence of operation.
- Compliance audit- immature organization. Some organization do betters than others.
- Audit- prohibited from going and making kinds of recommendations.
- Review existing and trying to develop more performance based standards?
- Should lay out what you need to do vs. how to do it.
- The problem with CIP 002 may be 003-009
- What would happen if left risk methodology in CIP 002. If fixed 003-009 would every one say.
- Response to industry from the drafting team should convey that we have read comments and we are considering things.
- De we make time to try another model? Model is in the concept paper. It identifies for us things we could keep in mind.
- Who can determine impact to the reliability of BES? Owner of asset has to even if they have no way to. Is this the right way to go. Who has wide enough view and is willing to do this.
- Consider the Abeline paradox regarding the impact of group think.

B. Walk-through- Cyber Approach

On day two, Joe Doetzl reminded the SDT that the concept paper offered entities the choice of an alternative approach that started with the cyber systems and map those. The concept suggested that the different starting points should result in the same ending point. The

complexity comes from the BES mapping and reliability functions and different levels of impacts on each of those systems. The question is whether if you start with the cyber system it will be a simpler approach to cyber security than starting with the reliability functions.

Member Walk-Through Key Questions

- What would a responsible entity do in determining what should be in the scope to protect?
- On cyber side, if the cyber is deemed impactful does it inherit the impact level/ of the function supporting the BES assets? Is anything not impactful not in scope?
- For the assessment of functions or on asset supporting reliability function, do you need an intermediate step?
- Do we agree we want to have multiple levels of impacts on function so we can connect the controls to those?
- Can the assets mapping be capable of translation to a systems approach?
- Any way to diminish the impact of the audit process on low impact sites?
- What does it mean for a BES cyber system to support a reliability function. Is it info for situational awareness, control to generation, etc?
- Are there systems we unequivocally expect to be protected? Basic SCADA systems shouldn't have a minimum set of auditable controls. Even isolated generation. This might take some complexity out.

Step 1- Inventory Cyber systems Involved

At the entity level, for this example, assume a complete inventory of cyber systems. A list of cyber systems you may find in a typical utility could include:

- Customer info and billing systems
- Financial info systems
- HR system
- EMS system
- Blackburn generating unit (2) and associated control system. (black start system)
- Load Master Units 1-8-single control system for all units
- Distribution automation system.
- Protection system (relays)

Member Comments

- 1000s of systems that won't fall into list. Monitoring, desktop systems, Corporate info security vs. power. Guidance will be needed to industry help understand what should be included on list. For example, what is the process for ruling out the HR system?
- Assume multiple security officers and do this more than once.
- What would a responsible entity do in determining what should be in the scope to protect? If start with cyber system need all cyber systems in inventory.
- Assume separate corp. systems from control? Manageable group of systems.

- At some point make an analysis that it isn't connected with reliability- impact categorization?

Step 2- BES Mapping for These Systems

Joe Doetzl suggested the key question here was do these systems directly support the reliability of BES?

- Customer info and billing systems NO
- Financial info systems NO
- HR system NO
- EMS system YES
- Blackburn generating unit (2) and associated control system. (black start system) YES
- Great Big Coal Burner Units 1-8-single control system for all units (big enough) YES (based on functions-
- Distribution automation system. ?? Depends- YES
- Protective system (relays) YES
- Smart grid (maybe, depends)

Member Comments

- AMI unit?
- Will distribution be covered? No, Federal Power Act- excludes distribution.

Step 3. Perform Impact assessment to determine what level of impact cyber systems on reliability of the BES.

BES Mapping Subgroup will be helping to address this through their mapping. In the alternative, any connection must put control on. We should give industry flexibility in choosing which controls will get them to baseline security for their assets. Ask the question, what is your worst-case scenario if this cyber system goes bad do the assessment.

Member Comment

- Assessment of functions or on asset supporting reliability function. Need an intermediate step.
- EMS will be easy case to tie to BES.
- In our BES mapping document we provide a methodology for saying H/M/L. Maybe there is a way to translate John Lim's work to get to H/M/L buckets.
- Complexity lies in that mapping.
- Alternative is if there is any level of impact- that dictates what you need to do.
- When do you look at inputs to the system to determine whether in scope? TOP approach?
- Step 4- look at this in examining security of each system. If our EMS system has a connection into HR system, brings it back in. Running on same server you are back in.

- Need to add a lot of detail to bring this together. We haven't done what this implies.

Step 4. Apply controls appropriate to the level of impact each cyber system needs to have.

Member Comment

- How will the level of impact be done?
- Should we do away with the impact of the cyber system itself? If the cyber system falls into category because it falls within one of the BES functions- That system automatically falls in the high. Have to make assessment of what is the effect of the cyber system if compromised, on the BES subsystem and make a determination then of what category would fall in.
- Confidentiality, integrity and availability of the system lost- resulting a categorization at H/M/L. Assessing the EMS system and go to functions mapped to- go to table being developed by John Lim vs. a matrix. It will have the BES cyber system and will help determine what the impacts would be using the impact "look up tables." Alternatively, no flexibility, this is set in advance.
- Choose in standard development process. Does your cyber system support reliability? If yes, apply baseline set of controls.
- SM: how do you do #3.
- Look at impact- generator- load support and system stability, ability to provide megawatt, loss of mw in short period of time. In restoration it doesn't. Depends on which impact you are looking at.
- Do we agree we want to have multiple levels of impacts on function so we can connect the controls to those? In end multiple levels of cyber systems impact on function.
- Categorization of cyber assets- if impactful, all or nothing, similar to CIP today.
- By starting with ALR, have we caused confusion? This e.g.- pp 17, entities may choose to use an alternative approach. Alternative method- straw dog.
- While the industry is not necessarily that familiar with the ALR, start with systems that are essential to the tenets in the ALR- e.g. to restoration. All the systems that support these things. Cut down the confusion about inventory.
- Mapping that John Lim has done has been on assets not systems. Maybe able to translate it to a systems approach. Customized to provide tool for systems not assets.
- Don't think this departs from 3 levels of impacts. Binary on cyber analysis side. Still have mapping to subsystems with H/M/L. You just look at whether it supports.
- 2 levels of impact analysis. BES asset and cyber impact analysis on assets/functions. Simplifying either one into binary step. Simplifying both would be drastic and less palatable.
- Complexity of impact assessments is large. In the end you have appropriate controls, are we better served than by picking a set of controls. Put on everything. Don't know yet in terms of controls.
- MITRE study that Jason Marshall talked about CIP 3-9 didn't meet the NIST moderate baseline.
- Would get industry documenting controls.

- Are we taking steps backwards? Not taking account levels. Check everything and add controls. Trying to do too much on cyber stuff and not worrying about BES first.

C. Lessons learned from the Walk-Throughs

SDT members discussed what was learned through the walk through of the functional and cyber approaches. Below are a summary of their comments:

- The two walk-throughs indicated there is a similarity in complexity in both approaches.
- The issue is how do we eliminate complexity not on which side we start the analysis. For example in the cyber approach the complexity is contained in Step 3 whereas in the functional approach it appeared in Step 2.
- Neither is more complex that the other as it will depend on the environment and context. Large number of BES and small number assets may start on cyber side. Small number BES and lots of cyber may want to start on the BES functional side. Neither is wrong.
- The categorization process for government systems is not cut-and-dried with ambiguity in it. Organization provides enough evidence to bosses that this is a correct categorization. Need something more cut and dried. Possibly thresholds. More consistent and cut and dry.
- Rather than dwell on 1 method that identifies 5K vs. 50K then big issues, we should be getting the same generally from both.
- Confusion about this in terms of what it would mean in changes. Simplification comments came. Simplify by saying you have to do a lot to everything. Flexibility in what we do to them. The latter is what we have today. Here is everything you have to do.
- If you simplify step 3- broad brush- not in the paper. Option #1- broad swath doing something to lots of things, you figure out what you want to do.
- The SDT should put in a lot of work in reducing complexity of the process. Make it clearer on where we are heading. On cyber side, is the cyber impactful, then it inherits the impact level/ function it supporting of the BES assets. Anything not impactful is not in scope. Could be one way to simplify the process.
- Eliminating cyber h/m/l.
- This is simpler than yesterday- fewer steps. Took less time. In support of simplifying the process. 2 impact assessment one for assets and one for systems.
- One is binary and the other is 3 levels.
- Is the team in support to simplifying the approach?
- Reducing the assessment to one that is binary vs. 3 levels to simplify?
- Assumed the BES subsystem impacts. Had the same complexity. Still have to look at BES subsystems.
- Performing impact on reliability functions.
- Define what it means for a BES cyber system to support a reliability function. Is it info for situational awareness, control to generation, etc?

- What does success look like for us at a Team? Do we get consistent and good answer going on both approaches. Part of problem in evaluating 2 different approaches. When everyone applies, do we get the same answer and does it provide BES reliability.
- Success=
  1. multiple groups of people running through the process with same inputs and requirements reach the same conclusion.
  2. End result passes the smell test- engineering analysis would agree with the results.
- Having too much is not as dangerous as not enough of the right thing.
- Success= a clear enforceable standard that doesn't create an unnecessary hardship on entities.
- Reliability functions important- protecting something and knowing why this is beneficial.
- E.g. generators- size, time and connectivity are considered. Focus on reliability functions can demonstrate reliability of BES.
- What will be the ultimate impact on entity?
- Complexity- current standard- complexity at the entity. Take complexity into the standard, doesn't go away.
- Are there systems we unequivocally expect to be protected. Basic scada systems shouldn't have a minimum set of auditable controls. Even isolated generation. This might take some complexity out
- SM: hide complexity behind the scenes in supporting documents and have some thresholds that are not arbitrary and capricious. Some threshold number a basis in power system engineering. Generation transmission and control centers.
- Simple- multiple step. Spend time figuring out the buckets.
- 4 Interconnections- transmissions characteristics within and between. 19 # in JLs document. Publish paper that justifies thresholds.
- Sacrilege to the planning and operating group.
- Simplifying what the expectations and obligations of what industry have to do.
- Rod: H- depends on what controls you are talking about. No explanation of what is happening downstream. Make decisions to place assets in too high a category. Costing a fortune for daily maintenance.
- More heavily weighted toward a high impact because of implications in implementing controls.
- Set of criteria- you have some high, more in medium and a heck a lot in low category. More rational and justifiable methodology.
- What will be the bucket sizes 10% less high, 40% less medium, 50% low. If we that many high assets something is wrong with the criteria.
- Yes we could come up with some numbers. New CIP 005 controls. 1000 RTUs and downstream devices with user management on them.
- Come up with classification levels and set of controls. Look at how applies to field distributed devices, substations, etc. This is where the push back comes from.
- Supports when you look at control system. what are the components of that system? Focus on impact and the function of device. This helps to set up boundaries.

- Impact analysis of cyber system: determine what is it's span of control? A relay on a single line is a small span of control. How much control with a single cyber system.
- Does low not mean zero? Baseline everywhere.
- Address cyber systems that have no impacts.
- Do we have a good handle on what is industry security posture? Significant number of entities avoiding audit world. Is there another way- certain auditable levels with high. Any way to diminish the impact of the audit process on low impact sites?
- ERCOT implemented for all systems- technical security framework. Figured out 1 set of rules. Biggest headache is documentation of compliance especially doesn't contribute to security baselines. Things in the "high" bucket auditable compliance. In reliability business, key to reliability is change control. Integration testing etc. Concerned about federal model and the volumes of documentation that may be required.
- How should we treat aggregated BES systems- 30 generators. In the categorization we should give consideration to aggregate assets with their own impact assessment performed vs. based on asset.
- Bringing up concept Jackie Collett brought up yesterday on a subsystem basis. Meeting multiple criteria at medium. Does it bump up from medium to high?
- When compound a bunch of functions- have to look whether it magnifies the impact? Is there any consideration for some kinds of redundancy?
- On the cyber side- span of control- from one plant to lots of plants. Do you factor in redundancy? Master control center and remote units. Are each as important as the Master?
- Control Center- doing something for one generation station. Cyber high. 1 low BES vs. 30 low BES.
- Span of control of asset that has overview over multiple.
- Didn't expect that system would get down to that granular level.
- Evaluating device as a control system. Cyber system has a common impact to multiple BES system- analyzed under a span of control.
- If I have connectivity to systems what is the scope of influence. Address a field system and a breaker on in terms of scope of influence? Span of control? Can you impact a high enough level e.g. of mw.?
- If on the same network- can I impact multiple units? Other considerations that are not covered.
- Work through these issues on a case study basis.
- BES subsystems- stretched thin when you deal with these sorts of things, e.g. high pressure oil lift system.
- We need flexibility so that standards lead you to the right conclusion.
- Area impacts. The control center is where the impact is assessed.

V. SUBGROUP REPORTS TO THE SDT

On the first day the SDT heard and discussed reports from each of the subgroups. The subgroups then met on second day to review and respond to the comments and suggestions of the SDT.

A. Reliability Functions Subgroup Reports, *Rich Kinas*

1. Day One Report

On the first day Rich Kinas reported, on behalf of John Varnell, on the Reliability Subgroup's work since the last meeting covering the following points:

- Defining Functions Critical to reliable operation of the BES
- 9 functions initially but after making some changes up to #5 there are probably only 8 functions
- "Balancing Load part of controlling frequency"? Leave it stand alone to make more sense to the industry
- Not planning to go further than 3 levels down.
- Tried to identify the functional subsystems that would have to be addressed.
- At which step of the process, do entities fall out of the flow? Consider within each of the 4 subgroups
- The BES Mapping subgroup (John Lim et al) is setting up thresholds.
- The SDT needs to be thinking of the subsystems and pieces of sub systems that will perform these functions.
- Address and protect everything in subsystem whether you own it or not.

Member Comments

- The Subgroup got feedback from John Lim's Mapping Subgroup.
- At the highest level- look at ALR and refine what this means in the world? All the current reliability standards are direct descendants of the ALR.
- Burning question- what do we do with this list? Input to scope the BES subsystems and cyber systems. Or are we defining impact? Where do we go from this list?
- The Subgroup wrestled with this. The sooner we define impact, the better. Do we do this before addressing subsystems?
- Impact criteria table-of several pages long- Will industry want this? Understand this?
- Create a list of questions that each entity had to answer, result would determine whether they meet the criteria or not? And at what level?
- At what level do you ask those questions. For every function? Take it to level that is feasible by December. Cant go to 3rd level.
- Look at individual functions vs. very generic criteria
- A question at top under dynamic response-
- BES Mapping subgroup – not going to go towards an increased granularity of functions. Define the scope of what subsystems should we apply the impact categorizations to. List of what must be included and categorized
- Impact criteria- high level only is the focus. List will help entities come up with list of subsystems that are required to be impact categorized.
- E.g. control and operation function-

- Would it be more beneficial- Should the mapping subgroup requirements fall under these? May not map to the functions.
- Some mapping criteria for every functions? Perhaps but extremely cumbersome and obtuse.
- Invested lots of effort in these functions to center the standards around. If we use these functions to get the subsystems it will move the complexity to Jackie's subgroup.
- This 3rd level of detail looks like BES sub systems. E.g. protection systems down to detail, sounds like a BES subsystem.
- Used these to trigger what we were thinking.
- This has been good work but the SDT is struggling with where are we going with this? What is the vision we are trying to put these pieces together to do?
- Take first one and flow all the way through. See how it might work.
- Keep looking for the integration of the problems/challenges.

2. Day Two Report

- The subgroup has redistributed its members into other subgroups.
- We will continue to try to put more definitions around what was meant by different functions.

Member Comments

- What we have from the subgroup is a list of functions. It would be helpful to have a brief paragraph on each and what is meant for benefit of and guidance to the other subgroups.

B. List of BES Subsystems/BES Cyber systems Subgroup Report and Reflections on Industry Comments, *Jackie Collett*

1. Day One Report

Jackie Collett noted the subgroup had no further meetings since the August Charlotte meeting. She noted that Jim Case and Matt Greek from Operating Committee are now participating on the subgroup.

2. Day Two Report

Jackie Collett presented the Subgroup's report on day two noting that they still need to put time and effort in defining what these BES subsystems are and move into drafting requirements.

Member Comments

- Consider some of these things for simplification on part of this? Requirements based on reliability functions- identify things they are doing that are more important. Maybe on the cyber assets.
- Agree- 2 modes of impact on BES assets and systems. Are we going to continue along both modes of analysis? If not, are we going to utilize impact assessment of both cyber assets and systems? Simplify the two impact analysis.
- BES identification of assets and impact analysis of BES assets.
- Streamline one of those impact analysis. Impact analysis of the cyber system. Will be utilize the output. So they get appropriate direction from the meeting.
- Concern about removing a necessary part of what we are doing.
- Simplify the process. Need to fill in a few more gaps. Look at some of these issues. Don't have all the pieces. This won't be simple. Need to have something that ultimately looks simple.
- Some gaps that need to be filled in. BES subsystem side work. Look at JL's work has done in detail.
- Try to determine where you get any simpler.
- May be an issue that we need to explain how we got to where we are.
- A lot of the complexity in the process is work the SDT has to do. Not necessarily what gets into the standard. Concept paper was similar to this as well. Get requirements on paper that are simple for entities to follow.
- Agree. Identified an ideal vision- down to a "cable driven" methodology. Team still has to go through the exercise. The gaps need to be identified since they will guide the empirical thresholds we need to establish.

Jackie concluded noting they would not say no to volunteers joining them on the work ahead.

C. BES Mapping Subgroup Report and Reflections on Industry Comments, *John Lim*

1. Day One Report

The Subgroup met September 3, 2009 to continue its work in developing the BES Mapping draft markup. The Subgroup was joined by members from the Functions subgroup. John noted two major issues the subgroup is dealing with:

- How do we validate an engineering study? Approval by regional reliability assurer? TFE type process? Need to look at this more. Not a lot of entities currently performing the role of reliability assurer.
- "Misuse"- need to describe this term. What is meant by this? Candidate for NERC Glossary

2.1.6- This addresses how transmission operators or owners classify as high if servicing a generation owner. Currently doesn't have to notify owners of the impact status of their BES systems. This might be an overall point or spread throughout. Thresholds- we can use as long as they are based on some method for the entity. Needs to be the possibility of a challenge of validity through engineering study. Use the numbers with some caveats?

Member comments

- Validation of engineering studies? A number of places reference this. How is this done?
- 3rd party approval is probably not the right approach. Big issue in terms of quality control.
- Can't have "fill in the blank" standards according to FERC. E.g. Regions will develop something everyone in region will have to follow. What we can do, NERC wide standard with different thresholds for different regions or interconnections.
- One of the changes in this version- Eastern and Western and other interconnections might have different thresholds.
- Criteria combines identification of functions and subsystems? Make the process less complex. Would it make sense to do a gap analysis on this criteria? Would reduce complexity.
- Welcome the reduction of complexity. 19 different criteria for this piece alone. How can we compress and simplify? If gap analysis can do this we should explore.
- Concerned that this drafting team puts out hard numbers without engineering analysis behind it. Somehow we need to address this head on.
- These numbers will have to have an engineering basis.

2. Day Two Report

John Lim reported following the Subgroup's meeting on day two. The Subgroup is drafting a set of requirements for High, Medium, Low. There are still questions on how to handle industry studies. In terms of generation sub systems, we are using terms that are not very well defined. E.g. subsystems in generating stations. The terminology we are using must be precise and consistent. We need to get together with Jackie Collett's subgroup. We don't believe there should be an expectation of a 1-to-1 mapping for every function. The rest of the subgroup's work will need to be coordinated with Jackie's subgroup and include input from John Varnell's functions subgroup and from the OC and PCs get something in a better form. Subgroup 1 has participated in past meetings.

D. Cyber Analysis Subgroup Report, and Reflections on Industry Comments, *Phil Huff*

1. Day One Report

Phil Huff delivered the initial report noting his confusion about how the subgroup should go forward. BES impact categorization as the black box is a failed assumption. Our team could reduce some of the complexity in the process. We assumed each function mapped would have an impact categorization so we could combine through a "look-up table."

Member Comments

- External cyber system- address that as a control?
- Target of protection- no requirement just trying to get definition down.

- Our problem is that we are dependent on how the pieces fit together.
- We should focus on impact subsystem.
- Need to determine what we are going to do with the reliability functions.
- Our team's confusion results from the fact that we don't have a clear vision as to how this fits together.

2. Day Two Report

Phil Huff noted that his subgroup would huddle when the SDT breaks. He noted that there may not be as much confusion as we stated yesterday. Impact criteria that are involved in John Lim's one-to-one mapping. Our team needs to develop on the cyber analysis side.

E. Definition and Selection of Controls Subgroup Report and Reflections on Industry Comments, *Keith Stouffer*

1. Day One Report

Keith Stoffer presented the subgroup's report. He noted that during Charlotte meeting the subgroup developed and presented an example based access control. We pulled together into one location the access control referenced in many places. Keith mentioned that the format is new and the subgroup doesn't know if this is acceptable. Need to nail down as soon as possible what is an acceptable format.

Member Comments

- Scott Mix noted an informal discussion with Gerry Adamski at NERC who indicated an openness to doing something to meet requirements. Front of each. Note the categorizations that it applies to.
- Have a table and checkmarks for those that apply.
- Use e.g. re-format.
- Access control- come up with sample sets, won't be meaningful until related to.

2. Day Two Report

The Subgroup will seek to nail the format decision down with NERC. E.g. exemptions. How we deal with conditional requirements? How do we deal with "Requirement"- H/M/L Critical path. What if we run into a brick wall? This is challenging as it is a moving target. Joe Buchiero will send latest work in progress of the Subgroup to all group leaders.

Member Comment

- Select an e.g. that has differences between high, medium and low.

VI. NEXT STEPS AND CLOSING

A. Industry Comments Review and SDT Response

- We will need to take regional differences into account in the standards.
- We haven't yet determined whether there is a null set or just H/M/L. Big issue we need to come to consensus on early.
- Concerns around increasing scope of what we are doing. Have to address this.

Gerry Freese agreed to draft a statement on behalf of the SDT for publication in NERC's newsletter thanking the industry for their input on the concept.

The Chair reviewed with the SDT the schedule for the next couple of meetings reminding members that at the conclusion of the October meeting in Kansas City we hope to have a single text of CIP 002 which we can refine in November and December. She thanked the members for their hard work together and in the Subgroups and encouraged them to continue working to make headway on each of their charges.

She noted that she would draft up the letter to the Standards Committee Chair based on the SDT's discussion of the TFE and Urgent Action approach at the August meeting.

Members completed an onsite meeting evaluation form *(See, Appendix #3).*

The SDT adjourned at 3:45 p.m. on September 10.

Appendix # 1— Meeting Agenda
Project 2008-06 Cyber Security Order 706 SDT
14th Meeting Agenda
September 9, 2009, Wednesday - 8 AM to 5 PM PDT
September 10, 2009, Thursday - 8 AM to 5 PM PDT
Western Area Power Administration, Sierra Nevada Regional Office
114 Parkshore Drive
Folsom, California
(916-353-4416)
NOTE: Subgroup Meetings May Not Have Access to Telephones and WebEx

Proposed Meeting Objectives/Outcomes

- Review the CIP 002 Workplan going forward
- Receive updates on TFE, VSL/VRF and related cyber security efforts
- Receive an overview of industry comments on the SDT concept paper
- Receive and discuss reports from CIP 002 Subgroups identifying key issues and coordination points
- Convene CIP 002 Subgroup meetings
- Receive and discuss Subgroup reports on progress made and responses to industry comments
- Agree on Workplan, next steps and assignments

Draft Agenda

Wednesday September 9, 2009

8:00 a.m.	Welcome and Opening Remarks- *Jeri Domingo-Brewer* Roll Call; NERC Antitrust Compliance Guidelines Facilitator review of August 20-21 Charlotte meeting summary and adoption
8:20	Review of Meeting Objectives, Agenda and Meeting Guidelines- *Jeri Domingo Brewer and Bob Jones*
8:30	Review of CIP 002 Workplan and CIP 002 Subgroup Process- *Stu Langton*
8:40	Webinar Report- *Jackie Collett & Phil Huff & Jeri Domingo Brewer*
8:45	Update on Technical Feasibility Exception (TFE) NERC Rules of Procedure – *Jeri Domingo Brewer and Scott Mix*
9:15	Update on VSLs/VRFs- *David Taylor or Scott Mix*
9:20	Update on other related cyber security initiatives- *SDT Members*
9:30	Overview of the Industry Comments on the Concept Paper- *Scott Mix*
10:00	Subgroup Reports to the SDT 1. Reliability Functions Subgroup Report and Reflections on Industry Comments, *John Varnell,* Q & A
10:40	*Break*
10:55	2. List of BES Subsystems/BES Cyber systems Subgroup Report and Reflections on Industry Comments, *Jackie Collett*, Q & A

11:35	3. BES Mapping Subgroup Report and Reflections on Industry Comments, *John Lim* Q & A
12:15	*Lunch*
1:00	4. Cyber Analysis Subgroup Report, and Reflections on Industry Comments, *Joe Doetzl*, Q & A
1:40	5. Definition and Selection of Controls Subgroup Report and Reflections on Industry Comments, *Keith Stouffer*, Q & A
2:20	Coordination Discussions and Plans among Sub Groups
2:45	Subgroup Meetings *(at various locations)*
5:00	*Recess*

Thursday **September 10, 2009**

8:00	Subgroup Meetings
11:00	Welcome and Agenda Review- *Jeri Domingo-Brewer*
11:05	Subgroup Reports – *Plenary Session* 1. Reliability Functions Subgroup Report and Reflection on Industry Comments, Q & A
11:50	2. List of BES Subsystems/BES Cyber Systems Subgroup Report and Reflection on Industry Comments, Q & A
12:35	*Working Lunch*
1:00	3. BES Mapping Subgroup Report and Reflection on Industry Comments, Q & A
1:45	4. Cyber Analysis Subgroup Report and Reflection on Industry Comments, Q & A
2:30	5. Definition and Selection of Controls Subgroup Report, Q & A
3:15	Discussion of and Agreement on Subgroup Coordination Strategies
3:30	Review Work Plan- • Review Next Steps for Subgroups and SDT and the creation of a single CIP 002 text
3:50	Review Proposed 2010 Meeting Schedule
4:00	Review October Kansas City, Missouri Meeting Objectives
4:10	Meeting Evaluation
4:30	*Adjourn*

Appendix # 2 Attendees List
September 9-10, 2009 Folsom, CA

Attending in Person — SDT Members

1. Rob Antonishen	Ontario Power Generation (Friday)
2. Jeri Domingo-Brewer, Chr.	U.S. Bureau of Reclamation
3. Jim Breton	ERCOT
4. Jackie Collett	Manitoba Hydro
5. Jay S. Cribb	Information Security Analyst, Southern Company Services
6. Joe Doetzl	Manager, Information Security, Kansas City Pwr. & Light Co.
7. Sharon Edwards	Duke Energy
8. Gerald S. Freese	Director, Enterprise Info. Security America Electric Pwr.
9. John Lim	CISSP, Department Manager, Consolidated Edison Co. NY
10. Frank Kim	Ontario Hydro
11. Christopher A. Peters	ICF International
12. Scott Rosenberger	Luminant Energy
13. David S. Revill	Georgia Transmission Corporation
14. Kevin Sherlin	Sacramento Municipal Utility District
15.Keith Stouffer	National Institute of Standards & Technology
1. Roger Lampilla	*NERC*
2. Scott Mix	*NERC*
3. Joe Bucciero	*NERC/Bucciero Assoc.*
4. Robert Jones	*FSU/FCRC Consensus Center (Wed. & Thursday)*
5. Stuart Langton	*FSU/FCRC Consensus Center*

SDT Members Attending via WebEx and Phone

1. Phillip Huff	Arkansas Electric Coop Corporation
2. Rich Kinas	Orlando Utilities Commission
3. Jonathan Stanford	Bonneville Power Administration
4.William Winters	Arizona Public Service, Inc.

SDT Members Unable to Attend

1. David Norton	Entergy
2. Kevin B. Perry, Vice Ch.	Director Critical Infrastructure Protection, Southwest Power Pool
3. John D. Varnell	Technology Director, Tenaska Power Services Co.

Others Attending in Person

Sam Merrill	CERT/SEI
Michael Toecker	BMcD
Peter Schneider	Subnet Solutions

Others Attending via WebEx and Phone

James Bassett	Lafayette
Matt Greek	
Rob Hardiman	
Doug Johnson	ConEd
Bill Johnson	TDI 9-9
Peter Schneider	
Jeff Gillan	ATC
Sam Merrill	9-10

Appendix # 3 — Meeting Evaluation Feedback Summary

CYBER SECURITY ORDER 706 SDT
SEPTEMBER 9-10, 2009, FOLSOM CA
MEETING EVALUATION FEEDBACK FOR INCLUSION IN FACILITATOR'S REPORT

Members used the following 0 to 10 scale in evaluating the meeting: 0 means totally disagree and 10 means totally agree.

1. Please assess the overall meeting.

7.78 The agenda packet was very useful.
6.83 The Webex document display and the audio were effective
8.50 The quality of the meeting facility was good.
7.40 The objectives for the meeting were stated at the outset.
8.30 Overall, the objectives of the meeting were fully achieved.

Were each of the following meeting objectives fully achieved:
7.90 Review the workplan going forward and assess "Version 2.5" possibilities.
8.10 Receive MRC presentation and Leadership Coordination Meeting summary.
7.13 Receive updates on TFE, VSL/VRF and related cyber security efforts;
8.50 Receive and discuss reports from CIP 002 Subroups identifying key issues and coordination points;
9.00 Convene CIP 002 Subroup meetings;
9.20 Receive and discuss Subroup reports on progress made; and
8.80 Agree on Workplan, next steps and assignments.

2. Please tell us how well you believe the Team engaged in the meeting.
8.70 The Chair and Vice Chair provided leadership and direction to Team and Facilitators
9.20 The Facilitators made sure the concerns of all members were heard.
8.30 The Facilitators helped clarify and summarize issues.
7.63 The Facilitators helped members build consensus.
9.10 The Facilitators made sure the concerns of all participants were heard.
8.10 The Facilitators helped us arrange our time well.

3. What is your level of satisfaction with what was achieved at the meeting?

8.11 Overall, I am very satisfied with the results of the meeting.
8.13 Overall, the design of the meeting agenda was effective.
8.22 I was very satisfied with the services provided by the Facilitators.
7.89 I am satisfied with the outcome of the meeting.
7.25 I am satisfied with the progress we are making as a Team.
8.75 I know what the next steps following this meeting will be.

8.75 I know who is responsible for the next steps.

See other side

4. Other comments (use other side)

- Small groups good!
- I'd like the sub-teams to do most work offline rather than taking most of our time in sub-team meetings. We need more time together as a group reviewing each other's work and integrating it.
- The inclusion of additional personnel with operating experience was helpful.
- No space on the other side! Until everyone sees responses from the paper we are doing make-work. I believe our over all direction will change when we see the replays. I am a lemming running over the cliff because the facilitators don't know the subject and history. Jerry, Kevin, Jon D, Philip only know normal IT processes.

What did we achieve?

- Make work
- Concrete work on CIP 002

What are our biggest challenges going forward?

- Finishing the amount of work within time parameters.
- Teaching history.
- A coherent/consistent and clear CIP 002.

What suggestions do you have for making our group more productive?

- Sub-team meetings are difficult without projectors.
- Much work is being done in sub-team Silos. This approach created some of the issues with CIP v1. More coordination is required among the various teams to ensure all issues are addressed but NOT addressed by multiple teams.

Appendix # 4 — NERC Antitrust Compliance Guidelines

I. General

It is NERC's policy and practice to obey the antitrust laws and to avoid all conduct that unreasonably restrains competition. This policy requires the avoidance of any conduct that violates, or that might appear to violate, the antitrust laws. Among other things, the antitrust laws forbid any agreement between or among competitors regarding prices, availability of service, product design, terms of sale, division of markets, allocation of customers or any other activity that unreasonably restrains competition.

It is the responsibility of every NERC participant and employee who may in any way affect NERC's compliance with the antitrust laws to carry out this commitment.

Antitrust laws are complex and subject to court interpretation that can vary over time and from one court to another. The purpose of these guidelines is to alert NERC participants and employees to potential antitrust problems and to set forth policies to be followed with respect to activities that may involve antitrust considerations. In some instances, the NERC policy contained in these guidelines is stricter than the applicable antitrust laws. Any NERC participant or employee who is uncertain about the legal ramifications of a particular course of conduct or who has doubts or concerns about whether NERC's antitrust compliance policy is implicated in any situation should consult NERC's General Counsel immediately.

II. Prohibited Activities

Participants in NERC activities (including those of its committees and Subroups) should refrain from the following when acting in their capacity as participants in NERC activities (e.g., at NERC meetings, conference calls and in informal discussions):

- Discussions involving pricing information, especially margin (profit) and internal cost
- information and participants' expectations as to their future prices or internal costs.
- Discussions of a participant's marketing strategies.
- Discussions regarding how customers and geographical areas are to be divided among competitors.
- Discussions concerning the exclusion of competitors from markets.
- Discussions concerning boycotting or group refusals to deal with competitors, vendors or suppliers.

III. Activities That Are Permitted

From time to time decisions or actions of NERC (including those of its committees and Subroups) may have a negative impact on particular entities and thus in that sense adversely impact competition. Decisions and actions by NERC (including its committees and Subroups)

should only be undertaken for the purpose of promoting and maintaining the reliability and adequacy of the bulk power system. If you do not have a legitimate purpose consistent with this objective for discussing a matter, please refrain from discussing the matter during NERC meetings and in other NERC-related communications.

You should also ensure that NERC procedures, including those set forth in NERC's Certificate of Incorporation and Bylaws are followed in conducting NERC business. Other NERC procedures that may be applicable to a particular NERC activity include the following:

- Reliability Standards Process Manual
- Organization and Procedures Manual for the NERC Standing Committees
- System Operator Certification Program

In addition, all discussions in NERC meetings and other NERC-related communications should be within the scope of the mandate for or assignment to the particular NERC committee or Subroup, as well as within the scope of the published agenda for the meeting.

No decisions should be made nor any actions taken in NERC activities for the purpose of giving an industry participant or group of participants a competitive advantage over other participants. In particular, decisions with respect to setting, revising, or assessing compliance with NERC reliability standards should not be influenced by anti-competitive motivations.

Subject to the foregoing restrictions, participants in NERC activities may discuss:

- Reliability matters relating to the bulk power system, including operation and planning matters such as establishing or revising reliability standards, special operating procedures, operating transfer capabilities, and plans for new facilities.
- Matters relating to the impact of reliability standards for the bulk power system on
- electricity markets, and the impact of electricity market operations on the reliability of the bulk power system.
- Proposed filings or other communications with state or federal regulatory authorities or other governmental entities.
- Matters relating to the internal governance, management and operation of NERC, such as nominations for vacant committee positions, budgeting and assessments, and
- employment matters; and procedural matters such as planning and scheduling meetings.

Any other matters that do not clearly fall within these guidelines should be reviewed with NERC's General Counsel before being discussed.

APPENDIX # 5
Meeting Schedule
October 2008–December 2010
Development of CIP Version 2 and Version 3 Framework
October 2008–July 2009

1. October 6–7, 2008 — Gaithersburg, MD Reviewed CIP-002-CIP-009, Agreed on Version 2 approach.
2. October 20–21 —Sacramento, CA CIP-002-CIP-009 Version 2 development
3. November 12–14, 2008 — Little Rock, AR CIP-002-CIP-009 Version 2 adoption for comment and balloting; CIP-002-CIP-009 Version 3 process reviewed.
4. December 4–5, 2008 — Washington D.C. CIP-002-CIP-009 Version 3 reviewed and debated, SDT member white papers assigned.
5. January 7–9 — Phoenix, AZ, Reviewed Technical Feasibility Exceptions white paper**,** reviewed industry comments on CIP-002-CIP-009 Version 2 products — established small groups to draft responses, reviewed Version 3 white papers.
January 15 — WebEx meeting(s) Small group drafted responses to industry Version 2 comments.
January 21 — WebEx meeting(s) Small group drafted responses to industry Version 2 comments.
6. February 2–4, 2009 — Phoenix, AZ Update on NERC Technical Feasibility Exceptions process**,** VSL process and SDT role**,** review of Version 3 White papers, strawman and principles**,** reviewed and adopted SDT responses to industry comments on Version 2 and Version 2 Product Revisions.
7. February 18–19, 2009 — Fairfax, VA Update on Version 2 process**,** NERC TFE process and VSL Team process; reviewed, discussed and refined Version 3 CIP-002 White papers, strawman, and principles.
8. March 10–11, 2009 — Orlando, FL Update on NERC TFE and VSL and VRF Team process and review and refine Version 3 CIP-002 Strawman Proposals
March 2–April 1, 2009 — 30-day Pre Ballot
Mid-March — NERC posts TFE draft Rules of Procedure for industry comment
March 30, 2009 — WebEx meeting(s) White Paper Drafting Team
April 1–10 — NERC Balloting on Version 2 Products
April 6, 2009 — WebEx meeting — White Paper Drafting Team
April 8, 2009 — WebEx meeting(s) — White Paper Preview- Full SDT Conference Call
April 11, 2009 — Version 2 Ballot Results (Quorum: 91.90% Approval: 84.06%) and Industry Comments-
9. April 14–16, 2009 — Charlotte NC Update on NERC TFE process, VSL Team process and NERC Critical Assets Survey; agreed and adopted responses for Version 2 industry comments for recirculation ballot; reviewed and refined Version 3 whitepaper and consensus points and progress report to NERC Member Representative Committee (MRC) May meeting.
April 28 and May 6, 2009 — White Paper Drafting Team Meetings and WebEx
April 17–27, 2009 — Recirculation Results: Quorum: 94.37% Approval: 88.32%
May 5, 2009 — NERC MRC Meeting, Arlington, VA- SDT progress report.
10. May 13–14, 2009 — Boulder City NV Reviewed MRC presentation and further SDT refinement and discussion of the Version 3 White Paper.
June 8 and June 15, 2009 — Working Paper Drafting Team Meetings and WebEx
11. June 17–18, 2009 — Portland OR Further SDT refinement of the draft CIP Version 3 Working Paper(s), reviewed SDT development process for June-December 2009; discussed potential SDT subcommittee structure and deliverables.
June — WebEx meeting(s)

- Working Paper drafting group sessions including inputs from selected industry personnel to help establish BES categorization criteria

CIP-002 Development of Requirements, Measures, Etc. July-December 2009

12. July 13–14, 2009 in Vancouver, B.C., Canada

- SDT plenary session to review, refine, and adopt SDT Working Paper
- Adopt SDT response to NERC for Interpretation of CIP-006-1
- Review and adopt proposal for CIP-002 Subgroups and Deliverables
- Convene subgroup organizational meetings to develop work plans
- Adopt 2010 Meeting Schedule

July–August Interim WebEx meeting(s)

- CIP-002 Subgroup meetings (as needed)
- CIP-002 Coordination Team meeting (as needed)

August 3–5, 2009 in Winnipeg, Manitoba **NERC Member Representative Committee**
Progress Report and presentation on new CIP Version 3 Working Paper-Concept- Reliability Standards on Cyber Security for MRC input.

13. August 20–21, 2009 in Charlotte, NC

- SDT Plenary session to review and respond to MRC input on Working Paper/CIP-002 Concepts
- SDT Subgroup and plenary meetings to develop CIP-002 requirements and "proof of concept" control (s).

July–September — 45-day Industry Comment Period on CIP-002 Concept Working Paper
NERC Webinar
August–September Interim WebEx meeting(s)

- CIP-002 Subgroup meetings (as needed)
- CIP-002 Coordination Team meeting

14. September 9–10, 2009 in Folsom, CA

- SDT plenary session to review and respond to any additional industry comments on Working Paper and CIP-002 Concepts
- SDT subgroup drafting meetings- consider industry comments, draft requirements and "proof of concept" control (s).
- SDT plenary session(s) Subgroup reports on requirements
- Review of CIP-002 Standards, Requirements, Measures, and Outline
- Address coordinating issues.
- Establish SDT meeting dates and proposed locations for January–December 2010

September–October Interim WebEx meeting(s)

- CIP-002 Subgroup meetings (as needed)
- CIP-002 Coordination Team meeting

15. October 20–22, 2009 in Kansas City, MI

- SDT Subgroup drafting meetings — day one
- SDT Plenary Session(s) — day two subgroup reports on CIP-002 requirements
- Review and refine initial draft of CIP-002 single text

October–November Interim WebEx meeting(s)

- CIP-002 Coordination Team meeting

16. November 17–19, 2009 in Orlando, FL

- SDT plenary session(s) — to review and refine CIP-002 standard, requirements, measures and controls.

November–December Interim WebEx meeting(s)

- Drafting teams as needed to finalize drafts
- CIP-002 Coordination Team meeting

17. December 15–16, 2009 in Little Rock AK

- SDT plenary session(s) to review, refine, and agree on and adopt CIP-002 standard, requirements, measures and controls.
- Agree on initial posting of draft CIP-002 for industry review and comment.

Refinement of CIP-002 and Development of Other CIP Standards
January–December 2010

(12 SDT monthly meetings and subgroup WebEx meetings as needed)

- SDT responds to industry comments on initial and subsequent postings of CIP-002, Version 3 (may be multiple comment periods, as required)
- Refine the CIP-002 through the comment period and submit new CIP-002 Version 3 Standard for Balloting along with the catalogue of controls (i.e. CIP-003-CIP-009 or its successor) OR
- Ballot CIP-002 while permitting industry to rely on CIP 003-CIP-009 until the full suite of controls (i.e. CIP-003-CIP-009 or its successor) is reviewed and presented for balloting.
- Submit the full suite of CIP Reliability Standards on Cyber Security for Industry Comment
- Refine and Submit the full suite of CIP standards for industry ballot
- NERC Board of Trustees adoption of the full suite of standards
- FERC approves and NERC Implements the full suite of CIP standards

Proposed 2010 Meeting Schedule

January 20–21 — Wednesday–Thursday, Atlanta GA	July 14–15, Wednesday–Thursday
February 18–19 —Thursday –Friday, Austin TX	August 11–12, Wednesday–Thursday
March 9–11 — Tuesday–Thursday, Phoenix, AZ	September 8–9, Wednesday–Thursday
April 14–15 — Wednesday–Thursday, Atlanta GA	Oct. 13–14, Wednesday–Thursday or Oct.12–14
May 12–13 — Wednesday–Thursday, Dallas TX	November 17–18, Wednesday–Thursday
June 9–10 — Wednesday–Thursday, Sacramento CA	December 15–16, Wednesday–Thursday

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Draft Meeting Executive Summary

Cyber Security Order 706 SDT — Project 2008-06

October 20, 2009 | 8 a.m.–5 p.m. CDT
October 21, 2009 | 8 a.m.–5 p.m. CDT
October 22, 2009 | 8 a.m.–3 p.m. CDT
Town Pavilion
1111 Main St.
Kansas City, MO 64105
http://www.nerc.com/filez/standards/Project_2008-06_Cyber_Security.html

Meeting Summary Contents

116-390 Village Blvd.
Princeton, NJ 08540
609.452.8060 | www.nerc.com

EXECUTIVE SUMMARY

Jeri Domingo-Brewer, Chair, welcomed everyone and Joe Bucciero conducted a roll call of members and participants in the room and on the conference call. The Chair reviewed the meeting objectives and Bob Jones, facilitator, reviewed the proposed meeting agenda. Mr. Bucciero reviewed the need to comply with NERC's Antitrust Guidelines and also reminded the group of the sensitive nature of the information under discussion. The SDT adopted the August 10–11 and September 9–10, 2009 meeting summaries without changes or objection.

On Thursday morning, Jeri Domingo Brewer, on behalf of the SDT, thanked Kevin Perry for his service and contributions in building consensus and helping the team decode the cyber security puzzle as Vice Chair and presented him with a small plaque as a token of the team's esteem and appreciation for Kevin's dedicated service.

Scott Mix provided the team with an update on the TFE posting noting that all the regions have portals for accepting filings. He then reviewed Version 2 VSLs and VRFs noting it looks like it will be approved, which will close that group's work. The CSO706 SDT will be responsible for the VSLs and VRFs for Version 4.

Scott Mix provided an overview of the FERC Order on CIP version 2 and the procedural steps. He agreed to create a checklist of the over 200 charges from FERC Order 706 to help the SDT keep track of the milestones.

Mr. Bucciero summarized the effort to bring the team together in the interim to develop a rapid response process. The members discussed both the substantive issues with the interpretation of the term "auditably compliant" and with the SDT process for reviewing and voting on the response to the FERC Order. It was agreed that in the future the expectations should be made clear as to what the team is being asked to do and the communication process should be improved.

Scott Mix reported on the Standards Committee meeting and decisions regarding the response to the FERC Order and the CIP Version 3 next steps. Later in the meeting the SDT agreed on the following Version 3 steps and schedule:

1. *Post for Industry Comment 10-13-09 to 11-12-09*
2. **November 13 Conference Call — Review of Industry Comments and Response**
3. **November 16 (5 p.m. through dinner) Meeting in Orlando — Response Document to Industry Comments**
4. **November 17 Meeting in Orlando — Complete and Adopt Industry Response Document**
5. *November 20 — Post Response Document and Start Initial Ballot*
6. **November 30 — Close Initial Ballot**
7. **December 1 Conference Call — Finalize Industry Consideration of Comments document**

8. *December 2–14 — Recirculation Ballot*
9. *December 16 — BOT Approval*
10. *December 29 — FERC Filing*

Scott Mix presented the "strawman" CIP-002-4 template format for the SDT's consideration. He noted that he incorporated the work done to-date by the subgroups into the document, and that the SDT and others should consider this very much a 'work in progress' subject to many changes between now and December 2009.

The subgroups provided progress reports to the SDT. John Varnell reported on the Reliability Functions Subgroup noting that they have not finished the definitions but hope to do so in the coming weeks. The members of this subgroup are also participating on three of the other subgroups.

Jackie Collett reported on the BES Subsystems/BES Cyber Systems Subgroup noting that they require more time to work and that in their last discussion the subgroup was stuck on "generation." She suggested that the SDT needs to think about all the components that are needed for each function. The subgroup was focused on multiple definitions of a BES Subsystem, and it has been using drawings to illustrate questions and guide discussion. Ownership of equipment has been another challenging question, along with who is responsible for paying to protect the equipment because it is critical. The subgroup hopes to resolve the first challenge during this meeting, but the second challenge may take more time.

John Lim reported on the BES Mapping Subgroup's progress noting that three subsystems were identified to map (generation, transmission, control center), but there was disagreement on this point. The subgroup spent time discussing scenarios related to high-medium-low impact levels and may need more than a high-medium-low in terms of effort and expense.

Phil Huff presented the report on the Cyber Analysis subgroup noting that they have all but eliminated the "target of protection" concept and centered discussion on BES cyber systems. The subgroup is exploring what potential functional impact the BES cyber system has on each of the associated BES operations and reliability functions. He noted that several definitions require additional work.

Keith Stouffer provided the report of the Definition and Selection of Controls Subgroup highlighting the control "template" format he has worked on with Scott Mix.

The SDT then had a full group discussion of the following topics:

- Number of impact categories and what that concept means — where to apply the reliability functions
- Linkage between functions and where BES mapping is headed

- High-medium-low definitions plus review of the two scenarios presented by Scott Rosenberger that focused on the amount of effort or number of controls required for each impact level
- Number of BES subsystems — how do you map the functions into physical assets you can assess and measure

The SDT discussion was wide ranging and touched on the following questions and topics, among others:

- As we develop formal requirements be careful not to simply create lists without a purpose — may be the first requirement is mapping of criteria and thresholds — allows for measurable standards for audit purposes
- Did we conclude how we would map cyber assets or categorize them into h-m-l based on functions? Level of combinations would be at the subsystem level — assign an impact level to the subsystem
- Trying to identify "juicy" targets — defining those is something we have to discuss and work out — do two mediums using the same asset raise it to a high or "juicy" level
- Any system supporting reliability should be part of the assessment process
- Expect the group to discuss and bring back a full set of requirements that take you from identifying cyber assets to full categorization
- What is "prescriptive" is in the eye of the holder — some need more detail to comply while others want more leeway to meet the standard
- Keep in mind how the entities would meet the requirement for an audit. May need to write the VSLs while writing the requirements

Following this discussion the SDT agreed to break into two "meta groups" that combined subgroups. One meta group combined the first three subgroups (reliability functions, BES subsystems/BES cyber systems, and BES mapping) and proceeded by moving through examples of generation and transmission, addressing the challenge of multiple owners, and working through the task of mapping functions. A second meta-group addressed the cyber analysis tasks focusing first on definitions, and then looking at reliability functions and impacts from the loss of integrity perspective, going back to the requirements language, and creating applicable guideline language.

The Chair presented and reviewed the schedule of activities for CIP version 4 and the FERC Order 706. The team discussed and tested a variety of options in terms of the pace of the schedule for producing the CIP Cyber Security standards and ultimately reached agreement on the following schedule:

CIP-002-4 Key Deliverables, Steps, Schedule (October-December 2009)

The SDT agreed that the CIP-002-4 deliverables for posting for industry comment in December 2009 include the following documents: CIP-002-4 requirements and measures; related VSLs and VRFs; guidance document attachment to CIP-002-4; "Proof of Concept" controls (2-3 examples) illustrating the High/Medium/Low concept and the conceptual approach to replacing CIP-003-009; comment form with questions; and cover letter. The steps included:

1. November 1: Jackie Collett, Phil Huff, John Lim and John Varnell, the chairs of the 4 CIP-002 subgroups will form the CIP-002 Strawman Drafting Group (SDG).
2. November 1: All CIP-002 "meta groups" and the first four subgroups will forward to the SDG their drafts for the standards text, including any guidance language and the subgroups and meta-groups will be dissolved.
3. Joe Doetzl will coordinate the work of the Cyber Security Controls Catalog Drafting Group (CSCC) consisting of: Jay Cribb, Jim Brenton, Keith Stouffer, Bill Winters, and Jon Stanford. They will produce at least two examples to illustrate high/medium/low impact concepts as defined in the draft requirements of CIP-002-4, as well as recommendations on whether the SDT should request guidance from the Standards Committee on referencing a catalogue of controls. These deliverables will be prepared for circulation to the SDT by Friday, November 13, 2009.
4. The SDG will prepare a strawman draft of the standard requirements and circulate it to the SDT by November 13, 2009 for their review.
5. The SDT will utilize the strawman draft to organize its November 16–19 meeting and reaffirm at the conclusion of the meeting if the SDT will continue to aim for the December 16th adoption of the initial CIP-002 draft requirements for posting for to the industry for comment.
6. The SDG and the CSCC will present their revised standards drafts during a SDT conference call the first week in December.
7. The SDT will refine and circulate a strawman draft following the December conference call but prior to the December 15–16 SDT meeting in Little Rock.
8. December 15–16, 2009, the SDT will refine, finalize, and adopt the initial draft CIP-002-4 standard text for posting to the industry for comment.

CIP Version 4 Key Deliverables, Steps, Schedule (January 2010-July 2011)

The SDT agreed that the CIP version 4 deliverables for initial posting in July 2010 include the following documents: initial draft of all the CIP Reliability Standards requirements and measures; VSLs and VRFs; guidance document attachment to the CIP version 4 standards; catalogue of security requirements; implementation plan; comment form with questions; and cover letter. The steps needed include the following with targeted completion dates:

1. January–June 2010: Develop 'catalogue of security requirements' as part of CIP Version 4

2. February–April 2010: Respond to industry comments on new CIP-002
3. July 2010: Initial draft of all CIP cyber security reliability standards prepared and ready for posting for industry comment as part of work plan, addressing all relevant Order 706 directives in a CIP Version 4
4. July 2011: Complete 3 Rounds of Drafts and Comments plus a final draft and implementation plan for balloting

On Thursday afternoon, the SDT identified and then discussed key open issues:

1. Better identification of reliability functions (BES cyber system identification based on reliability functions) — Meta Group 1 and 2
2. Better definition of terms used in BES mapping document: control centers/systems, generation systems, etc. — Meta Group 1
3. Cyber impact analysis alternative approaches and implications – avoid unintended consequences — Meta Group 2
4. Better sense of how all parts of the new standards fit together and how the entities will use it — reliability functions, where do they fit and how do you come up with cyber systems that apply — Meta Group 1 and 2

The Chair reviewed the next steps including the schedule for the version 3 response document and the CIP-002-4 effort. She thanked Joe Doetzl and Kansas City Power & Light for hosting the meeting and providing excellent catering and facilities.

The SDT adjourned at 2:45 p.m. on October 22, 2009.

MEETING SUMMARY

I. Introductions, Agenda, and SDT Work plan Review

Jeri Domingo-Brewer, Chair, welcomed everyone and Joe Bucciero conducted a roll call of members and participants in the room and on the conference call *(See appendix #2*). The Chair reviewed the meeting objectives and Bob Jones, facilitator, reviewed the proposed meeting agenda *(See appendix #1*).

Mr. Bucciero reviewed the need to comply with NERC's Antitrust Guidelines *(See Appendix #3).* He urged the team and other participants in the process to carefully review the guidelines as they would cover all participants and observers. He urged all to avoid behaviors or appearance that would be anti-competitive nature and also reminded the group of the sensitive nature of the information under discussion.

The SDT approved the September 9–10, 2009 meeting summary without changes or objections. On Thursday morning Jeri Domingo Brewer, on behalf of the SDT, thanked Kevin Perry for his service and contributions in building consensus and helping the team decode the cyber security puzzle as Vice Chair and presented him with a small plaque with the following inscription: "Breakfast at Epiphanies — Leadership in Cyber Consensus — Kevin Perry, Vice Chair, CSO706 SDT, October 2008-October 2009."

Scott Mix provided the team with an update on the TFE posting which generated the following comments:

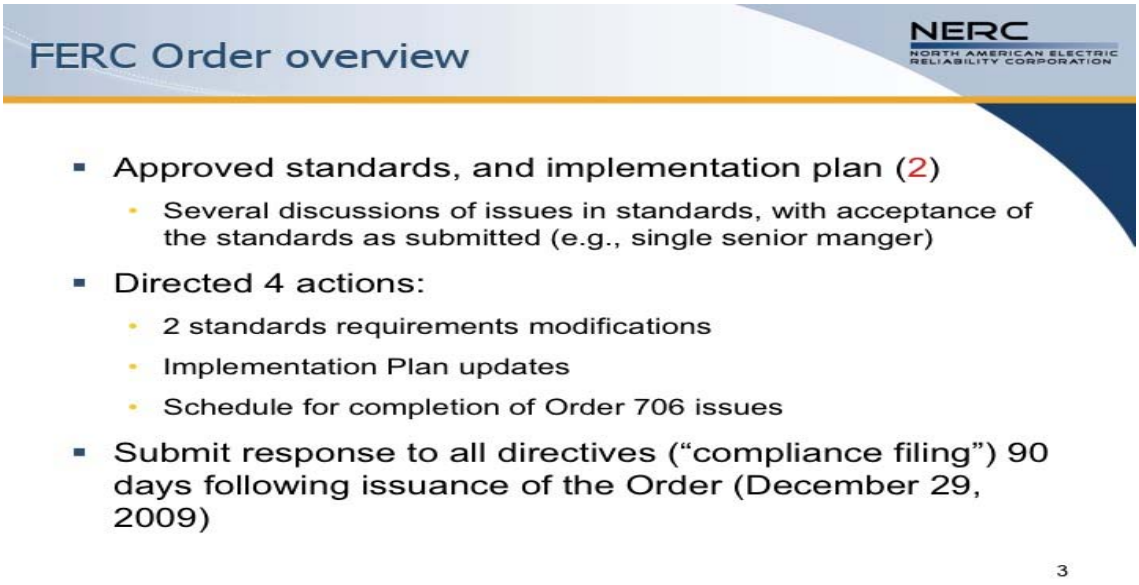
- Did FERC order say the TFEs did not need to be pre-approved? Yes, but they need to be pre-noticed.
- Will there be class based TFEs? Still debate about when it will appear and what it will mean — does not yet exist — still being discussed that may allow some form of pre-approval — question is what you will do to protect or mitigate and that cannot be pre-approved.
- All of the regions have portals for accepting filings.

In terms of the version 2 VSLs and VRFs Mr. Mix indicated that there will have to be a correction for a technical error but that it looks like it will be approved which will close that group's work. The SDT will be responsible for the VSLs and VRFs for version 4. The SDT VSL and VRF Chair will talk with the CSO706 SDT about their experience early next year to help us take on the task later in 2010.

II. FERC Order on CIP Version 2

A. Overview

Scott Mix provided an overview of the FERC order on CIP Version 2.



Member Comments on the Overview:

- When do we have to make the filing? (90 days — December 29th)
- Will they provide us with an attorney? Not clear
- Do we need to make the rule for Canada— not sure I can answer for Canada — NERC is required to file a response to the FERC directive by December 29th.

- Some of our work obviates some of the 200 but can we tell them we will not be done by December? The Order said "consider" not "adopt" the NIST standard — if adoption allows us to say we addressed the intent of the original order even if off in a different direction.
- Do we need legal assistance from NERC as part of this process to review? Do we need to integrate legal into the process? NERC is prohibited from developing the standard — does a legal representative blur that line?
- Mr. Huff addressed the time line not specifics of the order — a lot of details in how items are addressed over course of time – significant number of items to address – look at the 10,000 foot level first then zoom down as develop what the plan looks like.
- Concerned about legal input delaying the process – we debate the wording, legal would make that worse – Concerned with including legal in the standard development process — let NERC, FERC and industry legal review once the team has developed its response — let us develop the standards for protecting the system
- Maybe we need some substance expertise otherwise we may end up guessing in a limited time frame/
- In the past we had an electrical engineer/lawyer who helped with the wording — run the danger of letting them put in weasel words that dilute the product
- High level schedule discussed with NERC — (no, pulled from CIPC) — NERC is looking for this in formal form with more detail — (want to see a punch list for each item – this is an initial high level work plan — even this is very aggressive for developing consensus in the industry — need to discuss what is a realistic schedule because FERC will hold us to it)
- We need to do more to communicate to the industry on what we are thinking especially if we are accelerating our work — need to prepare the industry — make our meetings more efficient with substantive results — look into whether can we shorten the comment periods – communicate our direction early on
- For ballot period — ten days? How do we handle registration? (Not sure)
- Different team or us? (us – we will have to continue multi tasking)
- Looking for a spreadsheet punch list? We may not have an answer for every single one of the 200 items. What is required for the schedule response? What level of detail? What are the expectations?
- Mr. Huff offered a technical personal take — go through by subject area and group by subject — way to develop plan by subject areas with targets by areas — provides to industry and team the timeline for the plan)
- Some of our accounting may be that it no longer applies because of the approach taken — is that acceptable (it may be, given the approach you are taking)
- FERC Order punch list? Put on "parking lot". Is that useful for keeping track of progress. Scott Mix offered to try to produce.
- Useful if we send out to the SDT (we have two that Scott developed – one takes the order and extracts out issues on what did FERC decided with several colors – the pieces were then put into a spreadsheet to follow how and when each dealt with, also included a high-medium-low value to the industry – basis for earlier suggestion for how to schedule

approach to responding to the items – low hanging first, then the 15 or so highest most important then the bulk of the medium neither easy or complex items)

B. SDT Rapid Response Process — Special Meetings and Electronic Voting — Joe Bucciero

Mr. Bucciero summarized the effort to bring the Team together in the interim to develop a rapid response process. The members discussed both the substantive issues with the interpretation of the term "auditably compliant" and with the SDT process for reviewing and voting on the response to the FERC order. It was agreed that in the future the expectations should be made clear as to what the Team is being asked to do and the communication process should be improved.

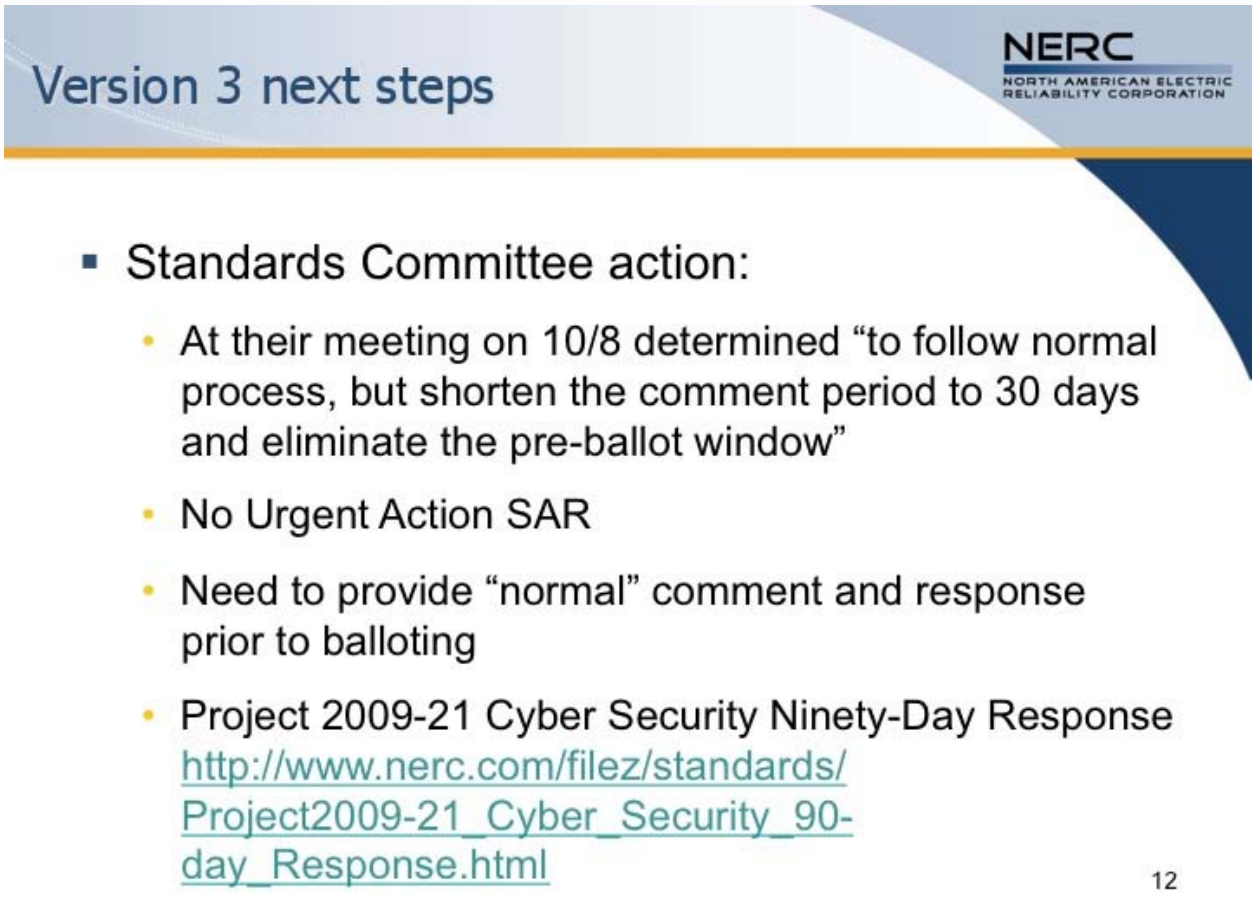
Workgroup Comments:

- We could/should have had a more transparent discussion than the last time – lesson learned, we need to communicate the discussion to the full group and the issues to be addressed
- We should have had a longer discussion to develop consensus before voting, especially the changes incorporated
- Many of the suggestions and additional change came after initial vote. Because of the rushed timeframe it was difficult to discuss those proposed changes and then revote.
- "Auditably compliant" has caused much confusion in the industry – many think it gives them an additional year contrary to what auditors think – compliant with full intent of the requirement and showing evidence of coming into compliance versus a year of data to show in full compliance – need to clarify the expectation going forward – this is important to Table 4 entities going forward and 2 and 3s carrying into a new year – to be fully compliant with intent you must conduct training – intent is that you do the action, not just periodically – collect logs for rolling last 90 days, maintain ongoing – if an incident (C date) then maintain for the past three years – you are compliant if you have the past 90 days – most disagreement centers around the periodic activity
- Did not get involved early enough – and then continued the discussion in the smaller group – question of what auditors are looking for – also difficult to get a full group together on such short notice, need sufficient lead time to include all – this was suppose to address the few issues FERC asked for - my concern was over the changes made after the team's discussion, changes the industry might not agree with – that is a compliance issue that may belong somewhere else – industry balloted and approved, thus looking at a few changes and now asked to look at significant changes without sufficient opportunity to discuss – I disagree on the compliance interpretation and we will not have consensus – My real concern was how the process was handled
- What are the concerns about the interpretation?
- I think you have the year to come into compliance – access log check prior to compliance date? Moving up compliance actions before the compliance date – many on the team and industry have this concern – also sending something out to industry that changes something they already approved.
- "Auditably compliant" means you have a full year of data to support –

- I concur that we were codifying at the last minute a new interpretation of "auditably compliant" – many entities have a different view – need to put the issue over in the compliance interpretation section – this was not the time to codify especially on such a short discussion time frame.
- Three years ago tried to educate on the three levels of compliance in a series of workshops across the country – there is confusion on this issue – this issue clouds moving forward rapidly as required – need to be pulled out and dealt with separately – we are now exposed to negative responses – agree with Kevin's interpretation and with Jackie's view that it should have been dealt with differently and separately.
- Disagree with Kevin's interpretation – requiring logs before the compliance date does not make sense.
- Our discussion should center around Table 2 compliance for new asset implementation
- There is no definition of "annual" from NERC
- The process and discussion could have and should have been handled better
- We can pull out the section from the ballot and NERC can put it out separately for comment since it is not under an urgent action order
- Compliance dates are based on when you wrote the procedures and when you started it
- Process lessons that we can apply going forward?
- Time to absorb and discuss, transparency of issues
- Decision on holding meeting on short notice was not taken lightly, but had no choice, only way to involve available members – it needed more time
- Even the limited opportunity for discussion improved the initial draft

C. Process and Schedule Going Forward

Scott Mix reported on the Standards Committee meeting and decisions regarding the response to the FERC Order and the CIP Version 3 next steps:



Later in the meeting the SDT agreed on the following Version 3 steps and schedule:

Version 3 Key Steps and Schedule

1. *Post for Industry Comment 10-13-09 to 11-12-09*
2. **November 13 Conference Call — Review of Industry Comments and Response**
3. **November 16 (5 p.m. through dinner) Meeting in Orlando — Response Document to Industry Comments**
4. **November 17 Meeting in Orlando — Complete and Adopt Industry Response Document**
5. *November 20 — Post Response Document and Start Initial Ballot*
6. **November 30 — Close Initial Ballot**
7. **December 1 Conference Call — Finalize Industry Consideration of Comments document**
8. *December 2–14 — Recirculation Ballot*
9. *December 16 — BOT Approval*
10. *December 29 — FERC Filing*

III. CIP 002 Strawman

A. Overview of CIP 002 Strawman Template

Scott Mix presented the "strawman" CIP-002 template format for the SDT's consideration. He noted that he incorporated the work to date of the subgroups into it and that the SDT and others should consider this very much a work in progress subject to many changes between now and December, 2009 (See Appendix # 5)

Member Comments

- Regional entity is a statutory requirement
- RRO does not exist anymore
- Because it was confused with RRE – that needs to be fixed
- New entity – RRA – we could break new ground and include
- In the narrative spell out interconnection variances – are they regional or should they be up in the standards (there is a number for the east, the west, etc., it is in the language of the requirement)
- For the interconnection is there a designation for the authority separate from the region? (East is a split authority)
- Good value added with the template

B. Subgroup Reports to the SDT

1. Reliability Functions Subgroup Report and Key Issues and Draft CIP 002 Language

John Varnell reported for the subgroup noted they have not finished the definitions but that should not hold the rest of the team up in moving forward. They have shared their initial work with other teams and the members are participating on the other 3 teams.

Member Comments

- Time frame for finishing the definitions? A couple of weeks
- Will this be published with the standards?
- Definitions do not affect what is being done on the other teams but how people will interpret so may be part of the filing, maybe as a FAQ or guidance document.
- This is an area where group may blaze new ground – may want to make part of standard to give it more weight than just a FAQ – consider a guidance document.
- Reliability functions – make those the basis for guidance to the functions

2. List of BES Subsystems/BES Cyber systems Subgroup Report Key Issues and Draft CIP 002 Language

Jackie Collett reported on the group's progress noted they require more time to work and that in their last discussion the subgroup got stuck on "generation" – we need to think about all the components that are needed for each function. Next conversation focused on multiple definitions of what a BES system is and they have been using drawings to

illustrate questions and guide discussion. Ownership of equipment has been another challenging question and who is responsible for and paying to cover them because they are critical. The subgroup hopes to resolve the first element while here but the second element may take more time

SDT Member Comments

- Group 1 and 2 need some in depth discussion together. They will meet together this afternoon.

3. BES Mapping Subgroup Report and Key Issues and Draft CIP 002 Language,

John Lim noted there were three subsystems to map and there was disagreement on this point. The subgroup spent time discussing scenarios related to high-medium-low impact levels – may need more than a high-medium-low in terms of effort/expense.

Member Comments

- We need to communicate together as a single group this afternoon rather than as subgroups- need to be sure we are on the same page rather than four or five groups doing distinct things
- May be premature to consider until we finish the sub team reports – will revisit after lunch and the rest of the reports

4. Cyber Analysis Subgroup Report, and Key Issues and Draft CIP 002 Language

Phil Huff presented the report on the Cyber Analysis subgroup noting that they have all but eliminated targeted protection – and centered discussion on BES cyber systems – reliability function assessment assesses the potential function impact the BES cyber system has on each of the associated BES operations. He noted that several definitions require additional work and more eyes (review) from others – protection of the system relies on the definitions and reliability functions. He also noted that they need more time as a sub group on definitions and for input form other groups too

5. Definition and Selection of Controls Subgroup Report, Key Issues and Draft CIP 002 Language

Keith Stouffer provided the report of the subgroup, noting the control "template" he has worked with Scott Mix on in terms of an acceptable format.

Member Comments

- How do we break this into l-m-h and for different systems? –generation, control and transmission?
- Estimated time needed? Maybe four or five years or within the time we have available.
- We will need more time to build common consensus in the group as a whole.
- Also need to run this format by the NERC staff
- This is just one requirement as an example – we will divide the group up to deal with the rest of the requirements.

- Need to be sure we are not continuing on the path where we are split up just to support and continue the process – we need to get back together as a whole to deal with key issues sooner rather than later
- This can be posted as an example of applicability – we will need to do a good job of communicating to the industry that this is an example and not asking for their comments in detail

C. Key Issues Going Forward.

The Chair and Vice Chairs tested whether to break into small groups or stay together to identify and document the several key outstanding issues to be addressed. The group suggested a full group discussion of the following topics:

- Number of impact categories and what that means – where to apply the reliability functions
- Linkage between functions and where BES mapping is headed
- High-medium-low definitions (first)
- Number of BES subsystems – how do you map the functions into physical assets you can assess and measure

1. High-medium-low definitions

Member Comments

- Do members have a notion how big each category is? – does low represent 50% of the assets? More or less than that? Is high equal 5 or 10 % of the assets? That may drive some of the criteria thresholds.
- Will have to meet the low standard for everything – the medium and high will require more.
- Do we need a category below low, such as none?
- No need for something below low – prefer scenario 1 with some adjustment of the percentages.

Conceptual discussions related to High, Med, Low Impact Levels (Scott Rosenberger)
There were many comments related to the adequacy of 3 levels of impact presented in our concept paper. Some of the need to suggest the possibility for the need for additional levels of impact stems, in my opinion, from the lack of clarity as to what the amount of effort or relative number of controls are associated with each level.

Scenario 1

Impact Level	Low	Med	High
Amount of effort/Number of controls (compared to High)	60%	80%	100%

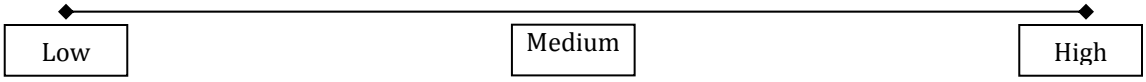
In this scenario, it is arguable that a Lower than Low is necessary as Low requires significant effort to accomplish (Low is not Low Effort). In this scenario, Lower than Low then turns into

0% (or no impact, no controls) and this scenario looks conceptually like the all or nothing environment that we are in today.

Scenario 2

Impact Level	Low	Med	High
Amount of effort/number of controls (compared to High)	10%	50%	100%

In this scenario, there is a significant difference in the effort/expense required for the three impact levels. A case could be made that most if not everything would at least fit into the low category. With the major focus being re-directed to the identification of Medium and High impact areas.



A significant benefit of Scenario 2 is that more Security work would be done on more assets and there would be few (if any) that have nothing done and would make the effort/expense required (Low) commensurate with the risk (Low). The industry could then focus on protecting those BES Subsystems that have a more significant impact to the BES

- Scenario 2 concerns me – the compliance load on the entities – requires documentation on every element of the system – 75% in the low would still require 90% of the compliance effort – prefer recognizing some will need little or no effort for compliance
- Need to determine how much is in each category – need something less arbitrary – how much is in each bucket?
- John Lim's group on the BES mapping only came up with the high and medium, everything else was put in low – the point here is determining what is low
- Scenario 1 allows for none
- Can reliability requirements deal with issues in generation
- Feedback form concept paper asked why we were going to this categorization of h-m-l – the high and medium were easy, low was everything else – low should be a low amount of work even if the largest category
- The concept reflects a cost perspective? Will groups simply assume everything should get a high level of protection to avoid liabilities?
- How big is the compliance requirement for those in the low category? Are there parts of the system that require little or no protection and thus lower than low?
- Every entity still has assets that have nothing to do with BES but will need to categorize them for auditors – they may have their own protection systems – you have assets that do not need cyber protection
- Careful that even the most remote part of the system if connected leaves the system vulnerable

- Prefer numbering rather than h=m=l which would require putting something in the buckets – industry might be more open to level 1, 2, or 3 of impact – there are assets out there that do not need anything because they do not have an attack vector
- Focused on BES elements or cyber assets? Does it matter? It does in my world
- NERC has statutory authority only over bulk electric system assets – not distribution or marketing systems
- But how do I group the assets and their functions in a control center?
- In the federal system, every single system has to have minimum level of security
- Few assists in the high, some in medium with the bulk in the low categories of impact – don't need many controls to protect the low, concern should be for protecting the high and then the medium – the three levels help direct the limited resources to ensure the most bang for the buck
- Functions define what you look at first for coverage – this is a penalty standard, a list of what you will be penalized for
- Yes, focus on the areas of the most risk – prefer scenario 2 because it allows focus on the highest risk and not on the lowest
- We are trying to minimize the risk to our company – we need to keep the focus on the security of the system in the most cost effective way possible – need to work on security, rather than on compliance
- Are we protecting all BES systems?
- Different systems balance the functions – how important is a subsystem to a function?

2. BES Subsystems

- Use an example of generation subsystem – for purposes of discussion – individual units may not be high – but may be as part of the larger system – look at it from a reliability requirement from different perspectives.
- How would requirement do that? How many steps would it take to cover all of the possible scenarios or related systems?
- You have to have the flexibility to address different subsystem configurations. The configurations could be in the hundreds
- Take them all in common, not necessary to figure out all the possible configurations – because you have the flexibility, the more reason to consider them collectively
- We have to determine the common elements. Need to work from the big down, not from the subsystem up – should not have to work through all the possibilities – the intent should not be to determine what is a requirement and how to avoid it but how to protect the highest priorities.
- Focus on the facility – don't have to focus on the whole facility just because it has one black start.
- Concerned about this slicing and dicing approach – what is the total generation from the facility and the functions – I don't see value in grouping elements.
- It is a requirement to look at it in multiple ways – analyze as a unit and a facility?
- Need definitions to be flexible.

- It is not flexible but rather prescriptive
- Industry needs an analytical approach with criteria for impact levels
- Need to focus on the facility as a whole and the subparts only as needed – suggest moving discussion toward functions
- Reading too much into the diagram

3. Reliability Functions:

- Need to look at how the functions impact the other groups.
- Look at where to apply the reliability functions as a basis for cyber security impact identification.
- Use as a basis for defining or identifying BES subsystems; the components that need to be defined -
- The performance of these functions is what has impact – have to protect the function rather than the asset.
- Define subsystems based on the reliability function they perform or support.
- We protect assets because they perform reliability functions – we protect transmission because it moves power from generation to consumption – which ones and how much depends on importance to the reliability of the system. That's why we split this up by function.
- I like the approach that looks at what we think the answer should be – start with the end in mind.
- If we start with the BES subsystems, we are starting in the middle – we need to start at the top, most important and work down.
- The control center is the physical building. Not everything in that center is essential to the function you are trying to protect.
- The control center is not a subsystem - we need to be careful how we use the words.
- Control center as a building is less important – talking about two different things – cannot possibly define everything into three subsystems.

4. General Discussion of CIP 002 Issues and Strategy Going Forward

- Need to determine what we need from groups to go into the requirements – first get list of BES systems, take that list and define its impact – what are we looking for? A requirement that says entity list their BES systems or say what kind of subsystems they are – guideline for determining function of the subsystem?
- Apparent yesterday we are not coordinating on BES subsystem versus subsystem – function or component to complete the task – each entity creates list of subsystems of items needed to perform a function or task.
- In categories we have special category for special subsystems – include subsystems that are not related to specific pieces of hardware but perform a BES function

- As we develop formal requirements be careful not to simply create lists without a purpose – may be the first requirement is mapping of criteria and thresholds – allows for measurable standards for audit purposes –
- Cyber Analysis subgroup might begin developing language this afternoon for full group to look at.
- Did we conclude how we would map cyber assets or categorize into h-m-l based on functions?
- Level of combinations would be at subsystem level – assign an impact level to the subsystem
- Trying to identify "juicy" targets – defining those is something we have to discuss and work out – do two mediums using the same asset raise it to a high or "juicy" level
- Still thinking electric grid not security – can kill a "juicy" target from a non-juicy source – control system is an overlay from a different plane than reliability of the electric grid
- Any system supporting reliability should be part of the assessment process.
- John Lim noted that what we have needs to be vetted by the full group – be sure we are on the right track – but how do we apply, either as a standard or second document – do we need a list for requirements guys or is the functions the categorization the list
- Three groups need to get together to determine what is in the standard – what are we asking the entities to do?
- Still confusion on what each needs to bring back for the standard and the support document
- Do the groups need additional input from the whole team as to what is expected?
- Expect our group to discuss and bring back a full set of requirements that take you from identifying cyber assets to full categorization
- Rich reviewed a rewrite of the language for the functions list and the impact value
- As we break to write requirements – keep in mind, 65% of requirements were prescriptive or administrative – stick to what's not the how's
- What is "prescriptive" is in the eye of the holder – some need more detail to comply will others want more leeway to meet the standard
- Keep in mind how your entity would meet the requirement for an audit
- May need to write the VSLs while writing the requirements

D. "Meta Groups" Meetings and Reports

Following this discussion the SDT agreed to break into two "meta groups" that combined subgroups.

1. Meta-Group #1 (Subgroups 1, 2, and 3 jointly met)

Scott Rosenberger suggested taking one of the functions and run through an example of how it would be implemented in the BES Mapping and BES Subsystem subgroups. Below are comments both in plenary and the meta subgroup:

- **Working through Examples.** Spent time identifying which reliability functions went with which mapping criteria – need more time to work through examples. Thought I would take

generator than met one of four then look at cyber functions identified for protection. Too many "can't be done" answers at the end – not sure what are the next steps/

- I learned the value of an example – thought we had agreement but then differences arose when we tried out an example.
- A few things came out – we made certain assumptions, taking into account the functions in looking at mapping criteria – We brought Phil in for some clarifications, found he was working based on clarifications of functions – pointed out the need to reconnect the criteria to the functions to begin bridging efforts – good start toward bridging in the future –
- Also, if you have a high on two different criteria, what happens then?
- We tend to bog down in the weeds – this prevents us from trying some things – eventually we may need to press through and ask for industry comments to help identify where clarifications are needed.
- Do we need a broad general definition?
- **Multiple Owners.**
- Different owners in the same subsystem – how do we tie them together?
- Multiple owners of subsystem is still concern.
- Some of the categories in the mapping we have to be able to say what is the generation subsystem – focus on what makes sense for generation subsystem rather than the ownership

- Concerned about using terms "transmission" or "control center" – change latter to control and operate function?
- **Generation**
- Look first at generation and transmission – have some drawings we can talk from – what is a generation subsystem? How does it relate to the BES function and or mapping?
- Those are filters to determine its impact on the system – if it is taken away what is the impact on the function
- Some of that is built into the criteria – some of the criteria addresses some of the functions
- Your list has seven functions related to the generator
- Those operating the transmission system don't care about most of these functions.
- How does BES cyber system affect the reliability function? The matrix tells you how the reliability function impacts.
- High impact generator – do any cyber systems affect that generator? It is on my BES mapping and is "high" – how do I determine what to protect?
- Impact based on security criteria not on impact on the BES
- **Functions and Mapping**
- Do we need to describe what the BES subsystem looks like for each of these functions?
- Same components for each of these functions? Many may be the same.
- The way you use the function is based on the criteria used to determine impact.
- Are we going to have a generation mapping and one based on reliability? Reliability overshadows all of the mapping pieces.
- Does mapping we already do that?

- There is not a direct mapping between reliability functions and subsystems. Instead functions are the underlying information for the impact criteria.
- This is an exercise to be sure reliability is mapped and accounted for
- Phil's group should come up with criteria related to reliability of cyber system
- He is looking at which application, not the same as BES big iron things
- Functions are used to define impacts – three definitions
- Subsystems are building blocks for criteria
- Phil Huff suggested that you assess cyber systems based on reliability functions – combine impact criteria.
- How does cyber system impact or perform reliability function? Can I do the function without that system?
- Come up with matrix to be sure the correct relative rating and appropriate controls
- Incredible amount of minutia to document and lots of "phrasing" of the considerations.
- Are we making this overly complicated? Today, we determine if you have a critical asset then look for all the systems that impact that asset, analyze it for all the criteria, look at the critical aspects for protection/
- Trying to write the CIP standard(s) less prescriptively
- A BES subsystem is not just big iron.
- Phil's group is going through the cyber system side and others are trying to go through the BES subsystem mapping – later work together to reconcile the two sides.
- If not defined by NERC reliability standard as criteria.
- Can have a "high" on the mapping side but a medium on the cyber side. The "High" water mark makes it high for both.
- Have to list the cyber systems that support the BES system function.
- Use the blue side (cyber asset) for those without the bulk electric generation assets.
- Generation, transmission, control and special systems – four areas for definition.
- Next: review functions first, then look for how mapping ties to functions
- In terms of function – what's missing?
- Talking about an automated real time response – "dynamic" response
- We walked through this as a group and added which function applied to BES mapping criteria

2. Meta Group #2 – Cyber Analysis and Controls Subgroup

Phil Huff noted they would be working on definitions and looking at reliability functions and look at impacts from loss of integrity. The may need to go back to the requirements language – and create guideline language – Are the standards ready to be combined by the end of this meeting? Concern with the BES mapping and what is in the standard or not.

Comments

- How should the list of functions from Varnell's group be handled and how they relate to the BES subsystems? Went back and looked at definitions of what is a cyber system and what is BES system. Then looked at the cyber analysis piece

- No true consensus yet on approach
- Map out the BES systems before doing a cyber analysis.
- Phil reviewed language changes in the draft document.
- Challenge to marrying things together in the lookup table
- Requirement 5B an alternative solution – using the BES mapping table – we need feedback from the full group – how do we get to the final picture? Is this an easier way to go?
  - Walk us through 5A?
  - Identify BEX subsystems through which the cyber system supports or has potential to impact reliability functions
  - Then assess the potential function impact the cyber system has on each of the BES subsystems – under Reliability function assessment
  - BES system mapping just associates or relates the cyber systems to the BES system
  - Does the scale of the generator play into the analysis?
  - No
  - Then you are double loading the cyber analysis process – the cyber impact is the same for big or small generator, but the BES analysis is different for each – will end up doubling the work
  - When you look at cyber system it is done once for the BES system
  - As an auditor I may expect to see what is the impact of each cyber system on any associated BES systems
  - Have not considered different BES cyber system categories
  - But the auditor is going to ask for a unique identifier for each cyber asset
  - Map device to specific BES subsystem and look up the impact – puts it into a sequential process rather than two parallel process that meet at the end
  - Should be able to take advantage of commonality of systems to do one analysis for economy of scale
  - The pieces may not be high but the system as a whole is high
  - How do you handle systems that talk IP up one system but not others?
  - That is a separate issue – just because data is exchanged or talking by IP does not mean it is attackable
  - BES mapping – 5B means is there anyway to make the cyber system cause high impact (3.1.1-4) then it is high – puts a big onus on defining your subsystems.
  - We should only care about systems that affect the BES not minor subsystems – suggest you check BES system first before checking the cyber system.
  - The only difference is that the medium and low are taken out of the analysis.
  - Look at BES systems first – they are going to look at the generator first, the control system, because they have the tools to do that.
  - Tighten up what we mean by a system – no single relay works by itself – do we need to qualify a system by the fact it communicates.
  - You may have to both – look at it from both perspectives – neither the green or blue side is correct alone – don't spend our time deciding which is right but work through examples.
  - Difficult to come up with something demonstrable and repeatable for an auditor – trying to do analysis once, not repeat it for both sides.

- If do BES system you knock out most and only do analysis of cyber systems related to those identified the BES system side.
- Doing separate analysis then trying to bring together is unnecessarily complicated
- As a company that cannot control the other end then I need to protect myself and my partners
- We have to look for the solution that covers the lowest common denominator
- Our group concluded that whatever h-m-l rating comes out we will apply – concerned about integrated systems that may be vulnerable to entry from the low side
- The highs are easy to identify but more difficult to identify lows that may allow access to the high or critical systems – but I can only control my equipment, I have to limit the attack vector by how I set up my "high" equipment
- The focus needs to be on what affects the BES
- Even the low may need some substantial protection if it talks up line
- The 5B approach captures the current gap which is aggregated BES subsystems where they were identified as low – still needs protection
- Look at potential span of control – what is the scope or range of control – iterative analysis or process–
- How do you write a requirement that allows for a high to change to medium where appropriate? If possible that would address much of my angst
- Getting into the weeds again – in terms of definition of boundaries

IV. CIP Review Milestones and Schedule

A. CIP Version 3 Key Steps and Schedule

The Chair presented and reviewed with the SDT the schedule for Version 3 and the FERC order discussed and agreed to on the first day (Tuesday):

1. Post for Industry Comment 10-13-09 to 11-12-09
2. **November 13 Conference Call — Review of Industry Comments and Response**
3. **November 16 (5 p.m. through dinner) Meeting in Orlando — Response Document to Industry Comments**
4. **November 17 Meeting in Orlando — Complete and Adopt Industry Response Document**
5. November 20 — Post Response Document and Start Initial Ballot
6. **November 30 — Close Initial Ballot**
7. **December 1 Conference Call — Finalize Industry Consideration of Comments document**
8. December 2–14 — Recirculation Ballot
9. December 16 — BOT Approval
10. December 29 — FERC Filing

B. CIP Version 4 Key Steps and Schedule

The team discussed and tested a variety of options in terms of the pace of the schedule for producing the final CIP 002-009 and ultimately reached agreement on the following schedule:

1. CIP 002-4 KEY STEPS/SCHEDULE (OCTOBER-DECEMBER, 2009)

The SDT agreed that the CIP-002-4 deliverables for posting to the industry for comment in December 2009 include the following documents: CIP-002-4 requirements and measures; related VSLs and VRFs; Guidance document attachment to CIP-002-4; "Proof of Concept" controls (2-3 examples) illustrating the High/Medium/Low concept and the conceptual approach to replacing CIP 003-009; Industry Comment Form with questions; and Cover letter. The steps included:

1. **November 1:** Jackie Collett, Phil Huff, John Lim and John Varnell, the chairs of the 4 CIP-002 Subgroups will form the CIP-002 Strawman Drafting Group (SDG).
2. **November 1:** All CIP-002 "meta groups" and the first four subgroups will forward to the SDG their drafts for the standards text, including any guidance language and the subgroups and meta-groups will be dissolved.
3. Joe Doetzl will coordinate the work of the Cyber Security Controls Catalog Drafting Group (CSCC) consisting of: Jay Cribb, Jim Brenton, Keith Stouffer, Bill Winters, and Jon Stanford. They will produce at least two examples to illustrate high/medium/low impact concepts as defined in the draft requirements of CIP-002-4, as well as recommendations on whether the SDT should request guidance from the Standards Committee on referencing a catalogue of controls. These deliverables will be prepared for circulation to the SDT **by Friday, November 13, 2009**.
4. The SDG will prepare a strawman draft of the standard requirements and circulate it to the SDT by **November 13, 2009** for their review.
5. The SDT will utilize the strawman draft to organize its **November 16-19 meeting** and reaffirm at the conclusion of the meeting if the SDT will continue to aim for the December 16th adoption of the initial CIP-002 draft requirements for posting for to the industry for comment.
6. The SDG and the CSCC will present their revised standards drafts during a SDT conference call the first week in December.
7. The SDT will refine and circulate a strawman draft following the December conference call but prior to the December 15-16 CSO706 SDT meeting in Little Rock.
8. **December 15-16**, **2009**, the SDT will refine, finalize, and adopt the initial draft CIP-002-4 standard text for posting to the industry for comment.

2. CIP VERSION 4 KEY STEPS/SCHEDULE (JANUARY, 2010-JULY 2011)

The SDT agreed that the CIP Version 4 deliverables for initial posting in July 2010 include the following documents: initial draft of all the CIP cyber security reliability standards requirements and measures; VSLs and VRFs; Guidance document attachment to the CIP Version 4 standards; catalogue of security requirements; Implementation Plan; Industry Comment Form with questions; and Cover letter. The steps needed include the following with targeted completion dates:

1. **January - June 2010**: Develop 'catalogue of security requirements' as part of CIP Version 4
2. **February- April 2010**: Respond to industry comments on new CIP-002
3. **July 2010**: Initial draft of all CIP cyber security reliability standards prepared and ready

for posting for industry comment as part of workplan, addressing all relevant Order 706 directives in a CIP Version 4.

4. **July 2011**: Complete 3 Rounds of Drafts and Comments plus a final draft and implementation plan for balloting.

Member Comments on the Schedule

- Unless team changes the current schedule, CIP Version 4 will have to be completed in 13 ½ months.
- Complete generation of catalogue controls is a huge task. Even reaching agreement among the SDT, we won't get industry to agree by balloting. Current draft schedule only has 2 rounds of comments built in to it. With 45 days for each.
- For Version 1- the SDT had conference calls every day for months. What is a reasonable number of rounds of member comments?
- Process vs. calendar base. Set a calendar and modify process? Can't do both.
- Need to say more than just four rounds without giving some times certain.
- We need to guard against rushing it out and not having a good product – schedule should be industry approval plus one or two months – if that is not good enough, let them give us a deadline – As much as I would like to, I am not optimistic we can get in done by Dec. 2010 – we cannot control industry comments and the number of ballots needed for approval.
- Here is what we think it would take to address issues – if industry says more work is needed then schedule could go out additional months.
- The critical date is draft one – does our current process allows us to get it out by Dec 2010?
- We have a defined process for Dec 2010 and the final approval but the middle is squishy
- Assume two cycle schedule and industry may require more – we can agree how long a cycle will take but not how many cycles will be necessary – two cycles is a good WAG
- Two cycles is optimistic given the changes we are suggesting to the regulatory environment – past efforts needed four cycles without the regulatory element – here we need four cycle minimum.
- Clarify ballot versus comment cycles – we are talking about post/comment cycles before sending to ballot.
- FERC says okay to our suggestion but do they leave a disclaimer to modify their order if needed?
- I would like to think we could file an amendment to add cycles based on industry comments as documentation.
- Concerned we will file a schedule with best estimate and it will not be politically acceptable – FERC will say accept but shorten time period.
- There is a perception or concern we are already late – the industry is just frittering away time – also depends on quality of comments – go as far as we think we can get away with, that may be first quarter of 2011 – what can we get without tipping it over – intuition says three cycles and first quarter 2011
- Others have taken five revisions over five years – precedent with standards that are not as complicated.

- Markey has hearings next Tuesday and plan to talk about how fast we are moving – high visibility issue.
- We are responsible for producing under the issues – function in the environment we are in –
- Do not believe Dec 2010 is achievable, question if Dec 2011 is achievable – have we addressed requirements put forth by the FERC? Do we quickly address the order, throw it over as version 4, then take time to address broken standards – this might get FERC off our back, may defer Congressional action too.
- Willing to think FERC is thinking about how we address the 706 requests – political reality will say get it done.
- Anything interim may help with FERC but not the politics – anything that hints at a redo or makeup will not sit well.
- The cantankerous Canadian view – impression from up north, we are doing a lot of second guessing – do what we think we need to do, a realistic schedule – band-aids will not serve the industry well – band-aids will not work with the industry, they want a fix – our role is to support the reliability of the BES
- Concern is founded in CIP8 where we thought we were doing what they asked and they did not approve – can we address all the issues within the proposed timeline? Would like to think all the issues will be addressed in the complete rewrite – how much are we going to have to do to address confusion in the industry? Does paragraph 25 require three levels of control? Applicable features of the NIST framework? We have to do our best to find door out of the dark hallway – this is the only process we have to get it done as quickly as possible – these standards were never designed for "smart grid" – not our job to address it now – focus on "addressing" the NIST framework.
- Focus on what is it we have control over? Some issues FERC will come back and clarify for us – cannot focus on what we think they want – do the best we can to give an estimate what we need to get the job done, caveat with maybe issues out of comments that may need more time – best estimate given what we know now.
- Number of issues up for interpretation – more issues are clear, don't need clarification and must be addressed even if concern is no longer applicable because of other changes suggested – have a good answer for each item
- Sent out matrix Scott and the Chair worked on with magnitude column – VH are the very high that may not fit in Version 4 – items that may require a V5.
- Now for the wake up call – testimony for Congress next week – NERC general counsel saying we will be done middle of next year, not even Dec. 2010
- We have the attention of the industry – shorten review cycles to 30 days – helps buy some time?
- All choices assume draft by April? Just a matter of how many cycles? Still need to discuss getting draft by April 2010
- Assume draft ready by April 2010? If so, then choice is between how many cycles
- Suggest when we think full package ready for post – beyond that why vote on how many cycles it will take?
- Because FERC asked – and NERC wants/needs to know what the estimate is.
- Nailed down realistic time frame for complete package for posting rather than ballot – currently April 2010.

- Optional dates for posting draft
- Realistically we will need time to respond to CIP 002 comments – amount of work putting together catalogue represents a shift in the industry paradigm.
- However we have resources and we are not reinventing the wheel.
- Did not consider the cycle of comments when I suggested July
- Should we put in cycles?
- This is a draft of the whole CIP 002-009?

Straw Poll- Date for First Full Draft of CIP 002-009

Date	April	July	October	January 2011
Member Votes	3 votes	10 votes	3 votes	3 votes

Member Discussion of Straw Poll
Comments of those favoring April 2010

- I was trying to keep us on schedule for NERC and Congress
- Feel the controls catalogue piece will go faster than you think
- Need to draw line in sand to shoot for

Comments of those favoring July 2010

- The line in the sand is when we will be done with CIP002 – how soon will we get there?
- JB: more realistic – April is not realistic given the way we have been working - do think catalogue will go quickly but still need enough time to reshape the wheel

Comments of those favoring October 2010 and January 2011

- SDT will need time to rewrite controls carefully and will need time to respond to industry comments
- We can make April 2010 if we restructure the SDT effort – want to discuss restructure to make that date – only voted October as realistic for how we operate now
- Does this proposed schedule include what Scott Mix calls the very high “uglies”?
- Some of those “ugly” issues are not addressed by this group.
- If the issues are in the 706 order to be considered and relate to CIP – can’t ignore it.
- Directives in 706 presupposed no radical changes to standards – as we radically change standards then many of FERC concerns may no longer be applicable – the current standards are fatally flawed and need more than band-aids – but a new set thrown over the wall, FERC may say did not respond to directives.
- Need to make sure that if there are FERC 706 issues not even addressed by the new approach, we know that sooner than later.
- Need to address serious issues that are not covered – also, we can claim meet 18 months if draft ready by July 2010 – look at two tracks: 1) control or data center and 2) field sites – more pain in the latter, but may address some of this with a separate additional effort looking at physical security.

C. SDT Structure and Deliverables Challenges

The SDT CIP-002-4 deliverables for posting in December include:

- CIP 002 requirements and measures,
- VSLs and VFRs
- Guidance document attachment – CIP-002-4
- "Proof of Concept" controls (2-3) illustrating the High/Medium/Low concept and the conceptual approach to CIP 003-009.
- Industry Comment Form with questions
- Cover letter

The SDT considered the following proposal:

By November 1 the current 5 subgroups will produce final thoughts for the new drafting teams, and then dissolve. A lead drafting team would be formed from current chairs. A catalogue of controls group would work on the 2-3 controls. In January, 2010 may need to re-divide to conquer on parallel paths: 1) Need more eyes on the controls for development of the controls language volunteers: Joe Doetzel, Jay Crib, Bill Winters(re-volunteering), Jim Brenton

Member Comments on the Proposal:

- Instead of four groups continue with the two groups formed yesterday to conclude by November 1?
- Concerned with what Keith Stouffer is doing – like to revisit – need to rationalize the 15 issues across the standards
- Still talking about creating an example of CIP5 – access control
- Looking at it from a functional model using other standards as potential entry points – and working with Scott on an acceptable format.
- One structure doesn't fit all – cannot design this with one entity in mind.
- January meeting will feature another discussion on basic points of all the controls? – Dec 2009 is just coming up with examples – Keith is still in the NERC standards format
- Maybe everything can be considered low.
- If just "low" then significantly broadening what security is applied to – Keith is shoehorning the standards into an example control – may need to look at how the federal government works under NIST with FSMA – you get a system of controls that are auditable
- The subgroup is tailoring statements to the current standards in response to NERC requirements for phrasing – yes, spending a lot of time trying to shoe horn it together – if that is not the way to go then let us know before we have created the wrong example.
- My understanding based on discussions with NERC staff –is that unless that statement that auditor is looking at is in a standard with an "Requirement" and been approved as a requirement, it cannot be audited – approval is a process question rather than content – cannot simply just borrow from NIST and run with it.
- Interested in finding out if we can offer it as an example
- Should this group make a formal request through Dave Taylor and Gerry Adamski to Standards Committee to ask for approval for the approach? If we ask now we maybe able to get an answer in 4-6 weeks assuming they do not consider it a change to the standards process
- Does the group want to pursue that option?

- They can authorize the executive committee to act quickly – get on the December docket of the Standards Committee – suggesting creating one bucket with three levels rather than three separate classes to apply NIST to CIP?
- Next standards committee meeting is in Phoenix in January
- Ask permission to put NIST standards out for review to let us go forward and use them?
- No, not the NIST catalogue but agreement that SDT can establish a controls catalogue – the concept, not a specific list.
- Can we produce a lot of controls from the SDT?
- Yes, asking permission to do so since it is not part of the typical standards process.
- This is much more of a risk management concept.
- Have to get a catalogue that goes through the process
- Suggesting a catalogue drawn from NIST and other sources that is appropriate for our industry then do some applicability mapping with h-m-l impact – vast majority of the list will not apply to any one system.
- Scoping and tailoring – not enthusiastic about taking NIST catalogue as a whole to modify.
- Agree to create our own catalogue – NIST just provides a starting point
- And a one size will not fit all
- We have an example of scoping and tailoring effort – careful not to scope and tailor all of the hard stuff out – the current NIST 853 is much more of a "how" than a "what" list – will need to tailor it to fit and also avoid the detail of how.
- Take this discussion into the group of volunteers identified earlier.
- Question- looking at separate document outside CIP-002 – still has to be FERC approved?
- We still need to determine the form and tools needed.
- Will default to be included in the standard anyway?
- Will need to determine what we are asking the Standards Committee – frame the question
- Why are we asking for permission? Don't standards have appendices? Why not go that route?
- Having a catalogue of controls relative to the level of rating to be applied and make it auditable – it may be an appendix – we don't not have a current model and need the Committee's concurrence in developing those controls.
- Question is do we want flexibility?
- 853 is the guidelines – NERC doesn't allow enforcement of guidelines – Keith is rewriting to make it an enforceable standard – catalogues have not been allowed in standards before so we need an okay from Standards Committee for the new model, whether it is in appendix or not.
- IS99 created a technical what standard – non-binding – but was run through their process – we are proposing something similar
- Still want to know why we can't develop as an appendix and simply appraise the committee for their approval – don't want to be distracted given the limited time – declare what we are doing, let them know, and keep moving.
- We can do this in parallel – move forward and create example and also ask Standards Committee for approval of the approach
- Doesn't matter where we put it – makes the standards more readable to put into appendix
- Agree if allowed under current structure

- We are getting wrapped up in format – what are we asking the Standards Committee? How is the catalogue applied? Give flexibility to the entity or have to apply catalogue?
- Catalogue needs to be developed to be dynamic, flexibility to adjust to changes and new attack vectors we can't anticipate
- That will not be acceptable to FERC, NERC or industry – the commission says only those things adopted through their process and made a mandatory reliability standard are enforceable
- We need to refocus on what needs to be accomplished today and going forward.
- Motion/2nd: Draft 1 should be ready by July 2010 for industry comment as part of workplan, addressing all of 706: Yes=11, No=3, Abstain=1.
- More comfortable offering October – we would have to do something different to get there by July – as much as I would like to say and get there in July, it is not realistic.
- Observation -- October is within the 24-month window.
- If deliver before then, all the better.
- Any in July willing to accept October?
- October may be more realistic – other factors mean we should shot for July – expectation is to show progress.
- When will there be a filing with FERC? That is the date that is valid – best possible date for that would be middle of 2011, maybe the end of 2011 to thrown over to FERC.
- Question: it will take a minimum two rounds of comments and minimum one calendar year after the Draft 1 posting to achieve consensus and go to ballot? Wants something formal that talks about the end game
- Question: in the best opinion of the standard drafting team, it will take four rounds of comments and eighteen months after the Draft 1 posting (July 2010) to achieve consensus and go to ballot? Yea=12; Nay=2; Abstain=0

D. SDT Agreements on Structure and Schedule

1. Strawman drafting team (made up of John, Jackie, Phil and John) – with current subgroups completion today or by Nov. 1? Deliverable - can we test what issues that group will tackle? Agreed.

2. Team of Catalogue of Controls volunteers (Joe Doetzl, Bill Winters, Keith Stouffer, Jon Stanford, Jim Breton, Jay Cribb) – address issue of appendix and approval from Standards Committee and report back in Orlando. Given discussion today – Keith's question of format is no longer relevant. Agreed.

3. In the best opinion of the standard drafting team, it will take four rounds of comments and eighteen months after the Draft 1 posting in July 2010 to achieve consensus and go to ballot. (Yes, 12; No 2, Abstain 0)

V. Guidance on issues and questions for the Straw Drafting Team

The SDT identified and then discussed key open issues:

5. Better identification of reliability functions (BES cyber system identification based on reliability functions) – MetaGroup 1 & 2
6. Better definition of terms used in BES mapping document: control centers/systems, generation systems, etc. – MetaGroup 1
7. Cyber impact analysis alternative approaches and implications – avoid unintended consequences – Group 2
8. Better sense of how the pieces fit together and how an entities will use it – reliability functions, where do they fit and how do you come up with cyber systems that apply – Meta Group 1 & 2

Following lunch, members discussed guidance on issues and questions for the Straw Drafting Team to consider including:

A. Better identification of reliability functions (BES cyber system identification based on reliability functions) – Meta Group 1 & 2

Member Comments:

- More than just operating systems.
- Original scope based on functions.
- Look at the definition in the template – changed during the SDT discussion yesterday.
- It appears more restrictive than what we have now you don't operate with a relay further down the system – is this "operate" in the right context?
- Cyber system which supports or performs?
- Strike "reliably" from this.
- Want it to tie into the reliability standards
- "Direct or indirect impact on the reliable operation of" – drawn from the old but has the key phrases
- We will still need good guidance
- Target of protection is a hard item to define.
- I like what is here because it is more the distributive element.
- But never referenced in the standards.
- Access control for connected systems
- Seems like a useful definition that may need to be moved to guidance
- Does the definition cover all the situations? How would control system be treated in terms of data? This is still missing something – this is an IT-centric definition – most people do not think of a relay as processing data.
- Cyber system can be a single device or several – "a discrete set of one or more" – industry sees an out they will take it – a minor add to clarify
- Should you add administration? – a hub is an administration point –
- I think administration is already encompassed here
- And/or display data? Does it add anything?
- Reliability Functions- need to make sure they are defined

- Get back to a brief description – Varnell's group had a list – use that to create definitions – Varnell and Kinas will work on and get to group by Nov. 1.

B. Better definition of terms used in BES mapping document: control centers/systems, generation systems, etc. – Meta Group 1

Member Comments:

- Better definition of BES subsystems?
- May need to use a different term for control center
- Also items that do not fall into the "control center" category – Jackie, John L. and others – will schedule time in the next week or so

C. Cyber impact analysis alternative approaches and implications – avoid unintended consequences – Meta Group 2

Member Comments:

- Are there medium or low cyber systems within BES subsystems?
- If interconnected with high impact systems, does it matter? Are they not high?
- Depends on how cyber system is structured
- Bigger the cyber system becomes the harder it is to manage the security – have to scope to maximum efficiency
- Look at RTUs independently? They are part of the system – some are higher impact than others – don't have to treat them like a control system
- Do all the pieces that make up the system default to high if any one part is high? If RTU is connected it is connected
- For some RTUs it would not matter if they go away
- This is why you need criteria to determine what is high or low impact on cyber impact side
- Can't make assumptions that those things in an integrated entity are all high – may not be in a non-integrated entity
- Reliability coordinator – everyone feeding the system becomes high
- Define the boundaries of the system – where does one begin and another end

D. How can we get a better sense of how the pieces fit together and how entities will use it? This includes where the reliability functions fit and how you come up with cyber systems that apply – Meta Group 1 and 2

VI. Next Steps and closing

The Chair reviewed the next steps including the schedule for the Version 3 response document and the CIP 002-4 effort. She thanked Joe Doetzl for hosting the meeting and providing excellent food and facilities.

The SDT adjourned at 2:45 p.m. on October 22.

Appendix # 1— October 20–22, 2009 Meeting Agenda

NOTE:
1. Agenda times may be adjusted as needed during the meeting
2. Subgroup meetings may not have access to telephones and WebEx

Proposed Meeting Objectives and Outcomes

- Welcome new members and outline SDT leadership transition
- Review FERC Order and Discussion of SDT response and industry comment process
- Review the CIP-002 work plan going forward
- Receive updates on TFE, VSLs, VRFs, and related cyber security efforts
- Receive and discuss reports from CIP-002 subgroups identifying key issues and coordination points
- Convene CIP-002 subgroup meetings
- Review and refine a draft outline for CIP-002
- Receive and discuss subgroup reports and draft CIP-002 language
- Agree on work plan, next steps and assignments

October 20, 2009

8:00 Welcome and Opening Remarks — Jeri Domingo-Brewer and Kevin Perry
Roll Call; NERC Antitrust Compliance Guidelines
Review of September 9-10 meeting summary and acceptance
8:20 Review of Meeting Objectives, Agenda and Meeting Guidelines — Bob Jones
8:25 Welcome New Members and Leadership Transition — Jeri Domingo-Brewer and Kevin Perry
8:40 Overview of FERC Order on CIP Version 2 — Scott Mix
8:45 Rapid Response Process — Special Meetings and Electronic Voting — Joe Bucciero
8:50 Review and Discussion of Response to FERC Order and Issues with Implementation Plan
10:15 Next Steps and Plan for mid-November Response Document
10:45 Review of CIP 002 Work plan and CIP 002 Subgroup Process — Stu Langton
11:15 Overview of CIP 002 Strawman Template — Joe Bucciero
11:30 Subgroup Reports to the SDT

1. Reliability Functions Subgroup Report and Key Issues and Draft CIP-002 Language — John Varnell
2. List of BES Subsystems/BES Cyber Systems Subgroup Report Key Issues and Draft CIP 002 Language — Jackie Collett
3. BES Mapping Subgroup Report and Key Issues and Draft CIP 002 Language — John Lim
4. Cyber Analysis Subgroup Report, and Key Issues and Draft CIP 002 Language — Phil Huff
5. Definition and Selection of Controls Subgroup Report, Key Issues and Draft CIP 002 Language — Keith Stouffer

3:25 Proposal for Subgroup Meetings — Jeri Domingo-Brewer and Kevin Perry
3:30 Subgroup Drafting Meetings (may be joint subgroups meetings at various locations)

October 21, 2009

8:00 Subgroup Drafting Meetings (at various locations)
10:30 Welcome and Agenda Review — Jeri Domingo-Brewer
10:35 Update on Technical Feasibility Exception (TFE) NERC Rules of Procedure — Jeri Domingo Brewer, Kevin Perry and Scott Mix
10:50 Update on VSLs/VRFs — Scott Mix
10:55 Update on other related cyber security initiatives — SDT Members
11:00 Subgroup Reports — Plenary Session

1. Reliability Functions Subgroup Report, Key Issues and Draft CIP 002 Language
2. List of BES Subsystems/BES Cyber Systems Subgroup Report, Key Issues and Draft CIP 002 Language
3. BES Mapping Subgroup Report Subgroup Report, Key Issues and Draft CIP 002 Language
4. Cyber Analysis Subgroup Report, Key Issues and Draft CIP 002 Language
5. Definition and Selection of Controls Subgroup Report, Key Issues and Draft CIP 002 Language

1:00 Continue Discussion of Key Issues from Subgroup Reports
3:15 Subgroup Drafting Meetings (may be joint subgroups meetings at various locations)

October 22, 2009

8:00 Subgroup Drafting Meetings (at various locations)
9:30 Welcome and Agenda Review — Jeri Domingo-Brewer
9:35 Review of CIP 002 Strawman and Subgroup Reports — Plenary Session

1. Reliability Functions Subgroup Report- Draft CIP 002 Language, Q & A
2. List of BES Subsystems/BES Cyber Systems Subgroup Report, Draft CIP 002 Language
3. BES Mapping Subgroup Report Subgroup Report, Key Issues and Draft CIP 002 Language
4. Cyber Analysis Subgroup Report, Key Issues and Draft CIP 002 Language
5. Definition and Selection of Controls Subgroup Report, Key Issues and Draft CIP-002 Language

1:15 Key Issues from Subgroup Reports and Drafting Assignments Going Forward
2:30 Review Work Plan

- Next Steps for Subgroups and SDT and the creation of a single CIP 002 text
- Review November Version 3 Response
- Meeting Evaluation

3:00 Adjourn

Appendix # 2 Attendees List

Attending in Person — SDT Members

1.	Rob Antonishen	Ontario Power Generation (Friday)
2.	Jeri Domingo-Brewer, Chair	U.S. Bureau of Reclamation
3.	Jim Breton	ERCOT
4.	Jay S. Cribb	Information Security Analyst, Southern Company Services
5.	Joe Doetzl Manager,	Information Security, Kansas City Pwr. & Light Co.
6.	Gerald S. Freese	Director, Enterprise Info. Security America Electric Pwr.
7.	Phillip Huff	Arkansas Electric Coop Corporation
8.	Doug Johnson	Exelon Corporation - Commonwealth Edison
9.	Frank Kim	Ontario Hydro
10.	Rich Kinas	Orlando Utilities Commission
11.	John Lim	CISSP, Department Manager, Consolidated Edison Co. NY
12.	David Norton	Entergy
13.	Kevin B. Perry, Vice Ch.	Director Critical Infrastructure Protection, SPP
14.	Christopher A. Peters	ICF International
15.	Scott Rosenberger	Luminant Energy
16.	David S. Revill	Georgia Transmission Corporation
17.	Kevin Sherlin	Sacramento Municipal Utility District
18.	Keith Stouffer	National Institute of Standards & Technology
19.	John D. Varnell	Technology Director, Tenaska Power Services Co.
20.	William Winters	Arizona Public Service, Inc.
21.	Scott Mix	NERC
22.	Joe Bucciero	NERC/Bucciero Assoc.
23.	Hal Beardall	FSU/FCRC
24.	Robert Jones	FSU/FCRC Consensus Center
25.	Stuart Langton	FSU/FCRC Consensus Center

SDT Members Attending via WebEx and Phone

26.	Brian McKay	Xcel
27.	Jackie Collett	Manitoba Hydro
28.	Tom Hofstetter	NERC

SDT Members Unable to Attend

29.	Jonathan Stanford	Bonneville Power Administration
30.	Sharon Edwards	Duke Energy

Others Attending in Person

31.	Bill Glynn	Westar Energy
32.	Rick Terrell	Luminant
33.	Chris Wright	Burns and MacDonald Engineering

Others Attending via WebEx and Phone

34.	Rob Hardiman	Southern Company Transmission (10-20, 21, 22)
35.	David Huff	FERC (10-20, 22)_
36.	Justin Kelly	FERC 10-21, 22)
37.	Hoang Neg	RRI Energy (10-20_
38.	Jon Stitzel	Burns and MacDonald Engineering

Appendix # 3 — NERC Antitrust Compliance Guidelines

I. General

It is NERC's policy and practice to obey the antitrust laws and to avoid all conduct that unreasonably restrains competition. This policy requires the avoidance of any conduct that violates, or that might appear to violate, the antitrust laws. Among other things, the antitrust laws forbid any agreement between or among competitors regarding prices, availability of service, product design, terms of sale, division of markets, allocation of customers or any other activity that unreasonably restrains competition.

It is the responsibility of every NERC participant and employee who may in any way affect NERC's compliance with the antitrust laws to carry out this commitment.

Antitrust laws are complex and subject to court interpretation that can vary over time and from one court to another. The purpose of these guidelines is to alert NERC participants and employees to potential antitrust problems and to set forth policies to be followed with respect to activities that may involve antitrust considerations. In some instances, the NERC policy contained in these guidelines is stricter than the applicable antitrust laws. Any NERC participant or employee who is uncertain about the legal ramifications of a particular course of conduct or who has doubts or concerns about whether NERC's antitrust compliance policy is implicated in any situation should consult NERC's General Counsel immediately.

II. Prohibited Activities

Participants in NERC activities (including those of its committees and Subroups) should refrain from the following when acting in their capacity as participants in NERC activities (e.g., at NERC meetings, conference calls and in informal discussions):

- Discussions involving pricing information, especially margin (profit) and internal cost information and participants' expectations as to their future prices or internal costs.
- Discussions of a participant's marketing strategies.
- Discussions regarding how customers and geographical areas are to be divided among competitors.
- Discussions concerning the exclusion of competitors from markets.
- Discussions concerning boycotting or group refusals to deal with competitors, vendors or suppliers.

III. Activities That Are Permitted

From time to time decisions or actions of NERC (including those of its committees and Subroups) may have a negative impact on particular entities and thus in that sense adversely impact competition. Decisions and actions by NERC (including its committees and Subroups)

should only be undertaken for the purpose of promoting and maintaining the reliability and adequacy of the bulk power system. If you do not have a legitimate purpose consistent with this objective for discussing a matter, please refrain from discussing the matter during NERC meetings and in other NERC-related communications.

You should also ensure that NERC procedures, including those set forth in NERC's Certificate of Incorporation and Bylaws are followed in conducting NERC business. Other NERC procedures that may be applicable to a particular NERC activity include the following:

- Reliability Standards Process Manual
- Organization and Procedures Manual for the NERC Standing Committees
- System Operator Certification Program

In addition, all discussions in NERC meetings and other NERC-related communications should be within the scope of the mandate for or assignment to the particular NERC committee or Subroup, as well as within the scope of the published agenda for the meeting.

No decisions should be made nor any actions taken in NERC activities for the purpose of giving an industry participant or group of participants a competitive advantage over other participants. In particular, decisions with respect to setting, revising, or assessing compliance with NERC reliability standards should not be influenced by anti-competitive motivations.

Subject to the foregoing restrictions, participants in NERC activities may discuss:

- Reliability matters relating to the bulk power system, including operation and planning matters such as establishing or revising reliability standards, special operating procedures, operating transfer capabilities, and plans for new facilities.
- Matters relating to the impact of reliability standards for the bulk power system on electricity markets, and the impact of electricity market operations on the reliability of the bulk power system.
- Proposed filings or other communications with state or federal regulatory authorities or other governmental entities.
- Matters relating to the internal governance, management and operation of NERC, such as nominations for vacant committee positions, budgeting and assessments, and employment matters; and procedural matters such as planning and scheduling meetings.

Any other matters that do not clearly fall within these guidelines should be reviewed with NERC's General Counsel before being discussed.

Appendix # 4 Meeting Schedule
October 2008–December 2010

Development of CIP Version 2 and Version 3 Framework
October 2008–July 2009
1. October 6–7, 2008 — Gaithersburg, MD Reviewed CIP-002-CIP-009, Agreed on Version 2 approach.
2. October 20–21 —Sacramento, CA CIP-002-CIP-009 Version 2 development
3. November 12–14, 2008 — Little Rock, AR CIP-002-CIP-009 Version 2 adoption for comment and balloting; CIP-002-CIP-009 Version 3 process reviewed.
4. December 4–5, 2008 — Washington D.C. CIP-002-CIP-009 Version 3 reviewed and debated, SDT member white papers assigned.
5. January 7–9 — Phoenix, AZ, Reviewed Technical Feasibility Exceptions white paper**,** reviewed industry comments on CIP-002-CIP-009 Version 2 products — established small groups to draft responses, reviewed Version 3 white papers.
January 15 — WebEx meeting(s) Small group drafted responses to industry Version 2 comments.
January 21 — WebEx meeting(s) Small group drafted responses to industry Version 2 comments.
6. February 2–4, 2009 — Phoenix, AZ Update on NERC Technical Feasibility Exceptions process**,** VSL process and SDT role**,** review of Version 3 White papers, strawman and principles**,** reviewed and adopted SDT responses to industry comments on Version 2 and Version 2 Product Revisions.
7. February 18–19, 2009 — Fairfax, VA Update on Version 2 process**,** NERC TFE process and VSL Team process; reviewed, discussed and refined Version 3 CIP-002 White papers, strawman, and principles.
8. March 10–11, 2009 — Orlando, FL Update on NERC TFE and VSL and VRF Team process and review and refine Version 3 CIP-002 Strawman Proposals
March 2–April 1, 2009 — 30-day Pre Ballot
Mid-March — NERC posts TFE draft Rules of Procedure for industry comment
March 30, 2009 — WebEx meeting(s) White Paper Drafting Team
April 1–10 — NERC Balloting on Version 2 Products
April 6, 2009 — WebEx meeting — White Paper Drafting Team
April 8, 2009 — WebEx meeting(s) — White Paper Preview- Full SDT Conference Call
April 11, 2009 — Version 2 Ballot Results (Quorum: 91.90% Approval: 84.06%) and Industry Comments-
9. April 14–16, 2009 — Charlotte NC Update on NERC TFE process, VSL Team process and NERC Critical Assets Survey; agreed and adopted responses for Version 2 industry comments for recirculation ballot; reviewed and refined Version 3 whitepaper and consensus points and progress report to NERC Member Representative Committee (MRC) May meeting.
April 28 and May 6, 2009 — White Paper Drafting Team Meetings and WebEx
April 17–27, 2009 — Recirculation Results: Quorum: 94.37% Approval: 88.32%
May 5, 2009 — NERC MRC Meeting, Arlington, VA- SDT progress report.
10. May 13–14, 2009 — Boulder City NV Reviewed MRC presentation and further SDT refinement and discussion of the Version 3 White Paper.
June 8 and June 15, 2009 — Working Paper Drafting Team Meetings and WebEx

11. June 17–18, 2009 — Portland OR Further SDT refinement of the draft CIP Version 3 Working Paper(s), reviewed SDT development process for June-December 2009; discussed potential SDT subcommittee structure and deliverables.
June **—** WebEx meeting(s)
Working Paper drafting group sessions including inputs from selected industry personnel to help establish BES categorization criteria

CIP-002 Development of Requirements, Measures, Etc. July-December 2009

12. July 13–14, 2009 in Vancouver, B.C., Canada
SDT reviewed, refined, and adopted SDT Working Paper. SDT adopted its response to NERC for Interpretation of CIP-006-1. SDT reviewed and adopted a proposal for CIP-002 Subgroups and Deliverables and convened subgroup organizational meetings to develop work plans. SDT adopted 2010 Meeting Schedule.

- July–August Interim Conference call meeting(s)
- CIP-002 Subgroup meetings
- CIP-002 Coordination Team meeting
- August 3**–**5, 2009 in Winnipeg, Manitoba **NERC Member Representative Committee**. Progress Report and presentation on new CIP Version 3 Working Paper-Concept- Reliability Standards on Cyber Security for MRC input.

13. August 20–21, 2009 in Charlotte, NC. SDT reviewed and responded to MRC input on Working Paper/CIP-002 Concepts and convened SDT Subgroup and plenary meetings to develop CIP-002 requirements and "proof of concept" control (s).
July–September — 45-day Industry Comment Period on CIP-002 Concept Working Paper
NERC Webinar- August–September Interim Conference Call meeting(s)

- CIP-002 Subgroup meetings (as ne
- CIP-002 Coordination Team meeting

14. September 9–10, 2009 in Folsom, CA. SDT reviewed and considered industry comments on the Working Paper and CIP-002 concepts and their application to the subgroup work and addressed coordinating issues through joint subgroup meetings. SDT agreed on meeting dates and proposed locations for January–December 2010
September–October Interim WebEx meeting(s)

- CIP-002 Subgroup meetings
- CIP-002 Coordination Team meeting

15. October 20–22, 2009 in Kansas City, MI

- SDT Subgroup drafting meetings — day one
- SDT Plenary Session(s) — day two subgroup reports on CIP-002 requirements
- Review and refine initial draft of CIP-002 single text

October–November Interim WebEx meeting(s)

- CIP-002 Coordination Team meeting

16. November 17–19, 2009 in Orlando, FL

- SDT plenary session(s) — to review and refine CIP-002 standard, requirements, measures and controls.
- November–December Interim WebEx meeting(s)
- Drafting teams as needed to finalize drafts

- CIP-002 Coordination Team meeting

17. December 15–16, 2009 in Little Rock AK

- SDT plenary session(s) to review, refine, and agree on and adopt CIP-002 standard, requirements, measures and controls.
- Agree on initial posting of draft CIP-002 for industry review and comment.

Refinement of CIP-002 and Development of Other CIP Standards
January–December 2010
(12 SDT monthly meetings and subgroup WebEx meetings as needed)

- SDT responds to industry comments on initial and subsequent postings of CIP-002, Version 3 (may be multiple comment periods, as required)
- Refine the CIP-002 through the comment period and submit new CIP-002 Version 3 Standard for Balloting along with the catalogue of controls (i.e. CIP-003-CIP-009 or its successor) OR
- Ballot CIP-002 while permitting industry to rely on CIP 003-CIP-009 until the full suite of controls (i.e. CIP-003-CIP-009 or its successor) is reviewed and presented for balloting.
- Submit the full suite of CIP Reliability Standards on Cyber Security for Industry Comment
- Refine and Submit the full suite of CIP standards for industry ballot
- NERC Board of Trustees adoption of the full suite of standards
- FERC approves and NERC Implements the full suite of CIP standards

Proposed 2010 Meeting Schedule

January 19–21 — Wednesday–Thursday, Atlanta GA	July 14–15, Wednesday–Thursday
February 17–19 —Thursday–Friday, Austin TX	August 11–12, Wednesday–Thursday
March 9–11 — Tuesday–Thursday, Phoenix, AZ	September 8–9, Wednesday–Thursday
April 14–15 — Wednesday–Thursday, Atlanta GA	Oct. 13–14, Wednesday–Thursday or Oct.12–14
May 12–13 — Wednesday–Thursday, Dallas TX	November 17–18, Wednesday–Thursday
June 9–10 — Wednesday–Thursday, Sacramento CA	December 15–16, Wednesday–Thursday

Appendix #5 CIP-002-4 Template

Standard Development Roadmap

This section is maintained by the drafting team during the development of the standard and will be removed when the standard becomes effective.

Development Steps Completed:

1. SAR posted for comment (insert dates of posting period).
2. Revised SAR and response to comments posted (insert dates of posting period).
3. Revised SAR and response to comments approved by SC (insert date of approval).
4. SDT appointed on (insert date).
5. First draft of proposed standard posted (insert dates of posting period).
6. Second draft of revised standard posted (insert dates of posting period).
7. Third draft of revised standard posted (insert dates of posting period).

Proposed Action Plan and Description of Current Draft:

This is the initial draft of the proposed standard and is being submitted to the Standards Committee with a request to authorize moving the standard forward to the next stage of the standards process.

Future Development Plan:

Anticipated Actions	Anticipated Date
1. Post for 30-day pre-ballot review.	(insert dates)
2. Conduct initial ballot.	(insert dates)
3. Post response to comments on initial ballot.	(insert date)
4. Conduct recirculation ballot.	(insert dates)
5. Submit standard to BOT for adoption.	(insert date)
6. File standard with regulatory authorities.	To be determined.

Definitions of Terms Used in Standard

This section includes all newly defined or revised terms used in the proposed standard. Terms already defined in the Reliability Standards Glossary of Terms are not repeated here. New or revised definitions listed below become approved when the proposed standard is approved. When the standard becomes effective, these defined terms will be removed from the individual standard and added to the Glossary.

1. **Cyber System —** A discrete set of one or more programmable electronic devices organized for the collection, storage, processing, maintenance, use, sharing, communication, disposition or display of data.

2. **BES Cyber System —** A Cyber System which has direct or indirect impact on the reliable operation of the Bulk Electric System.

3. **Target of Cyber Protection (Term may not be necessary) —** of the Target of Protection is (1) a set of BES Cyber Systems, (2) the components supporting their confidentiality, integrity, and availability requirements and (3) any other components needing protection based on their network or physical location within the BES Cyber System operating environment.

4. **Cyber System Confidentiality —**Preserving authorized restrictions on information access and disclosure.

5. **Cyber System Integrity —** Guarding against improper modification or destruction of Cyber System settings, presentation and/or data points. This includes ensuring the non-repudiation and authenticity of data.

6. **Cyber System Availability —** Ensuring timely and reliable access to and use of Cyber Systems.

7. **Generation Subsystem**

8. **Transmission Subsystem**

9. **Control Center**

Terms to be retired from the *Reliability Standards Glossary of Terms* once the standards that use those terms are replaced:

1. **Critical Assets**

2. **Critical Cyber Assets**

3. **Cyber Assets**

Appendix # 5

ROUGH DRAFT TEMPLATE FOR INITIAL CONSIDERATION OF CSO706 SDT

Introduction

Title: Cyber Security — BES Cyber System Identification and Classification

Number: CIP-002-4

Purpose: NERC Standards CIP-002-4 through CIP-xxx-4 provide a cyber security framework for the identification and protection of BES Cyber Systems to support reliable operation of the Bulk Electric System.

These standards recognize the differing roles of each entity in the operation of the Bulk Electric System, the criticality and vulnerability of the assets needed to manage Bulk Electric System reliability, and the risks to which they are exposed.

Business and operational demands for managing and maintaining a reliable Bulk Electric System increasingly rely on Cyber Assets supporting critical reliability functions and processes to communicate with each other, across functions and organizations, for services and data. This results in increased risks to these Cyber Assets.

Standard CIP-002-4 requires the identification, classification and documentation of the BES Cyber Systems associated with the BES Systems that support the reliability functions of the Bulk Electric System.

Applicability:

Within the text of Standard CIP-002-4, "Responsible Entity" shall mean:

Reliability Coordinator.

Balancing Authority.

Interchange Authority.

Transmission Service Provider.

Transmission Owner.

Transmission Operator.

Generator Owner.

Generator Operator.

Load Serving Entity.

NERC.

Regional Entity.

Structures, components, equipment and systems of facilities regulated by the U.S. Nuclear Regulatory Commission or the Canadian Nuclear Safety Commission that are determined to be associated with Balance of Plant.

Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

(Proposed) Effective Date: The first day of the eighth calendar quarter after applicable regulatory approvals have been received (or the Reliability Standard otherwise becomes effective the first day of the third calendar quarter after BOT adoption in those jurisdictions where regulatory approval is not required)

Requirements

Determine Functions *[Violation Risk Factor: High] [Time Horizon: Long-term Planning]*

Text, text, text

Text, text, text

Additional paragraphs.

Map Functions to BES Systems

Determine Classification of BES Systems

Responsible Entities shall apply the following criteria to map the list of BES Subsystems supporting the functions described in R1 to High, Medium and Low BES impact categories as follows:

3.1. High Impact (H)

3.1.1. Any Generation Subsystem whose loss results in a frequency deviation exceeding step A of the regional UFLS as calculated using the BA frequency bias setting. (Note BAL-003-0 R5) *(DHS Tier I)*

3.1.2. Any Generation Subsystem that, if lost or misused, results in an Interconnection Reliability Operating Limit (IROL) violation, as determined by an engineering evaluation or other assessment method. *(Critical Asset Guideline)*

3.1.3. Any Generation Subsystem pre-designated, long-term as Reliability “must run” units beyond the local utility area by the Balancing Authority, Reliability Coordinator, or Regional Reliability Assurer. *(Critical Asset Guideline)*

3.1.4. Any Generation Subsystem that has been determined to be essential to the reliability of the BES through an engineering evaluation or other assessment method approved by the Regional Reliability Assurer, for voltage stability beyond the local utility area. *(Critical Asset Guideline)*

3.1.5. Transmission Subsystems that contain switching stations 300 KV or higher with an aggregate rated switched capacity flow of 5000 MW or higher in the Eastern and Western Interconnections, or 200 KV or higher with an aggregate rated switched capacity flow of 3000 MW or higher in other Interconnections, unless they have been determined not to be essential to the reliability of the BES through an engineering evaluation or other assessment method approved by the Regional Reliability Assurer, either for voltage or frequency stability support. *(DHS Tier I)*

3.1.6. Transmission Subsystems that, if lost or misused, will result in an Interconnection Reliability Operating Limit (IROL) violation, as determined by an engineering evaluation or other assessment method. *(Critical Asset Guideline)*

3.1.7. Transmission Subsystems that, if lost or compromised, will result in the loss of a Generation Subsystem defined in this subsection 2.1, High Impact Subsystems. *(Critical Asset Guideline)*

3.1.8. Transmission Subsystems identified as essential to meeting Nuclear Plant Interface Requirements as per NUC-001 standard for high impact Nuclear facilities.*(Critical Asset Guideline)*

3.1.9. Transmission Subsystems that, if destroyed, degraded or otherwise rendered unavailable, may result in voltage collapse as determined through an engineering evaluation or other assessment method. *(Critical Asset Guideline)*

3.1.10. Transmission Subsystems that, if destroyed, degraded or otherwise rendered unavailable, may result in electric system collapse due to frequency related instability as determined through an engineering evaluation or other assessment method. *(Critical Asset Guideline)*

3.1.11. Transmission Subsystems that, if destroyed, degraded or otherwise rendered unavailable, may result in complete operational failure of the transmission system or separation or Cascading outages. *(Critical Asset Guideline)*

3.1.12. Special Protection System (SPS) or Remedial Action Schemes (RAS) Subsystems on 300 KV and above in the Eastern and Western Interconnections, or 200 KV and above in other Interconnections, that have an Adverse Reliability Impact. *(DHS Tier I)*

3.1.13. BES Subsystems that perform automatic load shedding of 300 MW or more.*(Critical Asset Guideline)*

3.1.14. Control Centers and backup Control Centers defined by the transmission assets they monitor or control with a threshold of 300,000 MW total transmission capability.

3.1.15. Control Centers and backup Control Centers defined by the generation assets they monitor or control with a threshold of 10,000 MW or more of total generation.

3.1.16. Control Centers and backup Control Centers defined by the total load they monitor or control with a threshold of 10,000 MW.

3.1.17. Control Centers and backup Control Centers performing Reliability Coordinator functions. .

3.2. Medium Impact (M)

3.2.1. High is: Any Generation Subsystem whose loss results in a frequency deviation exceeding step A of the regional UFLS as calculated using the BA frequency bias setting. (Note BAL-003-0 R5)

Low is: Any Generation Subsystem whose loss results in a frequency deviation up to .05 Hz as calculated using the BA frequency bias setting. (Note BAL-003-0 R5)

Need **"MEDIUM**"

3.2.2. Blackstart Generation Subsystems that have been included in the regional blackstart capability plan as described in EOP 007. *(DHS Tier I)*

3.2.3. Generation Subsystems which, if lost or misused, result in a System Operating Limit (SOL) violation, as determined by an engineering evaluation or other assessment method as explained in FAC-010 and FAC-011. *(Critical Asset Guideline)*

3.2.4. Any Generation Subsystem that has been determined to be essential to the reliability of the BES through an engineering evaluation or other assessment method, either for voltage stability within the local utility area. *(Critical Asset Guideline)*

3.2.5. Transmission Subsystems with 200 KV or higher with an aggregate switched capacity flow of 2,000 MW or higher in the Eastern and Western Interconnections, or with 100 KV or higher with an aggregate switched capacity flow of 1,000 MW or higher in other Interconnections, that have not been included in Section 2.1 above, that have been determined to be essential to the reliability of the BES through an engineering evaluation or other assessment method, either for voltage or frequency support. *(DHS Tier II)*

3.2.6. Transmission Subsystems comprising the Cranking Paths identified in EOP 005-2 R1.5. Transmission Subsystems that, if lost or misus*ed, results in a System Operating Lim*it (SOL) violation, as determined by an engineering evaluation or other assessment method. *(Critical Asset Guideline)*

3.2.7. Transmission Subsystems that, if lost or compromised, will result in the loss of a Generation Subsystem defined in this subsection 2.2, Medium Impact Subsystems. *(Critical Asset Guideline)*

3.2.8. Transmission Subsystems identified as essential to meeting Nuclear Plant Interface Requirements as per NUC-001-1 for Medium Impact Nuclear facilities.

3.2.9. Transmission Subsystems that, if destroyed, degraded or otherwise rendered unavailable, results in cascading outages that affect areas of the BES system within the local utility area, as determined through an engineering evaluation or other assessment method.

3.2.10. Transmission Subsystems that, if destroyed, degraded or otherwise rendered unavailable, may result in voltage going below the under-voltage load-shed points, as determined through an engineering evaluation or other assessment method. *(Critical Asset Guideline)*

3.2.11. Transmission Subsystems that, if destroyed, degraded or otherwise rendered unavailable, may result in frequency going below the under-frequency load-shed points, as determined through an engineering evaluation or other assessment method. *(Critical Asset Guideline)*

3.2.12. Special Protection Systems (SPS) or Remedial Action Scheme (RAS) Subsystems on less than 300 KV in the Eastern and Western Interconnections, or on less than 200 KV in other Interconnections that have an Adverse Reliability Impact. *)*

3.2.13. Control Centers and backup Control Centers defined by the transmission assets they monitor or control with a threshold of 100,000 MW or higher total transmission capability, not already included in Section 2.1 above.

3.2.14. Control Centers and backup Control Centers defined by the generation assets they monitor or control with a threshold of 5,000 MW or more of total generation, not already included in Section 2.1 above.

3.2.15. Control Centers and backup Control Centers defined by the total load they monitor or control with a threshold of 5,000 MW, not already included in Section 2.1 above.

3.3. Low Impact (L)
Everything else??

Determine BES Cyber Systems that support the BES Systems

(R5a) Determine Classification of BES Cyber Systems

The Responsible Entity shall identify and categorize its BES Cyber Systems using the following steps for each BES Cyber System:

- **BES Subsystem Mapping —** Identify all BES Subsystems through which the BES Cyber System supports or has the potential to impact one or more Reliability Functions.

- **Reliability Function Assessment —** Assess the potential function impact the BES Cyber System has on each of the associated BES Subsystems given the loss of Confidentiality, Integrity, or Availability within the BES Cyber System. Assign one of the following function impact categories for each BES Subsystem the BES Cyber System supports.

  - **High —** Severe degradation or loss of control of the BES Subsystem to an extent and duration that the Responsible Entity cannot perform one or more of its Reliability Functions.

  - **Medium —** Significant degradation or loss of control of the BES Subsystem to an extent or duration that the Responsible Entity can perform its Reliability Function, but the effectiveness is reduced.

  - **Low —** Degradation or loss of control of the BES Subsystem to an extent or duration that the Responsible Entity can perform its Reliability Function, but the effectiveness is noticeably reduced.

R5b. The Responsible Entity shall identify its BES Cyber Systems and determine the potential impact on the BES based on the loss, misuse or compromise of the BES Cyber System (according to [BES Mapping Table]). *(** Need to develop the reliability impact definition and the impact criteria definition for High, Med, and Low. Aggregation of BES subsystems and BES cyber systems versus the impact criteria needs to be defined. **)*

Merge Classification of BES Systems and BES Cyber Systems

Provisional Impact Categorization — Assign a provisional impact category to each BES Subsystem associated with the BES Cyber System using the following look-up table as a relation of both the potential function impact and BES impact mapping.

Function Impact \ BES Impact	High	Medium	Low
High	**High**	**Medium**	**Low**
Medium	**Medium**	**Medium**	**Low**
Low	**Low**	**Low**	**Low**

Final Categorization — Assign the resultant impact categorization of the BES Cyber System as the maximum provisional impact category from its associated reliability

functions. Once the Responsible Entity has determined a provisional impact of High, then they need not perform additional impact analysis.

Document resultant Classification

Approval resultant list

Measures

M1. Text

Compliance

Compliance Monitoring Process

Compliance Enforcement Authority

- Regional Entity for Responsible Entities that do not perform delegated tasks for their Regional Entity.
- ERO for Regional Entity.
- Third-party monitor without vested interest in the outcome for NERC.

Compliance Monitoring Period and Reset Time Frame

Not applicable.

Data Retention

- The Responsible Entity shall keep documentation required by Standard CIP-002-4 from the previous full calendar year unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.
- The Compliance Enforcement Authority in conjunction with the Registered Entity shall keep the last audit records and all requested and submitted subsequent audit records.

Compliance Monitoring and Assessment Processes

- Compliance Audits
- Self-Certifications
- Spot Checking
- Compliance Violation Investigations
- Self-Reporting
- Complaints

Additional Compliance Information

Text

Violation Severity Levels

R #	Lower VSL	Moderate VSL	High VSL	Severe VSL

Regional Variances

None.

Associated Documents

VERSION HISTORY

Version	Date	Action	Change Tracking
4.000	10/20/2009	Initial draft of Version 4 Use of new format standard template	

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Agenda
Cyber Security Order 706 SDT — Project 2008-06

October 20, 2009 | 8 a.m. – 5 p.m. CDT
October 21, 2009| 8 a.m. – 5 p.m. CDT
October 22, 2009| 8 a.m. – 3 p.m. CDT
Town Pavilion, 1111 Main St – *(cross street is 12th)*
Kansas City, MO 64105

NOTE:
1. Agenda Times May be Adjusted as Needed during the Meeting
2. Subgroup Meetings May Not Have Access to Telephones and WebEx

Tuesday, October 20, 2009

- Antitrust Compliance Guidelines
- Welcome new members and outline SDT leadership transition
- Review FERC Order and Discussion of SDT Response and Industry Comment Process
- Review the CIP 002 workplan going forward
- Receive and discuss reports from CIP 002 Subgroups identifying key issues and coordination points
- Convene CIP 002 Subgroup meetings

Wednesday, October 21, 2009

- *Subgroup Drafting Meetings (may be joint subgroups meetings at various locations)*
- Receive updates on TFE, VSL/VRF, and related cyber security efforts
- Review and refine a draft outline for CIP 002.
- Receive and discuss Subgroup reports and draft CIP 002 language
- *Subgroup Drafting Meetings (may be joint subgroups meetings at various locations)*

Thursday, October 22, 2009

- Review and refine a draft outline for CIP 002.
- Receive and discuss Subgroup reports and draft CIP 002 language
- Agree on work plan, next steps, and assignments

116-390 Village Blvd.
Princeton, NJ 08540
609.452.8060 | www.nerc.com

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Antitrust Compliance Guidelines

I. General

It is NERC's policy and practice to obey the antitrust laws and to avoid all conduct that unreasonably restrains competition. This policy requires the avoidance of any conduct that violates, or that might appear to violate, the antitrust laws. Among other things, the antitrust laws forbid any agreement between or among competitors regarding prices, availability of service, product design, terms of sale, division of markets, allocation of customers or any other activity that unreasonably restrains competition.

It is the responsibility of every NERC participant and employee who may in any way affect NERC's compliance with the antitrust laws to carry out this commitment.

Antitrust laws are complex and subject to court interpretation that can vary over time and from one court to another. The purpose of these guidelines is to alert NERC participants and employees to potential antitrust problems and to set forth policies to be followed with respect to activities that may involve antitrust considerations. In some instances, the NERC policy contained in these guidelines is stricter than the applicable antitrust laws. Any NERC participant or employee who is uncertain about the legal ramifications of a particular course of conduct or who has doubts or concerns about whether NERC's antitrust compliance policy is implicated in any situation should consult NERC's General Counsel immediately.

II. Prohibited Activities

Participants in NERC activities (including those of its committees and subgroups) should refrain from the following when acting in their capacity as participants in NERC activities (e.g., at NERC meetings, conference calls and in informal discussions):

- Discussions involving pricing information, especially margin (profit) and internal cost information and participants' expectations as to their future prices or internal costs.
- Discussions of a participant's marketing strategies.
- Discussions regarding how customers and geographical areas are to be divided among competitors.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Agenda
Cyber Security Order 706 SDT — Project 2008-06

November 16, 2009 | 5:00 p.m. – 9:00 p.m. EST
November 17, 2009 | 8:00 a.m. – 5:00 p.m. EST
November 18, 2009 | 8:00 a.m. – 5:00 p.m. EST
November 19, 2009 | 8:00 a.m. – 3:00 p.m. EST
Orlando Utilities Commission
6003 Pershing Ave.
Orlando, Florida 32822

NOTE:
1. Agenda times may be adjusted as needed during the meeting
2. Drafting group Meetings may not have access to telephones

Proposed Meeting Objectives and Outcomes

- Welcome new members and outline SDT leadership transition
- Review, Discuss, and Adopt SDT Response Document to Industry Comments on CIP Version 3
- Review the CIP-002-4 and CIP-002 through CIP-009-4 work plan going forward
- Receive updates on TFE, VSL, VRF, and related cyber security efforts
- Review CIP-002-4 Key Issues and Provide Guidance to Documents Drafting Groups
- Convene CIP-002-4 Document Drafting Groups
- Review and refine a draft CIP-002-4 strawman and related documents
- Agree on next steps and assignments

November 16, 2009
1. Consideration of FERC Version 3 Response Document Review

November 17, 2009
1. Review work plan decisions in October 2009 and feedback from NERC
2. Updates on Technical Feasibility Exception (TFE) NERC Rules of Procedure, VSLs, VRFs, and other related cyber security initiatives
3. Consideration and adoption of FERC Version 3 response document review — motion to adopt the CIP Version 3 response document *(when ready).*
4. Overview of CIP-002-4 and CIP-002 through CIP-009-4 work plan
5. Overview of CIP-002-4 strawman draft documents, format, and key remaining issues and challenges

November 18, 2009

1. Review of key remaining issues, challenges, and guidance to drafting groups
2. Convene SDT CIP-002-4 Document Drafting Groups
3. CIP-002-4 Document Drafting Group Reports and additional SDT guidance
4. Reconvene SDT CIP 002-4 Document Drafting Groups

November 19, 2009

1. Review, refinement, and consensus testing of CIP-002-4 strawman documents from Drafting Groups
2. Review of CIP-002-4 next steps for SDT Drafting Groups

- Discussions concerning the exclusion of competitors from markets.
- Discussions concerning boycotting or group refusals to deal with competitors, vendors or suppliers.
- Any other matters that do not clearly fall within these guidelines should be reviewed with NERC's General Counsel before being discussed.

III. Activities That Are Permitted

From time to time decisions or actions of NERC (including those of its committees and subgroups) may have a negative impact on particular entities and thus in that sense adversely impact competition. Decisions and actions by NERC (including its committees and subgroups) should only be undertaken for the purpose of promoting and maintaining the reliability and adequacy of the bulk power system. If you do not have a legitimate purpose consistent with this objective for discussing a matter, please refrain from discussing the matter during NERC meetings and in other NERC-related communications.

You should also ensure that NERC procedures, including those set forth in NERC's Certificate of Incorporation, Bylaws, and Rules of Procedure are followed in conducting NERC business.

In addition, all discussions in NERC meetings and other NERC-related communications should be within the scope of the mandate for or assignment to the particular NERC committee or subgroup, as well as within the scope of the published agenda for the meeting.

No decisions should be made nor any actions taken in NERC activities for the purpose of giving an industry participant or group of participants a competitive advantage over other participants. In particular, decisions with respect to setting, revising, or assessing compliance with NERC reliability standards should not be influenced by anti-competitive motivations.

Subject to the foregoing restrictions, participants in NERC activities may discuss:

- Reliability matters relating to the bulk power system, including operation and planning matters such as establishing or revising reliability standards, special operating procedures, operating transfer capabilities, and plans for new facilities.
- Matters relating to the impact of reliability standards for the bulk power system on electricity markets, and the impact of electricity market operations on the reliability of the bulk power system.
- Proposed filings or other communications with state or federal regulatory authorities or other governmental entities.
- Matters relating to the internal governance, management and operation of NERC, such as nominations for vacant committee positions, budgeting and assessments, and employment matters; and procedural matters such as planning and scheduling meetings.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Agenda
Cyber Security Order 706 SDT — Project 2008-06

November 16, 2009 | 5:00 p.m. – 9:00 p.m. EST
November 17, 2009 | 8:00 a.m. – 5:00 p.m. EST
November 18, 2009 | 8:00 a.m. – 5:00 p.m. EST
November 19, 2009 | 8:00 a.m. – 3:00 p.m. EST
Orlando Utilities Commission
6003 Pershing Ave.
Orlando, Florida 32822

NOTE:
1. Agenda times may be adjusted as needed during the meeting
2. Drafting group Meetings may not have access to telephones

Proposed Meeting Objectives and Outcomes

- Welcome new members and outline SDT leadership transition
- Review, Discuss, and Adopt SDT Response Document to Industry Comments on CIP Version 3
- Review the CIP-002-4 and CIP-002 through CIP-009-4 work plan going forward
- Receive updates on TFE, VSL, VRF, and related cyber security efforts
- Review CIP-002-4 Key Issues and Provide Guidance to Documents Drafting Groups
- Convene CIP-002-4 Document Drafting Groups
- Review and refine a draft CIP-002-4 strawman and related documents
- Agree on next steps and assignments

November 16, 2009
1. Consideration of FERC Version 3 Response Document Review

November 17, 2009
1. Review work plan decisions in October 2009 and feedback from NERC
2. Updates on Technical Feasibility Exception (TFE) NERC Rules of Procedure, VSLs, VRFs, and other related cyber security initiatives
3. Consideration and adoption of FERC Version 3 response document review — motion to adopt the CIP Version 3 response document *(when ready).*
4. Overview of CIP-002-4 and CIP-002 through CIP-009-4 work plan
5. Overview of CIP-002-4 strawman draft documents, format, and key remaining issues and challenges

November 18, 2009

1. Review of key remaining issues, challenges, and guidance to drafting groups
2. Convene SDT CIP-002-4 Document Drafting Groups
3. CIP-002-4 Document Drafting Group Reports and additional SDT guidance
4. Reconvene SDT CIP 002-4 Document Drafting Groups

November 19, 2009

1. Review, refinement, and consensus testing of CIP-002-4 strawman documents from Drafting Groups
2. Review of CIP-002-4 next steps for SDT Drafting Groups

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Draft 15th Meeting Executive Summary
Cyber Security Order 706 SDT — Project 2008-06

November 16, 2009 | 5:00 PM to 9 PM EDT
November 17, 2009 | 8:00 AM to 5 PM EDT
November 18, 2009 | 8:00 AM to 5 PM EDT
November 19, 2009 | 8:00 AM to 3 PM EDT

Orlando Utilities Commission, 6003 Pershing Ave.
Orlando Florida 32822

Robert Jones, Stuart Langton, and Hal Beardall
Facilitation and Meeting Design
FCRC Consensus Center, Florida State University

Joe Bucciero, Bucciero Consulting, LLC

http://www.nerc.com/filez/standards/Project_2008-06_Cyber_Security.html

116-390 Village Blvd.
Princeton, NJ 08540
609.452.8060 | www.nerc.com

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

CSO706 SDT November 16-19, 2009 Meeting Summary Contents

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

CSO706 SDT NOVEMBER 16-19, 2009 MEETING

EXECUTIVE SUMMARY

On Monday evening the Chair, Jeri Domingo-Brewer welcomed the members and Joe Bucciero conducted a roll call of members and participants in the room and on the conference call. The Chair reviewed the meeting objectives and Bob Jones, facilitator, reviewed the proposed meeting agenda. Mr. Bucciero reviewed the need to comply with NERC's Antitrust Guidelines.

Mr. Mix reminded the SDT of the FERC Order and 90-day response presented at the Kansas City meeting in October and provided an overview of the industry comments received the proposed revisions of CIP-002-2 through CIP-009-2, the Implementation Plan for Version 3 of the Cyber Security Standards, and the Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities, developed by the standard drafting team as part of Project 2009-21 Cyber Security Ninety-day Response. Mr. Mix noted that There were 29 sets of comments, including comments from more than 60 different people from approximately 40 companies representing 8 of the 10 Industry Segments.

The SDT reviewed, discussed and refined an initial strawman draft response document for CIP Version 3 prepared by Scott Mix for the 29 sets of comments received. At the end of Monday evening's meeting drafting assignments were reviewed. The SDT followed up on Tuesday morning and early afternoon and reviewed a refined document that included some new draft language for the consideration of comments document. The SDT reviewed a final draft with several revisions on Wednesday morning and unanimously adopted it for posting.

On Tuesday morning, Mr. Bucciero conducted a roll call of members and participants in the room and on the conference call and reviewed the need to comply with NERC's Antitrust Guidelines as he did on each of the following meeting days.

On Wednesday morning Scott Mix provided an Update on VSLs/VRFs noting that ballot had closed last Thursday with a high level of industry support. This would be approved by the NERC Board of Trustees and submitted to FERC. He noted the chair of the VSL/VRF SDT has volunteered to come in and give an update to the Team in January. In terms of the Version 2 VSL/VRF Mr. Mix indicated that there will have to be a correction for a technical error but that it looks like it will be approved which will close that group's work. The CSO706 SDT will be responsible for the VSLs/VRFs for Version 4. The SDT VSL/VRF chair will talk with the CSO706 SDT about their experience early next year to help us take on the task later in 2010.

SDT member discussed the updates on work related to the "smart grid" and its relation to the CIP development including the smart grid efforts and the need for coordinating this with the SDT's work.

Mr. Mix provided an update on the TFE process indicating that NERC is not expecting further actions by FERC – but will have to wait and see. He noted a compliance bulletin has been issued which directs industry to prepare for compliance – regions and NERC having discussions for a uniform system of compliance, should benefit those with coverage into different regions – have not seen a backlog of TFEs. The members discussed class based TFEs, mitigation plans, compliance schedules, and application to CAs and CCAs.

On Tuesday, facilitator Mr. Langton reviewed the workplan suggesting the SDT complete its initial draft of CIP-002-4 for posting by the conclusion of the December, 2009 meeting and launch the effort to develop the suite of controls (CIP 003-009) in early 2010. This will be a challenging parallel process with the SDT responding to industry comments and refining CIP 002-4 while simultaneously developing CIP 003-009. He noted that in January the SDT will review and agree on how best to organize to deliver on the milestones in the accelerated workplan.

At the end of the session on Tuesday afternoon, the SDT, at the request of NERC, engaged in a "blue sky" brainstorming session on ways to streamline the development process. The Team identified 36 suggestions in the following six categories: Changing ANSI Standards Procedures (3 options); Meeting Changes- Efficiency, Location, Tools (5 options); Commitment, Communication and Support (9 options); Team Structure (3 options); Substantive Changes in Approach/Scope to Standard Development (10 options); and More Talent and Expertise to Support SDT (6 options).

The Team agreed to engage in an exercise on Thursday to prioritize these options in terms of the highest priority and most helpful in facilitating the CIP standards development process. The results of the survey completed by 15 SDT members produced the following 5 options that received higher than a 4 rating on a 5-point scale *(from most helpful to don't do it):*

1. (4.46) Technical writer support (more writers like Scott Mix) (NERC) (11-5's & 4's and 2 -1's & 2's)
2. (4.43) Improve industry communications in getting the word out on the SDT and its progress? Webinars, workshops, etc. (NERC in Coordination with SDT) (11-5's & 4's and 0 -1's & 2's)
3. (4.36) Make the best use of our time. Start meetings on time and get the technology operational early(SDT)(8-5's & 4's and 0 -1's & 2's)
4. (4.21) Receive permission to use informal comment processes for the development of the CIP with a final 45-day comment period consistent with the ANSI process. (NERC) (7-5's & 4's and 1 -1's & 2's)
5. (4.00) Engage technical writers (NERC) (8-5's & 4's and 3 -1's & 2's)

On Thursday morning, the Chair and Vice Chairs participated on behalf of the SDT in a conference call with Mike Assante and Gerry Adamski at NERC and Alan Moser the Vice Chair of the NERC Standards Committee to discuss NERC's guidance to the Team on the schedule the Team reviewed and revised at their Kansas meeting in October. The NERC representatives

provided background in what is driving their schedule concerns noting in particular a perception from FERC and some on Capitol Hill that progress on Order 706 directives has been too slow which was underscored with the NERC survey back in the Spring. They noted that they believed that at least the CIP 002-4 (the asset categorization piece) needs to be filed with FERC by midyear and the CIP 003-009 by the end of the year. They offered commitment to providing the Team with whatever is need in terms of resources and communication with industry. The Team discussed the schedule and expressed concerns that: CIP 002-4 should not be watered down to fit today's CIP 003-009; that it might be difficult for the industry to adopt CIP 002-4 without seeing the controls in CIP 003-009; and the NERC conversation wasn't with the full team.

The Chair reviewed with the SDT the deliverables needed for posting in December, 2009 including: CIP-002-4 Requirements and measures; Sample controls (2-4 examples); Comment form with questions; Guidance document; Intro or cover letter; Related VSLs/VRFs: and Definitions.

John Lim provided an overview of Version 4 CIP 002 Strawman Draft Documents noting the current draft was still missing some definitions for the BES, generation and transmission subsystems and control centers. He noted that Jackie Collett and a sub-team (Scott Rosenberger, Gerry Freese, Jay Cribb) are tackling the definitions. He suggested that the critical assets guideline has started to create a definition that may serve as a starting point. Finally he pointed out that all of the generation assets in this draft has been moved from high to the medium level and that no unit by itself is considered high, but generation system could be in high. High also includes the major transmission facilities.

On Wednesday morning after reviewing and finalizing and adopting version 3 considerations document, the SDT broke into the following drafting groups for CIP 002-4: BES subsystem description/definition (led by Jackie Collett); Reliability functions definitions (led by John Varnell); Control Samples (Led by Keith Stouffer); and Guidance Document (led by Phil Huff). The facilitators noted that the SDT had to balance: getting it right; with getting enough consensus for acceptance; with getting it done in a timely manner. The SDT needs to optimize the three together.

Jackie Collett reported on the BES Subsystems Descriptions small group's results noting that they had a good start on a definition. John Varnell report that his group had developed 9 definitions for reliability functions and they had added definitions for each of the functions and included the examples which will be an attachment at end of CIP 002-4 standard and serve as a foundation for later sections.

Keith Stouffer noted that his group had developed two samples. He noted that the tables are designed to help the industry to understand the categorization process. The drafting group took two standards 009 and 006 to show how the categorization process might apply and their related requirements and asked the question: what is in the standard now is a "high" baseline. He suggested that even though we are adding categories, if you are low impact, there will be fewer requirements levied upon you.

Phil Huff noted that the Guidance Document group had found a way to simplify and the revised draft represented a major shift in name of simplicity. The proposal is to use the reliability functions for determining your BES cyber systems.

On Thursday, the drafting groups reported to the SDT. Keith Stouffer mentioned that in terms of the controls table format, the next big step to develop the information paragraph at the outset of each of the tables. Phil Huff noted that the Guidance Document would be developed further and circulated to the SDT in advance of the Little Rock meeting. The Chair noted she would circulate a draft of the "Comment Form". John Lim agreed to revise the CIP 002-4 draft for a preview in early December and then refine it and send it out to the SDT prior to the Little Rock meeting. Jackie Collett asked for time on the Little Rock agenda to go through a "walk through" of the CIP 002-4. She agreed to work with several SDT members to prepare materials for the walk through. NERC Staff (Maureen Long, Dave Taylor and Joel De Jesus) joined the SDT on Thursday morning and offered guidance in drafting the CIP 002-4.

The SDT Chair and Vice Chairs reviewed with the Team the updated agreed upon schedule for both the CSO 706 SDT Version 3 CIP and the Version 4 CIP 002 Process as follows:

CIP Version 3 Key Steps/Schedule

1. November 30, Monday *(after Thanksgiving)* Deadline for Votes and Industry Comments
2. December 2, Wednesday, CSO 706 SDT - Conference Call- finalize Response document to Industry Comments
3. December 3- 13, Recirculation Ballot
4. December 16, BoT Approval
5. December 29, 2009, FERC Filing

CIP 002-4 Key Steps/Schedule (October-December 2009)

1. December 7, 3:00-4:30 p.m. est. Previews of reviewed CIP 002 and related document drafts at a SDT conference call.
2. Other drafting groups will organize and schedule meetings prior to Little Rock.
3. The SDT will refine and circulate a revised strawman Draft by Monday, December 14, 2009 for review at the December 15-16 CSO706 SDT meeting in Little Rock
4. December 15-16 will refine, finalize and adopt draft CIP 002-4 for posting to the industry for informal comments.

The Chair reviewed the next steps including the schedule for the Version 3 response document and the CIP 002-4 effort. She thanked Rich Kinas for hosting the meeting and providing excellent food and facilities.

The SDT adjourned at 2:00 p.m. on November 19, 2009.

CSO706 SDT NOVEMBER 16-19, 2009 MEETING SUMMARY

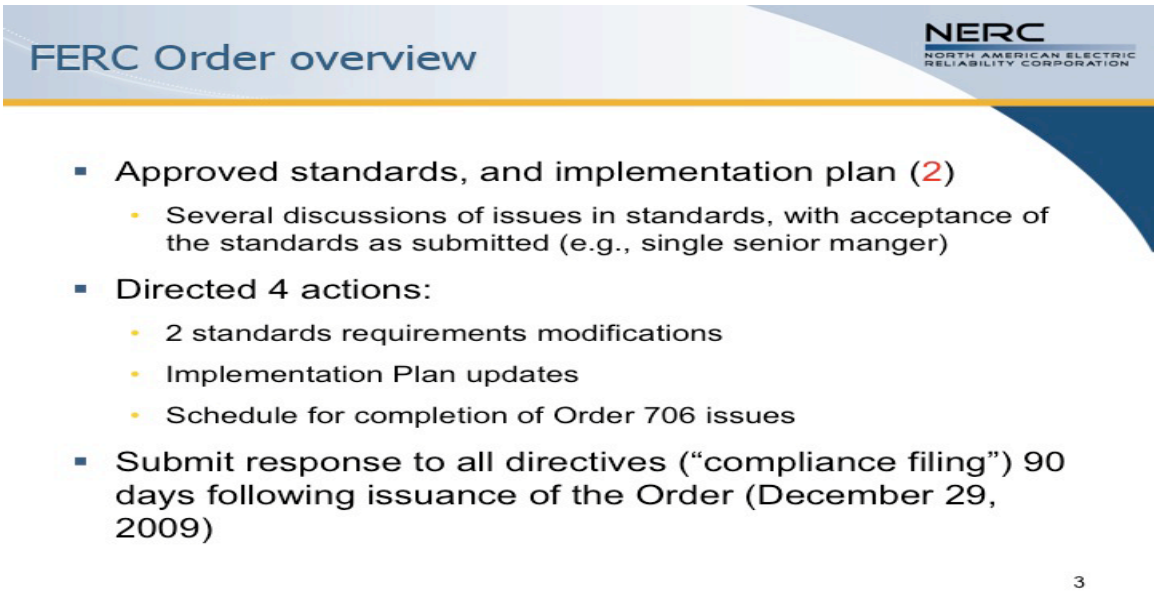
I. FERC ORDER ON CIP VERSION 2 AND VERSION 3 COMMENT RESPONSE DOCUMENT

A. Introduction

On Monday evening the Chair, Jeri Domingo-Brewer welcomed the members and Joe Bucciero conducted a roll call of members and participants in the room and on the conference call *(See appendix #2*). The Chair reviewed the meeting objectives and Bob Jones, facilitator, reviewed the proposed meeting agenda *(See appendix #1*). Mr. Bucciero reviewed the need to comply with NERC's Antitrust Guidelines *(See Appendix #3)* and repeated this the beginning of each day of the meeting. He urged the team and other participants in the process to carefully review the guidelines as they would cover all participants and observers. He urged all to avoid behaviors or appearance that would be anti-competitive nature and also reminded the group of the sensitive nature of the information under discussion.

B. CIP Version 3 90-day Comment Response Document

Mr. Mix reminded the SDT of the FERC Order and 90-day response presented at the Kansas City meeting in October:



He provided an overview of the industry comments received the proposed revisions of CIP-002-2 through CIP-009-2, the Implementation Plan for Version 3 of the Cyber Security Standards, and the Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities, developed by the standard drafting team as part of Project 2009-21 Cyber Security Ninety-day Response. These standards were posted for a 30-day public comment period from October 13, 2009 through November 12, 2009. The stakeholders were asked to provide feedback on the standards through a special Electronic Comment Form that included the following questions:

1. In its order approving CIP-002-2 through CIP-009-2, the Commission directed NERC to make changes to CIP-006-2 and CIP-008-2 as well as the implementation plan for newly identified critical cyber assets and file those changes within 90 days of the order. Do you agree that the SAR accurately addresses the scope of these directives? If not, please identify what you feel is missing in the SAR.
2. Do you agree that the proposed modifications to CIP-006-2, CIP-008-2, and the implementation plans meet the intent of the Commission's directives? If not, please identify what changes you feel are needed to meet the intent of these directives.
3. Do you have any additional comments associated with the proposed SAR for Project 2009-21: Cyber Security Ninety-day Response? If yes, please explain.
4. Do you have any additional comments associated with the proposed CIP-006-2, CIP-008-2, and the implementation plans? If yes, please explain.

Mr. Mix noted that There were 29 sets of comments, including comments from more than 60 different people from approximately 40 companies representing 8 of the 10 Industry Segments as shown in the table on the following pages.

http://www.nerc.com/filez/standards/Project2009-21_Cyber_Security_90-day_Response.html

The SDT reviewed, discussed and refined an initial strawman draft response document for CIP Version 3 prepared by Scott Mix for the 29 sets of comments received. At the end of Monday evening's meeting drafting assignments were reviewed. The SDT followed up on Tuesday morning and early afternoon and reviewed a refined document that included some new draft language for the consideration of comments document. The SDT reviewed a final draft with several revisions on Wednesday morning and unanimously adopted it for posting as show on the following pages:
http://www.nerc.com/docs/standards/sar/C-of-C_Cyber_90day_Response_Initial_Ballot_2009Dec3.pdf

A. AGENDA REVIEW AND UPDATES

A. Agenda Review

On Tuesday morning, the Chair, Jeri Domingo-Brewer welcomed the members and Joe Bucciero conducted a roll call of members and participants in the room and on the conference

call *(See appendix #2*). The Chair reviewed the meeting objectives and Bob Jones, facilitator, reviewed the proposed meeting agenda *(See appendix #1*).

Mr. Bucciero reviewed the need to comply with NERC's Antitrust Guidelines *(See Appendix #3).* He urged the team and other participants in the process to carefully review the guidelines as they would cover all participants and observers. He urged all to avoid behaviors or appearance that would be anti-competitive nature and also reminded the group of the sensitive nature of the information under discussion.

B. Updates

VSLs/VFRs. On Wednesday morning Scott Mix provided an Update on VSLs/VRFs noting that ballot had closed last Thursday with a high level of industry support. This would be approved by the NERC Board of Trustees and submitted to FERC. He noted the chair of the VSL/VRF SDT has volunteered to come in and give an update to the Team in January.

In terms of the Version 2 VSL/VRF Mr. Mix indicated that there will have to be a correction for a technical error but that it looks like it will be approved which will close that group's work. The CSO706 SDT will be responsible for the VSLs/VRFs for Version 4. The SDT VSL/VRF chair will talk with the CSO706 SDT about their experience early next year to help us take on the task later in 2010.

Other Cyber Security Initaitives. SDT member discussed the updates on work related to the "smart grid" and its relation to the CIP development.

SDT Comments on Related Cyber Security Initiatives

- Don't hear us talking much about smart grid or smart grid people talking much about the CIP standards – seem to have a gap in communication
- NERC standards only apply to the BES assets – not small production – smart grid is looking at everything from production, transmission all the way into the home –
- NIST is getting lots of pressure to roll things out.
- Who is supposed to be making the link? There is a group that is supposed to coordinate security across all the groups. But key issues haven't been raised to date such as: do we really want a system that is fully inter-operative? Do we want millions of smart meters running through the same system as our control systems? If it works really well in AMI how do you make sure it is good for transmission or is complimentary – also note it is another security system to be aware of and prepared for.
- A Wisconsin study commissioned by FERC was briefly discussed.

Technical Feasibility Exceptions. Mr. Mix provided an update on the TFE process indicating that NERC is not expecting further actions by FERC – but will have to wait and see. He noted a

compliance bulletin has been issued which directs industry to prepare for compliance – regions and NERC having discussions for a uniform system of compliance, should benefit those with coverage into different regions – have not seen a backlog of TFEs

Member Comments on TFE Update

- What is going on with class based TFEs?
- Personal view – list is an after the fact addition to the list once we see what is out there rather than trying to come up with a complete omniscient list to start with
- Mitigation plans? Personal opinion – do not give examples because too many will rely on example as to how to comply, rather leave it up to individuals to determine what to do with TFEs initially
- Do not see class will give companies much help in defining mitigating measures – not buy you much time
- Why January cut off if you can retroactively identify and add to the list?
- Does the device you are requesting TFE on have to be a CA or CCA? May not identify if there is disagreement within an organization or may identify only to cover potential.
- Standards only apply to CCAs. Sounds like you are creating a significant workload for approval for something you will not be held accountable for. No harm waiting until it is on the CCA list.

A. WORKPLAN REVIEW AND STREAMLINING THE CIP DEVELOPMENT PROCESS

A. Workplan Review

Mr. Langton reviewed the workplan suggesting the SDT complete its initial draft of CIP-002-4 for posting by the conclusion of the December, 2009 meeting and launch the effort to develop the suite of controls (CIP 003-009) in early 2010. This will be a challenging parallel process with the SDT responding to industry comments and refining CIP 002-4 while simultaneously developing CIP 003-009. He noted that in January the SDT will review and agree on how best to organize to deliver on the milestones in the accelerated workplan.

B. Considerations in Streamlining the CIP Development Process

At the end of the session on Tuesday afternoon, the SDT, at the request of NERC, engaged in a "blue sky" brainstorming session on ways to streamline the development process. The Team identified 36 suggestions in the following six categories:

A. CHANGING ANSI STANDARDS PROCEDURES (3 options)
B. MEETING CHANGES- EFFICIENCY, LOCATION, TOOLS (5 options)
C. COMMITMENT, COMMUNICATION AND SUPPORT (9 options)
D. TEAM STRUCTURE (3 options)
E. SUBSTANTIVE CHANGES IN APPROACH/SCOPE TO STANDARD DEVELOPMENT (10 options)
F. MORE TALENT AND EXPERTISE TO SUPPORT SDT (6 options)

The Team agreed to engage in an exercise on Thursday to prioritize these options in terms of the highest priority and most helpful in facilitating the CIP standards development process. The results of the survey (See Appendix # 6) completed by 15 SDT members produced the following 5 options that received higher than a 4 rating on a 5-point scale (from most helpful to don't do it):

1. (4.46) Technical writer support (more writers like Scott Mix) *(NERC) (11-5's & 4's and 2 -1's & 2's)*
2.(4.43) Improve industry communications in getting the word out on the SDT and its progress? Webinars, workshops, etc. *(NERC in Coordination with SDT)* ***(11-5's & 4's and 0 -1's & 2's)***
3.(4.36) Make the best use of our time. Start meetings on time and get the technology operational early*(SDT)*(8-5's & 4's and 0 -1's & 2's)
4. (4.21) Receive permission to use informal comment processes for the development of the CIP with a final 45-day comment period consistent with the ANSI process. ***(NERC) (7-5's & 4's and 1 -1's & 2's)***
5. (4.00) Engage technical writers *(NERC (8-5's & 4's and 3 -1's & 2's)*

In terms of possible substantive changes to the SDT approach or scope the ranked the following 10 strategies on the 5-point scale:

E. SUBSTANTIVE CHANGES IN APPROACH/SCOPE TO STANDARD DEVELOPMENT

Avg. Ranking	*Streamlining Strategy*	*# of 5's & 4's*	*# of 1's & 2's*
3.62	Refocus on security issues and less on compliance *(SDT)*	**8**	**3**
3.54	Remove penalty base requirements (you get what you measure) *(NERC, FERC, Congress)*	**6**	**4**
3.46	Simplify the approach and strategy to the standards to reduce com *(SDT)*	**7**	**3**
3.08	Adapt 800-82 (targeted for industrial control systems) *(NERC & S*	**3**	**7**
2.92	Adopt 800-53 Rev 3 for control centers and data centers *(NERC & SDT)*	**4**	**6**
2.92	Review Order 706 and remove items included that should be give	**4**	**5**

	another group, challenged or deferred. *(NERC & SDT)*		
2.46	Throw in with CSCTG from NIST *(NERC)*	**2**	**8**
2.38	Go back to the 'original, original' standards for cyber security as a basis for the new CIP (see NERC Website archive) *(SDT)*	**2**	**7**
2.08	Skip BES Mapping and install minimum security controls for all a after establishing clear cut agreed upon objectives on what we are securing. *(SDT)*	**2**	**10**
1.85	Abandon the NIST based approach and improve existing standards framework. *(SDT)*	**0**	**13**

On Thursday morning, the Chair and Vice Chairs participated in a conference call with Mike Assante and Gerry Adamski at NERC and Alan Moser the Vice Chair of the NERC Standards Committee to discuss NERC's guidance to the Team on the schedule the Team reviewed and revised at their Kansas meeting in October. The NERC representative provided background in what is driving their schedule concerns noting in particular a perception from FERC and some on Capitol Hill that progress on Order 706 directives has been too slow which was underscored with the NERC survey back in the Spring. They noted that they believed that at least the CIP 002-4 (the asset categorization piece) needs to be filed with FERC by midyear and the CIP 003-009 by the end of the year. They offered commitment to providing the Team with whatever is need in terms of resources and communication with industry.

SDT Member Comments on the Schedule

- NERC wants to know what we need to do the job. Getting the asset categorization issue fixed and filed.
- Exercise with language in CIP requirements- SDT does a cut these existing requirements apply to H/M/L.
- Impact level piece of CIP out there. Could be a transition point and is familiar for industry.
- Addressing directives and FERC order and problems identified in CIP requirements.
- May need a Version 5 or more.
- NERC Acknowledged the concept paper and suggested the Team is on the right path.
- Nervous about writing the new 002 and apply 3-9 beneath it. 3-9 as they are now only apply to the high.
- Don't water down the new 2 to fit with the 3-9 today. Get 002 right and then tweak 003-009.
- Concern of pushing 002 to ballot ahead of 003-009?
- How to handle the critical/non critical.

- If we do this on version 2- don't leave pieces in that will cause problems in just changing CIP 002.
- Not just changing categorization of only BES assets. Could be dangers down this path.
- We have to finish this job.
- How is the industry going to feel about being thrown a different set of requirements- then another change.
- Will the industry have to do anything with the controls? Especially mentioned an implementation plan.
- This would be expected to be done?
- If go H/M/L on existing requirements? Industry will have to apply to more stuff. But the plan is to have all of the CIPs done in 2010.
- June 2010- CIP 002 balloted. Current requirements should be at least applicable to all the highs.
- Will entities identify additional high assets that were not critical?
- The implementation plan should address how much time you give the entities to apply the controls to meet the requirements for the newly identified high impact facilities.
- Medium and low? Take current requirements and determine which are applicable to medium resulting in another implementation schedule.
- Main concern is to put something out there to push industry to stop "gaming" the system. You are going apply 3-9 to the high level categories at a minimum and then file your TFEs
- For part of the Order 706 directives, we are showing progress.
- Interim measures may not a good value.
- 2 issues on urgency raised by NERC- perceived deficiencies. FERC and Congress believe there are a lot of facilities that should be critical but are not. Second the all or nothing approach of the current standards.
- Our concept paper laid out the proposition that everything needs some level of protection- i.e. "all in."
- Concerned that NERC didn't open up this discussion to the whole team. Would have been less disruptive and more efficient.
- Another way: going with formal comments- implementation plan change.
- Going to ballot on Friday for the implementation plan. We are about to ballot something that will have impact which will change all that. This comes along with V2 as part packet.

- June for just CIP 002? Another 7 months?
- This is not a surprise. 6 months/ another 6 months. We have ignored the growing concerns and this has happened. Doesn't see a problem with 3-9. We can do a better job.
- New CIP 002 would introduce new categories. Connectivity issue was to be addressed later by controls. i.d. by CAs without CCAs. Big count.
- Would the existing 3-9 given H/M/L on each requirements meet the Order 706 requirements? Probably not. The industry may not vote yes if you don't know what you are going to have to do in 003-009.
- If we are going to get this done, the SDT needs NERC at every meeting with their attention solely on this meeting. They need to answer questions at the moment they come up so we will need someone with authority and expertise.
- I am not surprised about time crunch. Direction doesn't surprise. 002 doesn't surprise. What is the proposal for 003-009 requirements?
- Is the expectation of industry approval of 002 without knowing exactly what this means. What do I do now? This was something to do with the 3 lists.
- We should seek to get a fairly solid CIP 002 in December and stick with that.
- Likes this approach of providing some relief of participating team members and their organization from CIP audit schedule.
- Congressman Langevin asked Jon Stanford about progress being made by the SDT. Congress recognizes the hard work and challenges we have. Mr. Stanford asked what he should bring back to the Team from him. He said to tell the Team to continue the hard work and try to work towards a NIST like model with impact levels for assets. Our current path could receive a lot of support from congressional side. We know that if we don't change the standards, there will be legislation. There are at least several draft bills pending. Need to think about our priorities for cyber security and no so much about the ballot body.

IV. CIP 002 VERSION 4 STRAWMAN

A. Introduction

The Chair reviewed with the SDT the deliverables needed for posting in December, 2009 including: CIP-002-4 Requirements and measures; Sample controls (2-4 examples); Comment form with questions; Guidance document; Intro or cover letter; Related VSLs/VRFs: and Definitions

B. Overview of CIP 002-4 Strawman

John Lim provided an overview of Version 4 CIP 002 Strawman Draft Documents noting the current draft was still missing some definitions for the BES, generation and transmission subsystems and control centers. He noted that Jackie Collett and a sub-team (Scott Rosenberger, Gerry Freese, Jay Cribb) are tackling the definitions. He suggested that the critical assets guideline has started to create a definition that may serve as a starting point. Finally he pointed out that all of the generation assets in this draft has been moved from high to the medium level and that no unit by itself is considered high, but generation system could be in high. High also includes the major transmission facilities.

SDT Comments on Strawman Draft

- Some others have already set markers as to what they think is high – do we need to socialize those with ours? What happens if our list is less? Is that politically acceptable?
- We may eventually be told what to include and need to focus on the controls.
- Still having trouble understanding if intent of step 2 is to categorize by impact and step 3 is to assess impact on the BES – where are we in syncing these pieces?
- Two separate assessments, but have to do both assessments to understand the related impact on each other.
- R2 feeds into R3 – not completely separate assessments.
- Want to be sure we keep going down the path we are headed regardless of whether or not we think they may come in and take it away from us
- Want to be sure we produce a polished product the industry can understand and use
- How the two pieces come together may be addressed in the Guidance document.
- Uncertain whether we need to include a reliability function assessment – brought it down from three to two level system of high/low
- The current strawman takes a low water mark approach rather than the high water mark approach.
- Detection starts with who “owns and operate” – should it be “owns or operates it”? Big difference
- Like the definition of high and low but still begs question of “none”
- “None” may falls out of the definition of BES cyber system
- In case of a generator – if I have just one and my role ends there, do I have to make an assessment? Can they get the information they need from the generation system to make the assessment?

- You can get pricing data but not much else
- Reviewed tables/matrix in response to "none"
- Reliability coordinators can decide this.
- R3.2 in the matrix – from "optics" perspective difficult to explain why it drops from high to low
- Are assets being assigned to the BES system or the subsystems?
- It is not the concept but the wording that causes confusion. Change to "assigning the reliability impact to the BES cyber system that supports the subsystem" (wording from Jackie Collett)
- R2.4.2 vs. R4: separate requirement in each or just one time?
- Problem is with initial list – explicitly calls each out to avoid question of whether I must have a list before compliance assessment.
- Senior manager signs off on original and annual.
- Matrix – function impact correlates to cyber systems – may need to adjust the high BES impact and function impact from low to medium.
- Just because there is connectivity doesn't mean something will go through.
- Concerned about the level of complexity we are creating – more words give more opportunity to vector off course.
- There are a lot more words but a simpler system to use than what we have currently – we will probably make mistakes, but also progress.
- We were told last week by NERC not to use the measures in an assessment. Measures are included in the requirements here for that reason.
- In our recent NERC audit they did not use measures, only looked at requirements
- Intent is to include it in an appendix to the standard.
- We need examples to illustrate the tables –
- We will have descriptions of the functions in the next day or so as well as the definitions.
- Keep in mind the comment form questions too
- Existing single control example shows little gradation
- Hope to have a second example with more gradation drafted tomorrow (Keith, Bill and Joe will work on)

C. CIP 002-4 Small Group Discussions

On Wednesday morning after reviewing and finalizing and adopting version 3 considerations document, the facilitators reviewed the proposal for the SDT breaking into the following drafting groups for CIP 002-4: BES subsystem description/definition (led by Jackie Collett); Reliability functions definitions (led by John Varnell); Control Samples (Led by Keith Stouffer); and Guidance Document (led by Phil Huff).

SDT Comments on the Proposal:

- What are we doing with brainstormed list of ideas? The Chair noted she contacted Mike Assante by email last night and he agreed to call in later today to discuss then full group can discuss ways to accelerate the work plan.
- I have a concern that we spend time today and tomorrow going down the wrong way if we are going to entertain a new direction?
- We have made a commitment to NERC, industry and congress to get the CIP 002 review document out in December 2009 and we are close. If the SDT revisits our decisions it may derail the progress we have made on the December deliverable.
- Would be a disservice to put something out that will not work or is not understood.
- If put something out it has to be credible – good start but not enough time to vet decisions we are making – recommend starting a small subgroup to work in parallel to look at modifying current CIP standard to see how much of the FERC order can be incorporated – it stands the best chance of getting approval by the June time frame.
- When we put the concept paper out in July, we thought we would get more push back – it was more accepted than expected – commitment as a group to take a certain approach and have invested a year – have not heard negative comment from the industry for the approach we are taking – underestimating it would take to modify current standard – just as much effort as the approach we are taking – rehashing the same issue over again would be a step backward and impede us from focusing on our objectives and charge.
- The facilitator noted that the SDT is balancing three values:
  - 1. Getting it right;
  - 2. Getting enough consensus for acceptance;
  - 3. Getting it done in a timely manner. The SDT needs to optimize the three together – yesterday was an opportunity to put ideas on table, need to hear back from NERC before we discuss the issues further.
- Going back into 706? One big issue was criteria for selection, could be a show stopper if Regions refuse to do it – looking at order is a good idea but on this point could be arguing for a year without resolution.
- Modifying current CIP 2 would not be derailed by consideration of external reviews

- Issue is not about philosophy but rather one of resources and liability. Regions are very concerned.
- Lack of industry response may not be acceptance – could be a lack of understanding or commitment to engage until they get a final version. This needs to be crisper more easily understood --complexity is a problem.
- NERC has many balls in the air for industry to consider and respond to at the same time

On Wednesday the facilitators reviewed the proposal for the SDT breaking into the following drafting groups for CIP 002-4:

1. BES subsystem description/definition (Jackie Collett, Scott Rosenberger, Gerry Freese)
2. Reliability functions definitions (John Varnell, Rick Kinas, John Lim, Doug Johnson)
3. Control Samples (Keith Stouffer, Bill Winters, Jeri Brewer Domingo, John Stanford, Sharon Edwards and Jim Breton)
4. Guidance Document (Phil Huff, Dave Revill and Rob Antonishen) – needs help to review for accuracy of process, and the generation, transmission and control

Following small group meetings, the leaders of each group presented a report to the full SDT.

1. BES Subsystems Descriptions

Jackie Collett reported on the small group's results noting that they had a good start on a definition. The group is looking at basic building blocks for each.

SDT Member Comments and Guidance

- Generation- "Big Iron" side. Cyber system treated as a subsystem? Yes.
- BES Subsystem not defined as a single thing. Combinations of units that create an impact. Words intended to drive towards identifying combinations.
- Transmission subsystems.
- Control Centers- CIPSE critical asset guideline.
- How did you determine how a subsystem? Is there a common BES transmission bus(s) connecting generation units?
- Collection of units supported by a shared cyber system.
- From BES side and from the Cyber side- separated in documents.

2. Reliability Functions

John Varnell noted that they had developed 9 definitions for reliability functions and they had added definitions for each of the functions and included the examples. This will be an attachment at end of CIP 002-4 standard and serve as a foundation for later sections

SDT Member Comments and Guidance

- Is there anything in reliability in functions not included in BES mapping functions?

3. Control Samples

Keith Stouffer noted that his group had "kicked some CIP ass" and described two samples they have developed. He noted that the table are designed to help the industry to understand the categorization process. The drafting group took two standards 009 and 006 to show how the categorization process might apply and their related requirements and asked the question: what is in the standard now is a "high" baseline. Pare back for medium and low systems. Should note that even though we are adding categories, if you are low impact, there will be fewer requirements levied upon you. They will put this into new standard format and displaying same content in table or requirement formats. Stuck to low moderate and high. Not ready yet.

SDT Member comments

- Assumption is current CIP are all high? Because they apply to critical assets?
- Careful we don't get boxed in.
- Make clear that this is only showing an existing standard not what the 009-4 standard will look like.
- Took declaratives from FERC order? E.g. Firewalls from multiple vendors.
- Concerned with adding complexity by getting into the particulars/standards at this point.
- Give a before and after example. Mapping before and after. Access control requirement.
- How much complexity are in these examples?
- We told industry that we have been building upon work already being done. Shows a transition to a future- where you will have impact levels. Ability to target resources.
- This is not time to introduce something complicated- don't use the access control requirement.
- How does this relates to currently existing to show where we are heading? We need to be clear that requirements will be changes, moved around, added as we add a full suite of standards.
- Unlike other attachments, this will be an addition separate from the standard.
- This connects the dots to work going on now to future proposals.
- Everyone now doing the high and that these things will get simpler?

- Assets under consideration will be expanded to apply security protection- but not as onerous as the current critical assets now.
- Assume 10% classified as critical. Applying all controls to that 10%. Other 90% have to do something, but it will be less.
- Is this a roadmap as to how to do nothing?
- Reservations- this looks like the medium and lows don't have to do much. Careful with chart.
- Problem is with the presentation- summary at beginning and format.
- 800-53 families- similar- something required if low moderate high. Others little required is a low.

4. Guidance Document

Phil Huff noted that the group had found a way to simplify and the revised draft represented a major shift in name of simplicity. The group understood that the reliability function impact married together in the "hook up table" is confusing. If the team doesn't understand, won't communicate well in the industry. The proposal is to use the reliability functions for determining your BES cyber systems. Then back to impact criteria for BES system. No mapping will be needed. Simplifies significantly and reduces complexity.

SDT Member comments

- Does this negate everything we have done? No, this is not a major shift- build on reliability functions.
- Single row look up table.
- Same scoping exercise- Take BES cyber systems only in look up table. We are here for BES.
- Starting either with cyber or BES subsystems is valid in scoping your cyber systems.
- Once you scope your cyber systems. You inherit the impact level of whatever the BES subsystem supporting happens to be.
- H/M/L- if you have a cyber system supporting BES subsystem- cyber subsystem inherits.
- An entity has to do both parts. Unless both parts are done won't be right. Who merges the two pieces. IT more capable of merging the two? Can't do one and make assumptions about the other.
- This is not a IT/engineering fight. Still have to look at reach of cyber system.
- Will this be doomed for failure? Assume IT reach of the system. Won't be Bulk Power people. They will make assumptions that will be wrong.

- Energy management system (e.g. servers, routers, firewalls), before that applications data, in terms of IT people- individual components. They identify all components. Need to go to applications and see what the functions are. We assess the impact of the functions. Then we map. We are done. Box now becomes the AGC mapping. Automatically rolls to the BES impact mapping. IT and Operations- automatically maps to the function. IT not making an objective judgment.
- The problem is we can't say how this all is going to work.
- I can give these criteria to our people and get the work done.
- Operations people in the field. What are the important things we have to do. Started with the applications. What do they talk with etc. They came up with where the data stored. Understood reach of critical reliability functions. You know the reach of the app and where the data is flowing to, you can determine criticality.
- We are here to do cyber security- not BES. What are we trying to secure?
- We need a matrix- BES and cyber piece. Started with functions. What does it take to do on cyber side. Take BES pieces.
- We are not throwing out matrix, rather we have reduced it to single row. If cyber subsystem has impact to the BES, this is based on the BES impact.
- Started with functions, applications.
- Start with the "terminals"- in the field-? Need the feeds from the field- need to turn on/ off.
- Understating the stuff out there? Looking at BES in very narrow areas. Control centers are easy.
- It is a 1 by 3. We need to simply the process
- 3 by 3. Why don't we need it anymore?
- Focus on what are you performing an impact assessment on? Cyber Impacts reliability functions. Criteria for reliability.
- Cyber asset that affects multiple functions.
- We are still trying to map to subsystems- will try to show this visually.
- If you start with BES items, you may not have to look at so many cyber assets.
- Data flow modeling? Need to use this as a tool to help with determining what is critical. Enterprise architecture modeling tools would have value. E.g. have a relay as a cyber device. Low medium high for that device. It's the BES thing that matters?
- Are we confusing connectivity and communication vs. the focus on the device?
- BES high-impact to BES reliability function. First identify the reliability functions.

- Have a list of cyber systems- this may be a big assumption that is not incorrect.
- The SDT should treat as an ongoing process which will be designed to reduce that gap as you go forward. It is a change management strategy.
- Is that path too risky?
- In terms of the 3-3 game. When you do it. Fill in with examples.
- How to tell the difference between the rows and the columns?
- Hypothetical- switchyard is a low medium high. Cyber assets within switchyard. L/M/H. High= loss or compromise would immediately cause. What is the function- of switch yard. 500 KV line. Operation of a single break?
- Look at high impacts to the BES function. Lost, compromised. What about connectivity?
- Is this dealt with by controls?
- If no on connectivity, makes it lower.
- E.g. two identical physical devices one is connected the other is not. Have a different cyber impact?
- Why are you dealing with physical?
- If not connected, are they out?
- Looking at cyber asset- what's the cyber impact of this connected relay. The one not connected fall off the list.
- Separating BES analysis and a cyber analysis-
- Cyber perspective the impact may be higher.
- Impact analysis is separate from the cyber assessment.
- Is cyber about connectivity? Wouldn't have physical requirements.
- Impact to a function- walk into yard.
- Game is not helping very much.
- Struggling with a way to explain to the industry to show how we fit together.
- If we can't express it. Modify.
- When I say connectivity, it is a difference- but it is discounted by others.
- Communication and impact- Sweitzer relay on a line without connectivity. I can trip that line. If the relay has connectivity- I could get to it and fake it out. Can factor into a bigger impact. Connectivity adds another/extra layers of potential impacts that has to be factored in.

- Relay engineers- "Aurora" thing- if you get into a relays set low or high. Micro processor. BES impact with a non processor.
- Withdrawn game. Raised point- 2 different interpretations about what impact is. Difference between impact and risk. "Impact assessment" has to include potential risk or not? Need to determine this.
- This is not designed to for physical security. Threat exists of a terrorist states controlling from a remote. Connectivity is the key /core to this threat.
- Appreciates connectivity- how do you define the cyber system? Framework was about systems in a management ways including interconnection component. Define the impacts to the function. Examine what risks are at play whether interconnected or not. Some protections are physical. Look at procedural controls. Impact assessment vs. risk analysis—
- Are we talking about "systems" in an appropriate way?
- Someone gets into cyber relay and changes setting, Control center would not know. Can happen on any device in that substation.
- We should consider the MRC (Jerry Cauley) results based performance methodology. Would be helpful to understand what he's looking for.
- The performance methodology has no official standing as yet. Won't have in front of Standards- committee or this team by the time we finish our work.

5. CIP 002-4 Revisions

John Lim and Phil Huff presented revisions to the CIP 002-4 strawman.

SDT Comments on CIP 002-4

- Removed "senior leadership"- not BES impact categorization issue.
- If standards not viewed as a complete set. Audits 1 at a time. Must have senior manager sign off.
- Senior manager sign off in every standard?
- Consider a standard that everyone complies with that deals with governance issue. Then move into technical controls. Clear focus on soft issues. XX vs. 002.
- This should be explained in the cover letter that the Team is soliciting comments on technical area, while organization of standards has yet to be determined.
- R2: each BES subsystem associated with. Take the system high. E.g. associated with 1 BES, same as today. If you have multiple, take the highest category of those.

- Sub-requirements? VRF issue made. Break out 1,2,3. These are listed. May be clearer to see.
- If sub requirements, must be clearly written for future audits. Numbers do each.
- R3 redone. Combined R4 with R3.
- R1.4.2 eliminate-
- R1. R2 talks about BES cyber system. "For each"- need to identify and list.
- R1- copy and place categorizing list.
- Have to keep in mind how NERC audits- reported on a requirement level not sub-requirement level.
- Take requirement numbers off- bullets or options?
- Have to be numbered apply the "following criteria," not requirements.
- Writing of violations based on how writing the VSL? No. Only looked at once violation confirmed, what is the sanction or penalty.
- Are these standards for compliance?
- If posting like this? Don't want to accept but have to. But it is wrong.
- Are these criteria? Go through each one to apply criteria applicable to them? That is the way it is written.
- Only Rs will be in front of major requirements. Not requirements but under numbered lists. A violation of one thing way down, is a violation of the requirement?
- Each of the sub-requirements become requirements?
- A true violation is you didn't do the mapping, vs. 1 of the 16 things.
- Double jeopardy- single instance leading to a violation of 2 requirements.
- This could be tighter with fewer words. Reduce to a phrase. Considerations that should go into analysis. If you don't consider, maybe should be dinged. This is how to set up mappings- these are filters not requirements.
- Need to map and follow through with the mapping- in Version 2- "and implement"
- R1- is requirement. Rest of list is numbered list containing criteria in order to do the mapping and assign levels.
- Audit question- and fine requirements.
- This has the applicability right in the front.
- New template? E.g. VRF and VSL at R. 1.1.1 and each one.
- Remove the R- and you are in violation-

- One option would be to make R1-"identify and categorize impact levels", apply criteria in an appendix to identify the impact levels. If in an appendix not mandatory.
- Does this leave us where we are now in terms of making up your own?
- Remove R1 as a statement and have instead an "Introduction."
- Intro paragraph are outside of a requirement. Template doesn't have a provision for introduction on a requirement lists.
- SDT needs to work within the boundaries.
- Make each sub/sub a requirement on its own? Each has to reference the requirement or category.
- Same amount of work you have to do.
- Need to level set – reframe the standards within the CIP structure. Look at this approach to categorization. Making everything a requirement? Have to do or deliver something. Requirement is to provide a process. Deliverable under R1- sub-requirements. If we do this, really a strange number of standards.
- Post something as a draft standard- or we post another concept paper that looks like a draft standard but doesn't meet the format. More important to get a revised concept out to industry?
- Conceptually how you do categorization, this is what you do with this when you get it done.
- Revised detailed concept that will lead to a standard. Make it an outline.
- Have to worry about these things as doing process. Going to miss if we don't.
- Support this approach.
- What of the discussion- BES subsystems not yet in?
- We will call this a working draft- post- of the mapping and categorization of BES cyber systems. Put something out that is close to a standard format. Putting out another concept paper won't generate industry comments and input.
- Put this out- this is as far as we could get. How does this help us look at this in the future?
- NERC format- we need editors in the room. We are guessing at what they want. Dave Taylor. Maureen need to be at our next meeting.
- Commitment to draft standards in December. Problems with putting out in this format. Not a bad thing. Makes more apparent problems with current template that NERC has. Hard to explain to outsiders if we are doing a "concept".
- The SDT needs to meet expectations for a standard. Don't call a concept, instead call it a preliminary draft.

- The SDT has to agree on the concept of what we want people doing. Need to make it through- get the flow right- worry about the formatting later. We don't yet have the flow.
- Walk through the process and see if there is consensus.
- Scoping BES cyber system can be done from either direction- should come up with the same cyber systems.
- R2- "as determined in R1
- R2- any BES cyber system associated with any BES subsystems. If you go back to definition, some things are not BES cyber systems (e.g. revenue metering device, thermal data logger in generation system). Ascertaining a BES cyber system. Be clear- rewrite R1 as R2.
- Say it all over again just to be clear?
- Good with BES cyber system. But problems with Cyber system: "disposition of information"?
- Requirement – identify all your BES cyber system.
- We need to go through this from top to bottom.
- Use the tables as a starting point.
- Maureen Long and Joel De Jesus from NERC can help the SDT.
- NERC is trying to minimize the use of sub-requirements.
- Requirement a separate piece of work with some reliability benefit by itself. Removed R from sub requirements. Refer to as parts. If subject to liability itself.
- If a sub-requirement is embedded within a requirement- it will be treated and audits as a violation.

6. Summary of Discussion Points with NERC Staff

NERC Staff (Maureen Long, Dave Taylor and Joel De Jesus) joined the SDT on Thursday morning and offered the following guidance to the SDT:

1. Define in the Glossary: High Impact; Medium Impact; and Low Impact.
2. Remove the sub/sub requirements (R1.1.1., R1.1.2., R1.2.3, R1.2.4. etc.) from the draft standard and put them into a separate numbered list attachment document.
3. State in the attachment document that the Responsible Entity (TO, GO, BA, etc) has to comply with only the applicable items, i.e., TO does not have to include generation if it does not apply. They did not think this distinction of what items applied to TO or GO only was clear using the currently proposed draft standard format which was displayed on the Webex they were looking at.
4. Add to the main requirement what the impact is to reliability. Maureen stated that under

the new NERC template each requirement is to include how it contributes to reliability.

5. Use the existing latitude available in establishing violation severity levels (VSL's). Consider using percentages ,i.e.:
   - (Entity missed either <10% of items (or perhaps 4 items) = low,
   - Entity missed >10% but < 25% = Medium, etc.)
6. If the proposed standard remains in the format that is current proposed, as shown on the Webex, then any missed item will result in a finding of non-compliance by the auditor. As an example of how severe this could be, in the current draft standard format, auditing of a TO entity who did not have generation listed in their R1 analysis would result in a finding of non-compliance sent to compliance staff for further investigation.

V. NEXT STEPS

The SDT Chair and Vice Chairs reviewed with the Team the updated agreed upon schedule for both the CSO 706 SDT Version 3 CIP and the Version 4 CIP 002 Process as follows:

CIP Version 3 Key Steps/Schedule

1. *Post for Industry Comment 10-13-09 to 11-12-09*
2. **November 13 SDT Conference Call- Review of Industry Comments and Response**
3. **November 16, CSO 706 SDT Meeting in Orlando, Monday, 5:00 p.m.- through dinner- Response Document to Industry Comments**
4. **November 17**, Tuesday, CSO 706 SDT Meeting, Orlando, Complete and Adopt Response Document to Industry Comments
5. **November 20**, Wednesday, Post Response Document and Initiate Ballot
6. **November 30**, Monday *(after Thanksgiving)* Deadline for Votes and Industry Comments
7. **December 2, Wednesday, CSO 706 SDT - Conference Call- finalize Response document to Industry Comments**
8. **December 3- 13,** Recirculation Ballot
9. **December 16,** BoT Approval
10. **December 29, 2009,** FERC Filing

CIP 002-4 Key Steps/Schedule (October-December 2009)

1. **November 1:** Jackie Collett, Phil Huff, John Lim and John Varnell, the chairs of the 4 CIP 002 Subgroups will form the CIP 002 Strawman Drafting Group (SDG).
2. **November 1:** All CIP 002 "meta groups" and subgroups will forward to the Strawman Drafting Group their standards text drafts including any guidance language**.**
3. Joe Doetzl will coordinate the work of the Controls Drafting Group (CDG) members: Jim Brenton, Keith Stouffer, Bill Winters, Jon Stanford. They will produce several recommended sample controls to illustrate high/medium/low concepts in CIP 002 as well as recommendations on whether the SDT should request guidance from the

Standards Committee on referencing a 'catalogue of security requirements', for circulation to the SDT **by Friday, November 13, 2009**

4. The SDG will prepare a strawman draft by **November 13, 2009** for review by the SDT in advance of November 16-19, 2009 SDT meeting
5. The SDT will utilize the strawman draft to organize its **November 16-19 meeting** and determine at the conclusion of the meeting if the SDT will continue to aim for the December 16th adoption of CIP 002 draft for posting for industry comment
6. **December 7, 3:00-4:30 p.m. est**. Previews of reviewed CIP 002 and related document drafts at a SDT conference call.
7. The SDT will refine and circulate a revised strawman Draft by Monday, December 14, 2009 for review at the **December 15-16** CSO706 SDT meeting in Little Rock
8. **December 15-16** will refine, finalize and adopt draft CIP 002-4 for posting to the industry for informal comments.

Keith Stouffer mentioned that in terms of the table format the next big step to develop the information paragraph at the outset of each of the tables. Phil Huff noted that the guidance document would be developed further and circulated to the SDT in advance of the Little Rock meeting. The Chair noted she would circulate a draft of the "comment form" and cover letter. Jackie Collett asked for time on the Little Rock agenda to go through a "walk through" of the CIP 002-4. She agreed to work with several SDT members to prepare materials for the walk through.

The Chair reviewed the next steps including the schedule for the Version 3 response document and the CIP 002-4 effort. She thanked Rich Kinas for hosting the meeting and providing excellent food and facilities.

The SDT adjourned at 2:45 p.m. on November 19, 2009.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Appendix # 1— Meeting Agenda

NERC SDT Order 706 November 16-19, 2009 Meeting Agenda Packet

Project 2008-06 Cyber Security Order 706 SDT
Draft 16th Meeting Agenda
November 16, 2009, Monday - 5 PM to 9 PM EST
November 17, 2009, Tuesday - 8 AM to 5 PM EST
November 18, 2009, Wednesday - 8 AM to 5 PM EST
November 19, 2009, Thursday - 8 AM to 3 PM EST
Orlando Utilities Commission, 6003 Pershing Ave.
Orlando, Florida 32822

NOTE:
1. Agenda Times May be Adjusted as Needed during the Meeting
2. Drafting Group Meetings May Not Have Access to Telephones and

Proposed Meeting Objectives/Outcomes

- Welcome new members and outline SDT leadership transition
- Review, Discuss and Adopt SDT Response Document to Industry Comments on CIP Version 3
- Review the CIP 002-4 and CIP 002-009-4 workplan going forward
- Receive updates on TFE, VSL/VRF and related cyber security efforts
- Review CIP 002-4 Key Issues and Provide Guidance to Documents Drafting Groups
- Convene CIP 002-4 Document Drafting Groups
- Review and refine a draft CIP 002-4 strawman and related documents
- Agree on next steps and assignments

Draft Agenda

Monday November 16, 2009

5:00 p.m. &	Welcome and Opening Remarks and Review of Evening Agenda- *Jeri Domingo-Brewer* *Phil Huff* Roll Call; NERC Antitrust Compliance Guidelines
5:10	Overview of FERC Order on CIP Version 2 and Version 3 Procedural Steps - *Scott Mix*
5:15	Consideration of Full Group/Small Group Format for Response Document Review--*Jeri Domingo-Brewer*
5:20	Review of Strawman SDT Industry Response Document on FERC Order, CIP Version 3
7:00	*Working Dinner*

7:30 Continue Review of Strawman SDT Industry Response Document on FERC Order, CIP Version 3
9:00 *Recess*

Tuesday November 17, 2009

8:00 a.m. Welcome and Opening Remarks- *Jeri Domingo-Brewer & Phil Huff*
Roll Call; NERC Antitrust Compliance Guidelines
Facilitator review and SDT acceptance of October 20-22 Kansas City SDT meeting summary
8:20 Review of Meeting Objectives, Agenda and Meeting Guidelines- *Bob Jones*
8:25 Welcome and SDT Leadership Transition- *Jeri Domingo-Brewer & Phil Huff*
8:30 Current Membership Changes and Call for New Members - *Jeri Domingo-Brewer & Phil Huff*
8:35 Review of SDT 706 Workplan Decisions in October, 2009 and Feedback from NERC
9:00 Update on Technical Feasibility Exception (TFE) NERC Rules of Procedure –*Scott Mix*
9:05 Update on VSLs/VRFs- *Scott Mix*
9:10 Update on other related cyber security initiatives- *SDT Members*
9:15 Review and Refinement of CIP Version 3 Strawman Response Document
10:00 *Break*
10:15 Review and Refinement of CIP Version 3 Strawman Response Document
12:00 Motion to Adopt the SDT 706 CIP Version 3 Response Document *(when ready).*
12:30 *Lunch*
1:30 Overview of CIP 002-4 and CIP 002-009-4 Workplan - *Stu Langton*
1:40 Overview of list of CIP 002-4 Documents for posting in December.
1:45 Overview of CIP 002-4 Strawman Draft Documents, Format and Key Remaining Issues and
Challenges- *John Lim et al. (e.g. Defining BES Subsystems; Descriptions of reliability functions; 2-3 examples of controls; and categorization of cyber systems in guidance documents).*
3:30 *Break*
3:45 Review and Refinement of CIP 002-4 Key Remaining Issues and Guidance for Drafting Groups
5:15 Organizing SDT Document Drafting Groups for Wednesday
5:30 *Recess*

Wednesday November 18, 2009

8:00 Welcome and Agenda Review- *Jeri Domingo-Brewer & Phil Huff*
8:10 Review of Key Remaining Issues and Challenges and Guidance to Drafting Groups
8:30 Convene SDT CIP 002-4 Document Drafting Groups
12:00 *Working Lunch*
12:45 CIP 002-4 Document Drafting Group Reports and Additional SDT Guidance
3:00 *Break*

3:15	Reconvene SDT CIP 002-4 Document Drafting Groups
5:30	*Recess*

Thursday November 19, 2009

8:00	Welcome and Agenda Review- *Jeri Domingo-Brewer & Phil Huff*
8:15	Review and Refinement and Consensus Testing of CIP 002-4 Strawman Documents from Drafting Groups
10:00	*Break*
10:15	Review and Refinement and Consensus Testing of CIP 002-4 Strawman Documents from Drafting Groups
12:15	*Working Lunch*
1:00	Review and Refinement and Consensus Testing of CIP 002-4 Strawman Documents from Drafting Groups
2:45	Review and Agree on CIP 002-4 Next Steps for SDT Drafting Group(s) Meeting Evaluation
3:00	*Adjourn*

Appendix # 2 Attendees List
November 16-19, 2009 Orlando, Florida

Attending in Person — SDT Members and Staff

1. Rob Antonishen	Ontario Power Generation (Friday)
2. Jeri Domingo-Brewer, Chr.	U.S. Bureau of Reclamation
3. Jackie Collett	Manitoba Hydro
4. Sharon Edwards	Duke Energy
5. Gerald S. Freese	Director, Enterprise Info. Security America Electric Pwr.
6. Phillip Huff	Arkansas Electric Coop Corporation
7. Doug Johnson	Exelon Corporation - Commonwealth Edison
8. Frank Kim	Ontario Hydro *(Mon. & Tuesday)*
9. Rich Kinas	Orlando Utilities Commission
10.John Lim	CISSP, Department Manager, Consolidated Edison Co. NY
11. David Norton	Entergy
12. Scott Rosenberger	Luminant Energy
13. David S. Revill	Georgia Transmission Corporation
14.Keith Stouffer	National Institute of Standards & Technology
15. John D. Varnell	Technology Director, Tenaska Power Services Co.
16. William Winters	Arizona Public Service, Inc. (Mon., Tues, Thurs)
1. Scott Mix	*NERC*
2. Joe Bucciero	*NERC/Bucciero Assoc.*
3.Hal Beardall	*FSU/FCRC*
4. Robert Jones	*FSU/FCRC Consensus Center*
5. Stuart Langton	*FSU/FCRC Consensus Center*

SDT Members Attending via WebEx and Phone

17. Jim Breton	ERCOT
18. Jonathan Stanford	Bonneville Power Administration
19. Kevin Sherlin	Sacramento Municipal Utility District (Mon., Tues, Wed)
Maureen Long,	NERC (Thurs)

SDT Members Unable to Attend

Jay S. Cribb	Information Security Analyst, Southern Company Services
Joe Doetzl	Manager, Information Security, Kansas City Pwr. & Light Co.
Christopher A. Peters	ICF International

Others Attending in Person

Bill Glynn	Westar Energy
Rick Terrell	Luminant
Chris Wright	Burns and MacDonald Engineering

Others Attending via WebEx and Phone

Rob Hardiman	Southern Company Transmission (10-20, 21, 22)
David Huff	FERC (10-20, 22)_
Justin Kelly	FERC 10-21, 22)
Hoang Neg	RRI Energy (10-20_
Jon Stitzel	Burns and MacDonald Engineering

Appendix # 3 Meeting Evaluation Summary

CYBER SECURITY ORDER 706 SDT
NOVEMBER 16-19, 2009, ORLANDO, FLORIDA
MEETING EVALUATION SUMMARY

Members used the following 0 to 10 scale in evaluating the meeting: 0= totally disagree and 10= totally agree. The results below represent the average rankings and include 12 SDT member evaluations.

1. Please assess the overall meeting.

7.27 The agenda packet was very useful.
7.75 The Webex document display and the audio were effective
8.90 The quality of the meeting facility was good.
7.45 The objectives for the meeting were stated at the outset.
7.20 Overall, the objectives of the meeting were fully achieved.

Were each of the following meeting objectives fully achieved:
9.18 Welcome new members and outline SDT leadership transition
9.36 Review, Discuss and Adopt SDT Response Document to Industry Comments on CIP Version 3
6.73 Review the CIP 002-4 and CIP 002-009-4 workplan going forward
7.73 Receive updates on TFE, VSL/VRF and related cyber security efforts
6.91 Review CIP 002-4 Key Issues and Provide Guidance to Documents Drafting Groups
7.50 Convene CIP 002-4 Document Drafting Groups
6.55 Review and refine a draft CIP 002-4 strawman and related documents
7.00 Agree on next steps and assignments

2. Please tell us how well you believe the Team engaged in the meeting.
7.09 The Chair and Vice Chair provided leadership and direction to Team and Facilitators
8.82 The Facilitators made sure the concerns of all members were heard.
8.82 The Facilitators made sure the concerns of all participants were heard.
7.36 The Facilitators helped clarify and summarize issues.
7.18 The Facilitators helped members build consensus.
7.18 The Facilitators helped us arrange our time well.

3. What is your level of satisfaction with what was achieved at the meeting?

6.82 Overall, I am very satisfied with the results of the meeting.
7.45 Overall, the design of the meeting agenda was effective.
7.73 I was very satisfied with the services provided by the Facilitators.
6.60 I am satisfied with the outcome of the meeting.
6.18 I am satisfied with the progress we are making as a Team.
7.09 I know what the next steps following this meeting will be.

7.18 I know who is responsible for the next steps.

4. Other comments

What did we achieve?

- Version 3 ready for posting.
- CIP002 now makes sense but more work is needed on the format.
- Comments were answered and package proposed.
- The NIST only people still don't understand about penalty's.

What are our biggest challenges going forward?

- Wasting time. The call with NERC leadership should have included the whole team. We ended up spending up extra time going over what was said and the team didn't get first hand information.
- Clean direction on CIP002.
- Format 002 so that our intent is followed.
- Develop and publish corresponding counts for high, medium and low.
- Separation of team lead and others.

What suggestions do you have for making our group more productive?

- More rigid structure. Make sure concepts are understood. Use parking lot.
- Greater use of small groups.
- The group as a whole is too large to make progress.
- Too much time is devoted in the large group to discussion and too little time to actual progress.
- Have meeting at an airport hotel only!!! That is a HUB DFW, Saint Louis, Chicago (Mid. States).

Appendix # 4 — NERC Antitrust Compliance Guidelines

I. General

It is NERC's policy and practice to obey the antitrust laws and to avoid all conduct that unreasonably restrains competition. This policy requires the avoidance of any conduct that violates, or that might appear to violate, the antitrust laws. Among other things, the antitrust laws forbid any agreement between or among competitors regarding prices, availability of service, product design, terms of sale, division of markets, allocation of customers or any other activity that unreasonably restrains competition.

It is the responsibility of every NERC participant and employee who may in any way affect NERC's compliance with the antitrust laws to carry out this commitment.

Antitrust laws are complex and subject to court interpretation that can vary over time and from one court to another. The purpose of these guidelines is to alert NERC participants and employees to potential antitrust problems and to set forth policies to be followed with respect to activities that may involve antitrust considerations. In some instances, the NERC policy contained in these guidelines is stricter than the applicable antitrust laws. Any NERC participant or employee who is uncertain about the legal ramifications of a particular course of conduct or who has doubts or concerns about whether NERC's antitrust compliance policy is implicated in any situation should consult NERC's General Counsel immediately.

II. Prohibited Activities

Participants in NERC activities (including those of its committees and Subroups) should refrain from the following when acting in their capacity as participants in NERC activities (e.g., at NERC meetings, conference calls and in informal discussions):

- Discussions involving pricing information, especially margin (profit) and internal cost
- information and participants' expectations as to their future prices or internal costs.
- Discussions of a participant's marketing strategies.
- Discussions regarding how customers and geographical areas are to be divided among competitors.
- Discussions concerning the exclusion of competitors from markets.
- Discussions concerning boycotting or group refusals to deal with competitors, vendors or suppliers.

III. Activities That Are Permitted

From time to time decisions or actions of NERC (including those of its committees and Subroups) may have a negative impact on particular entities and thus in that sense adversely impact competition. Decisions and actions by NERC (including its committees and Subroups) should only be undertaken for the purpose of promoting and maintaining the reliability and adequacy of the bulk power system. If you do not have a legitimate purpose consistent with this objective for discussing a matter, please refrain from discussing the matter during NERC meetings and in other NERC-related communications.

You should also ensure that NERC procedures, including those set forth in NERC's Certificate of Incorporation and Bylaws are followed in conducting NERC business. Other NERC procedures that may be applicable to a particular NERC activity include the following:

- Reliability Standards Process Manual
- Organization and Procedures Manual for the NERC Standing Committees
- System Operator Certification Program

In addition, all discussions in NERC meetings and other NERC-related communications should be within the scope of the mandate for or assignment to the particular NERC committee or Subroup, as well as within the scope of the published agenda for the meeting.

No decisions should be made nor any actions taken in NERC activities for the purpose of giving an industry participant or group of participants a competitive advantage over other participants. In particular, decisions with respect to setting, revising, or assessing compliance with NERC reliability standards should not be influenced by anti-competitive motivations.

Subject to the foregoing restrictions, participants in NERC activities may discuss:

- Reliability matters relating to the bulk power system, including operation and planning matters such as establishing or revising reliability standards, special operating procedures, operating transfer capabilities, and plans for new facilities.
- Matters relating to the impact of reliability standards for the bulk power system on
- electricity markets, and the impact of electricity market operations on the reliability of the bulk power system.
- Proposed filings or other communications with state or federal regulatory authorities or other governmental entities.
- Matters relating to the internal governance, management and operation of NERC, such as nominations for vacant committee positions, budgeting and assessments, and
- employment matters; and procedural matters such as planning and scheduling meetings.

Any other matters that do not clearly fall within these guidelines should be reviewed with NERC's General Counsel before being discussed.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

APPENDIX # 5 CSO 706 SDT Meeting Schedule

CSO 706 SDT MEETING SCHEDULE
OCTOBER 2008–DECEMBER 2010

DEVELOPMENT OF CIP VERSION 2 AND NEW VERSION FRAMEWORK
OCTOBER 2008–JULY 2009

1. October 6–7, 2008 — Gaithersburg, MD Reviewed CIP-002-CIP-009, Agreed on Version 2 approach.
2. October 20–21 —Sacramento, CA CIP-002-CIP-009 Version 2 development
3. November 12–14, 2008 — Little Rock, AR CIP-002-CIP-009 Version 2 adoption for comment and balloting; CIP-002-CIP-009 New Version process reviewed.
4. December 4–5, 2008 — Washington D.C. CIP-002-CIP-009 Version 3 reviewed and debated, SDT member white "working" papers assigned, Technical Feasibility Exceptions white paper reviewed and refined.
5. January 7–9 — Phoenix, AZ, Reviewed Technical Feasibility Exceptions white paper**,** reviewed industry comments on CIP-002-CIP-009 Version 2 products — established small groups to draft responses, reviewed New Version white "working" papers.
January 15 — WebEx meeting(s) Small group drafted responses to industry Version 2 comments.
January 21 — WebEx meeting(s) Small group drafted responses to industry Version 2 comments.
6. February 2–4, 2009 — Phoenix, AZ Update on NERC Technical Feasibility Exceptions process**,** VSL process and SDT role**,** review of Version 3 White papers, strawman and principles**,** reviewed and adopted SDT responses to industry comments on Version 2 and Version 2 Product Revisions.
7. February 18–19, 2009 — Fairfax, VA Update on Version 2 process**,** NERC TFE process and VSL Team process; reviewed, discussed and refined Version 3 CIP-002 White papers, strawman, and principles.
8. March 10–11, 2009 — Orlando, FL Update on NERC TFE and VSL and VRF Team process and review and refine Version 3 CIP-002 Strawman Proposals
March 2–April 1, 2009 — 30-day Pre Ballot
Mid-March — NERC posts TFE draft Rules of Procedure for industry comment
March 30, 2009 — WebEx meeting(s) White Paper Drafting Team
April 1–10 — NERC Balloting on Version 2 Products
April 6, 2009 — WebEx meeting — White Paper Drafting Team
April 8, 2009 — WebEx meeting(s) — White Paper Preview- Full SDT Conference Call
April 11, 2009 — Version 2 Ballot Results (Quorum: 91.90% Approval: 84.06%) and Industry Comments
9. April 14–16, 2009 — Charlotte NC Update on NERC TFE process, VSL Team process and NERC Critical Assets Survey; agreed and adopted responses for Version 2 industry comments for recirculation ballot; reviewed and refined Version 3 whitepaper and consensus points and progress report to NERC Member Representative Committee (MRC) May meeting.
April 28 and May 6, 2009 — White Paper Drafting Team Meetings and WebEx
April 17–27, 2009 — Recirculation Results: Quorum: 94.37% Approval: 88.32%
May 5, 2009 — NERC MRC Meeting, Arlington, VA- SDT progress report.
10. May 13–14, 2009 — Boulder City NV Reviewed MRC presentation and further SDT refinement and discussion of the Version 3 White Paper.
June 8 and June 15, 2009 — Working Paper Drafting Team Meetings and WebEx

11. June 17–18, 2009 — Portland OR Further SDT refinement of the draft CIP Version 3 Working Paper(s), reviewed SDT development process for June-December 2009; discussed potential SDT subcommittee structure and deliverables.

- *June — WebEx meeting(s)*
- *Working Paper drafting group sessions including inputs from selected industry personnel to help establish BES categorization criteria*

CIP-002 DEVELOPMENT OF REQUIREMENTS, MEASURES, ETC. JULY-DECEMBER 2009

12. July 13–14, 2009 in Vancouver, B.C., Canada
SDT reviewed, refined, and adopted SDT Working Paper. SDT adopted its response to NERC for Interpretation of CIP-006-1. SDT reviewed and adopted a proposal for CIP-002 Subgroups and Deliverables and convened subgroup organizational meetings to develop work plans. SDT adopted 2010 Meeting Schedule.

- *July–August Interim Conference call meeting(s)*
- *CIP-002 Subgroup meetings*
- *CIP-002 Coordination Team meeting*
- *August 3–5, 2009 in Winnipeg, Manitoba **NERC Member Representative Committee**. Progress Report and presentation on new CIP Version 3 Working Paper-Concept- Reliability Standards on Cyber Security for MRC input.*

13. August 20–21, 2009 in Charlotte, NC. SDT reviewed and responded to MRC input on Working Paper/CIP-002 Concepts and convened SDT Subgroup and plenary meetings to develop CIP-002 requirements and "proof of concept" control (s).

- *July–September — 45-day Industry Comment Period on CIP-002 Concept Working Paper*
- *NERC Webinar- August–September Interim Conference Call meeting(s)*
- *CIP-002 Subgroup meetings (as ne*
- *CIP-002 Coordination Team meeting*

14. September 9–10, 2009 in Folsom, CA. SDT reviewed and considered industry comments on the Working Paper and CIP-002 concepts and their application to the subgroup work and addressed coordinating issues through joint subgroup meetings. SDT agreed on meeting dates and proposed locations for January–December 2010
September–October Interim WebEx meeting(s)

- *FERC Version 3 Urgent Action SDT conference call meetings*
- *CIP-002 Coordination Team meeting*

CIP VERSION 3 RESPONSE TO FERC ORDER, OCTOBER-DECEMBER, 2009

15. October 20–22, 2009 in Kansas City, MI. Reviewed new FERC Order and urgent action CIP Version 3 process; discussed key issues raised by SDT CIP 002 Subgroups, small group meetings and agreement on refinements to the CIP 002-009 schedule and drafting process for CIP 002-4.

- *October–November Drafting Team meeting(s)*
- *CIP-002 Coordination Team meeting*

16. November 16–19, 2009 in Orlando, FL

- SDT review, refine and adopt Version 3 "industry response" document.
- SDT plenary and drafting group session(s) — to draft, review and refine CIP-002-4 standard, requirements, measures and controls and related documents.
- November–December Interim Conference call meeting(s)

- Drafting teams as needed to finalize draft CIP 002-4 documents
- CIP-002 Coordination Team meeting
- *CIP 002-4 Drafting Team produces next draft based on Orlando Meeting input.*
- *December 2 CSO 706 SDT Version 3 Consideration of Comments Draft Conference Call*
- *December X, CSO 706 SDT CIP 002-4 Preview Conference Call*

17. December 15–16, 2009 in Little Rock AK

- SDT scenario "walk through" to test flow of CIP 002-4.
- SDT plenary and drafting group session(s) to review, refine, and agree on and adopt CIP-002 standard, requirements, measures and controls and related documents.
- Agree on initial posting of draft CIP-002 for industry review and comment.
- Agree on next steps and 2010 Workplan and schedule

REFINEMENT AND ADOPTION OF CIP-002 VERSION 4 AND DEVELOPMENT AND ADOPTION OF CIP STANDARDS (003-009)
JANUARY 2010–DECEMBER 2010

18. January 19-20–21-22 — Tue-PM- to Friday AM, Tucker, GA (GTC)

- SDT Work on Developing CIP 003-009 Strawman Drafts

19. February 17-18–19 —Wed--Thursday –Friday, Austin TX (ERCOT)

- SDT Reviews Industry Comments and Refines CIP 002 for posting for 45-day industry formal comment period.
- SDT continues CIP 003-009 Strawman Drafts

20. March 9–10-11 — Tuesday–Thursday, Phoenix, AZ (APS)

- SDT continues CIP 003-009 Strawman Drafts

21. April 13-14–15 — Tue-Wednesday–Thursday, Atlanta GA (Southern Co)

- SDT Reviews and Responds to Industry Comments, Refines and Adopts CIP 002 for balloting
- SDT posts a draft CIP 003-009 for informal industry comment.

22. May 11-12–13 — Tue-Wednesday–Thursday, Dallas TX (Luminant)

- SDT reviews Industry 1st Ballot Comments and Drafts Responses
- SDT reviews CIP 003-009 informal industry comments and refines the draft.

23. June 8-10- Tues, Wed. Thursday- (Sacramento)

- SDT refines CIP 003-009 and posts for 2nd round of informal industry comments and refines the draft.

24. July 13-14–15, Tue-Wednesday–Thursday, Pittsburgh, PA (CERT)

- SDT reviews CIP 003-009 informal industry comments and refines the draft.

25. August 10-11–12, Tue-Wednesday–Thursday- TBD

- SDT refines CIP 003-009 and posts for formal 45 day industry comment

26. September 7,8,9, Tues-Thurs. TBD (if needed)

27. Oct. 12-13–14, Tue-Wednesday–Thursday- TBD

- SDT Reviews and Responds to Industry Comments, Refines and Adopts CIP 002 for balloting

28. November 16-17–18, Tue-Wednesday–Thursday- TBD

- SDT reviews Industry 1st Ballot Comments and Drafts Responses

29. December 14-15–16, Tue-Wednesday–Thursday- TBD

Appendix # 6 Prioritizing Streamlining Options

CONSIDERING STRATEGIES FOR STREAMLINING THE SDT 706 WORKPLAN MEMBER SURVEY FORM RESULTS-PRIORITY RANKING

(15 SDT Respondents: Jeri Brewer, Jim Brenton, Jackie Collett, Sharon Edwards, Phil Huff, Doug Johnson, Rich Kinas, John Lim, Dave Norton, Dave Revill, Scott Rosenberger, Jon Stanford, Keith Stouffer, John Varnell & Bill Winters)

SDT Members "brainstormed" SDT streamlining ideas on 11-17-09 and completed this survey during lunch on 11-19-09 using the following scale in ranking the strategies:

5= highest priority/most helpful; 4= priority/helpful; 3= important/somewhat helpful; 2= less important and helpful; 1=don't do it-unacceptable.

SURVEY CATEGORIES

A. CHANGING ANSI STANDARDS PROCEDURES
B. MEETING CHANGES- EFFICIENCY, LOCATION, TOOLS
C. COMMITMENT, COMMUNICATION AND SUPPORT
D. TEAM STRUCTURE
E. SUBSTANTIVE CHANGES IN APPROACH/SCOPE TO STANDARD DEVELOPMENT
F. MORE TALENT AND EXPERTISE TO SUPPORT SDT

1.	**(4.46)**	**Technical writer support (more writers like Scott Mix)** *(NERC)* *(***11-*5's & 4's and* 2 *-1's & 2's)*
2.	**(4.43)**	**Improve industry communications in getting the word out on the SDT and its progress? Webinars, workshops, etc.** *(NERC in Coordination with SDT)* *(***11-*5's & 4's and* 0 *-1's & 2's)*
3.	**(4.36)**	**Make the best use of our time. Start meetings on time and get the technology operational early** *(SDT)* *(***8-*5's & 4's and* 0 *-1's & 2's)*
4.	**(4.21)**	**Receive permission to use informal comment processes for the development of the CIP with a final 45-day comment period consistent with the ANSI process.** *(NERC)* *(***7-*5's & 4's and* 1 *-1's & 2's)*
5.	**(4.00)**	**Engage technical writers** *(NERC)* *(***8-*5's & 4's and* 3 *-1's & 2's)*
6.	(3.93)	Meet in central US locations minimizing travel time and maximizing Team productivity and time. *(SDT and NERC)* *(***5-*5's & 4's and* **1** *-1's & 2's)*
7.	(3.86)	No audits for drafting team member organizations *(NERC).* *(***8-*5's & 4's and* **2** *-1's & 2's)*
8.	(3.62)	Refocus on security issues and less on compliance *(SDT)* *(***8-*5's & 4's and* **3** *-1's & 2's)*
9.	(3.54)	Breakup the SDT into many small drafting groups--divide the work and focus on specific tasks. *(SDT)* *(***7-*5's & 4's and* **3** *-1's & 2's)*
10.	(3.54)	Remove penalty base requirements (you get what you measure) *(NERC, FERC, Congress)* *(***6-*5's & 4's and* **4** *-1's & 2's)*
11.	(3.46)	Simplify the approach and strategy to the standards to reduce complexity *(SDT)* *(***7-*5's & 4's and* **3** *-1's & 2's)*
12.	(3.38)	NERC support funding member expenses (1/2 of costs) for meetings. *(NERC)* *(***5-*5's & 4's and* **5** *-1's & 2's)*
13.	(3.36)	Longer, extended intensive meetings of the SDT (2-3 weeks at a time) *(SDT and NERC)* *(***8-*5's & 4's and* **7**-*1's & 2's)*
14.	(3.29)	Charge the SDT to complete CIP by April 1, 2010 – working outside the constraints of the current ANSI process. *(NERC)* *(***5-*5's & 4's and* **4** *-1's & 2's)*
15.	(3.15)	NERC letter to CEOs acknowledging the contributions of members and appreciation of work done so far (as requested by members) *(NERC)* *(***6-*5's & 4's and* **5**-*1's & 2's)*
16.	(3.15)	Station engineers *(NERC)* *(***6-*5's & 4's and* **6**-*1's & 2's)*
17.	(3.15)	Bring generating station engineers onto the SDT. *(NERC)* *(***4-*5's & 4's and* **5** *-1's & 2's)*
18.	(3.08)	Establish a small core SDT drafting group that will commit to meeting frequently between SDT meetings to prepare materials and drafts for full group consideration at meetings. *(SDT)* *(***5-*5's & 4's and* **7** *-1's & 2's)*
19.	(3.08)	Divide the standards deliverables and organize the SDT to develop drafts for each. *(SDT)* *(***5-*5's & 4's and* **5** *-1's & 2's)*

20. (3.08) Adapt 800-82 (targeted for industrial control systems) *(NERC & SDT)* *(***7***-5's & 4's and* **3** *-1's & 2's)*
21. (3.08) Legal support for the SDT *(NERC)* *(***4***-5's & 4's and* **6** *-1's & 2's)*
22. (3.07) Establish idea sharing center on the NERC Website *(NERC)* *(***4***-5's & 4's and* **7** *-1's & 2's)*
23. (2.93) Revise the work plan to produce interim CIP deliverables prior to the final CIP deliverable that can be implemented more rapidly with less onerous comment response process required. *(NERC and SDT)* *(***1***-5's & 4's and* **2** *-1's & 2's)*
24. (2.92) Full Commitment and support of members from their organizations extending down to include managers and lower level executives, not just pay lip service. *(SDT Members)* *(***2***-5's & 4's and* **7***-1's & 2's)*
24. (2.92) Adopt 800-53 Rev 3 for control centers and data centers *(NERC & SDT)* *(***4***-5's & 4's and* **6** *-1's & 2's)*
25. (2.92) Review Order 706 and remove items included that should be given to another group, challenged or deferred. *(NERC & SDT)* *(***7***-5's & 4's and* **1** *-1's & 2's*
26. (2.86) Bring Team together for as long as it takes to get the job done (somewhere nice) *(SDT and NERC)* *(***4***-5's & 4's and* **6***-1's & 2's*
27. (2.85) Support outside expert presentations on security issues and standards in other industries. *(NERC)* *(***3***-5's & 4's and* **5***-1's & 2's)*
28. (2.79) Support the use of video technology for SDT meetings(e.g., Cisco Telepresence) *(NERC)* *(***4***-5's & 4's and* **5** *-1's & 2's)*
29. (2.50) NERC letters to CEO's to secure full commitments from CEOs of member organizations. *(NERC)* *(***2***-5's & 4's and* **6***-1's & 2's*
30. *(2.50)* Leverage FERC Power (influence) for immediate needs *(NERC)* *(***2***-5's & 4's and* **8***-1's & 2's)*
31. (2.46) Throw in with CSCTG from NIST *(NERC)* *(***2***-5's & 4's and* **8***-1's & 2's)*
32. (2.38) Go back to the 'original, original' standards for cyber security as a basis for the new CIP (see NERC Website archive) *(SDT)* *(***2***-5's & 4's and* **7***-1's & 2's)*
33. *(*2.36) Open up the discussions beyond our electric industry *(NERC)* *(***1***-5's & 4's and* **10***-1's & 2's)*
34. (2.08) Skip BES Mapping and install minimum security controls for all assets after establishing clear cut agreed upon objectives on what we are securing. *(SDT)* *(***2***-5's & 4's and* **10** *-1's & 2's)*
35. (1.85) Abandon the NIST based approach and improve existing standards framework. *(SDT)* *(***0***-5's & 4's and]* **13***-1's & 2's)*

List any other strategies or comments:

NERC Team Support and Expertise

- NERC establish a location for meetings with all the needed support and technology.
- Compliance input during team meetings.
- NERC Standards Development process resource to provide guidance on process questions.
- NERC provide someone to create and organize webinars.

Outside Pressure and Changes in Workplan Objectives

- Consistent objectives; less reactionary pressure from NERC and FERC on schedule.

Communication with Industry

- Communications plan needs to be a priority with NERC.

Team Structure

- All open meeting!!! Not lead team communicating with others.
- Small group meet for a longer separate session to produce strawman specific documents created for use at larger group meetings.
- I think greater use of small groups for creation of a strawdog to be brought back to the group for adoption would be a model for everyone.

CONSIDERING STRATEGIES FOR STREAMLINING THE SDT 706 WORK-PLAN MEMBER SURVEY RESPONSES BY CATEGORY (11-19-09)

(15 SDT Respondents: Jeri Brewer, Jim Brenton, Jackie Collett, Sharon Edwards, Phil Huff, Doug Johnson, Rich Kinas, John Lim, Dave Norton, Dave Revill, Scott Rosenberger, Jon Stanford, Keith Stoffer, John Varnell & Bill Winters)

SDT Members "brainstormed" SDT streamlining ideas on 11-17-09 and completed this survey during lunch on 11-19-09 using the following scale in ranking the strategies:
5= highest priority/most helpful; 4= priority/helpful; 3= important/somewhat helpful;
2= less important and helpful; 1=don't do it-unacceptable.

A. CHANGING ANSI STANDARDS PROCEDURES

Avg. Ranking	*Streamlining Strategy*	*# of 5's & 4's*	*# of 1's & 2's*
4.21	Receive permission to use informal comment processes for the development of the CIP with a final 45-day comment period consistent with the ANSI process. *(NERC)*	**7**	**1**
3.29	Charge the SDT to complete CIP by April 1, 2010 – working outside the constraints of the current ANSI process. *(NERC)*	**5**	**4**
2.93	Revise the work plan to produce interim CIP deliverables prior to the final CIP deliverable that can be implemented more rapidly with less onerous comment response required. *(NERC and SDT)*	**1**	**2**

B. MEETING CHANGES- EFFICIENCY, LOCATION, TOOLS

Avg. Ranking	*Streamlining Strategy*	*# of 5's & 4's*	*# of 1's & 2's*
4.36	Make the best use of our time. Start meetings on time and get the technology operational early *(SDT)*	**8**	**0**
3.93	Meet in central US locations minimizing travel time and maximizing Team productivity and time. *(SDT and NERC)*	**5**	**1**
3.36	Longer, extended intensive meetings of the SDT (2-3 weeks at a time) *(SDT and NERC)*	**8**	**7**
2.86	Bring Team together for as long as it takes to get the job done (somewher *(SDT and NERC)*	**4**	**6**
2.79	Support the use of video technology for SDT meetings (e.g., Cisco Telepresence) *(NERC)*	**4**	**5**

C. COMMITMENT COMMUNICATION AND SUPPORT

Avg. Ranking	*Streamlining Strategy*	*# of 5's & 4's*	*# of 1's & 2's*
4.43	Improve industry communications in getting the word out on the SDT and its progress? Webinars, workshops, etc. *(NERC with SDT help)*	**11**	**0**
3.86	No audits for drafting team member organizations *(NERC).*	**8**	**2**
3.38	NERC support funding member expenses (1/2 of costs) for meetings. *(NERC)*	**5**	**5**
3.15	NERC letter to CEOs acknowledge the contributions of members and appreciation of work done so far (as requested by members) *(NERC)*	**6**	**5**
3.07	Establish idea sharing center on the NERC Website *(NERC)*	**4**	**7**
2.92	Full Commitment and support of members from their organizations extending down to include mgrs and lower level executives, not just pay lip service. *(SDT Members)*	**2**	**7**
2.50	NERC letters to CEO's to secure full commitments from CEOs of member organizations. *(NERC)*	**2**	**6**

2.50	Leverage FERC Power (influence) for immediate needs *(NERC)*	2	8
2.36	Open up the discussions beyond our electric industry *(NERC)*	1	10

D. TEAM STRUCTURE

Avg. Ranking	*Streamlining Strategy*	*# of 5's & 4's*	*# of 1's & 2's*
3.54	Break up the SDT into many small drafting groups--divide the work and focus on specific tasks. *(SDT)*	7	3
3.08	Establish a small core SDT drafting group that will commit to meeting frequently between SDT meetings to prepare materials and drafts for full group consideration at meetings. *(SDT)*	5	7
3.08	Divide the standards deliverables and organize the SDT to develop drafts for each. *(SDT)*	5	5

E. SUBSTANTIVE CHANGES IN APPROACH/SCOPE TO STANDARD DEVELOPMENT

Avg. Ranking	*Streamlining Strategy*	*# of 5's & 4's*	*# of 1's & 2's*
3.62	Refocus on security issues and less on compliance *(SDT)*	8	3
3.54	Remove penalty base requirements (you get what you measure) *(NERC, FERC, Congress)*	6	4
3.46	Simplify the approach and strategy to the standards to reduce complexity *(SDT)*	7	3
3.08	Adapt 800-82 (targeted for industrial control systems) *(NERC & SDT)*	3	7
2.92	Adopt 800-53 Rev 3 for control centers and data centers *(NERC & SDT)*	4	6
2.92	Review Order 706 and remove items included that should be given to ano group, challenged or deferred. *(NERC & SDT)*	4	5
2.46	Throw in with CSCTG from NIST *(NERC)*	2	8
2.38	Go back to the 'original, original' standards for cyber security as a basis for the new CIP (see NERC Website archive) *(SDT)*	2	7
2.08	Skip BES Mapping and install minimum security controls for all assets aft establishing clear cut agreed upon objectives on what we are securing. *(SD*	2	10
1.85	Abandon the NIST based approach and improve existing standards framework. *(SDT)*	0	13

F. MORE TALENT AND EXPERTISE TO SUPPORT SDT

Avg. Ranking	*Streamlining Strategy*	*# of 5's & 4's*	*# of 1's & 2's*
4.46	Technical writer support (More like Scott Mix) *(NERC)*	11	2
4.00	Engage technical writers *(NERC)*	8	3
3.15	Station engineers *(NERC)*	6	6
3.15	Legal support for the SDT *(NERC)*	4	6
3.08	Bring generating station engineers onto the SDT. *(NERC)*	4	5
2.85	Support outside expert presentations on security issues and standards in o industries. *(NERC)*	3	5

Appendix #7 CIP-002-4 Template

FERC Specific directives from order 706:

Compiled by Scott Mix, NERC

The following table contains the status of all issues raised in the order that were either "direct"ed, specifically in the order, or "adopt"ed from the NOPR..

Note: Given the confusion over the SDT's inclusion of the change in CIP-008 ("Testing the Cyber Security Incident response plan does not require removing a component or system from service during the test") that the commission did not "direct", even though p 687 states: "In light of the comments received, the Commission clarifies that, with respect to full operational testing under CIP-008-1, such testing need not require a responsible entity to remove any systems from service," I did not include any issue that was not actively directed for change, such as those designated "should consider" or similar.

Issue #	Paragraph #	Text	Phase[1]
1	13	NERC is directed to develop a timetable for development of the modifications to the CIP Reliability Standards and, if warranted, to develop and file with the Commission for approval, a second implementation plan.	This compliance filing; and an implementation plan is filed with each submitted version of the standards
2	25	we direct NERC to address revisions to the CIP Reliability Standards CIP-002-1 through CIP-009-1 considering applicable features of	Version 4

[1] Schedule phases in this column mean one or more of the following:
- "Version 2" – complete in filed version 2
- "Version 4" – planned for next major version (12-18 months plus)
- "Guideline" – stand alone guidance started after corresponding requirement is determined
- "TFE Filing" – 2009 filing on TFE proposal and Appendix 4D to RoP
- "not scheduled" – beyond Version 4
- "CMEP" – part of an existing or ongoing compliance audit, self-report or other process
- "VRF Filing(s)" – one of several already-filed (or very soon to be filed in the case of Version 2) VRF and/or VSL filings

Phase may also be self-explanatory if not one of these entries

		the NIST framework.	
3	47	The Commission adopts the CIP NOPR approach regarding NERC and Regional Entity compliance with the CIP Reliability Standards.	Rules of Procedure statement
4	49	The Commission also adopts its CIP NOPR approach and concludes that reliance on the NERC registration process at this time is an appropriate means of identifying the entities that must comply with the CIP Reliability Standards	Compliance registry process
5	72	We adopt our proposal in the CIP NOPR that responsible entities must comply with the substance of a Requirement.	CMEP
6	75	we direct the ERO to develop modifications to the CIP Reliability Standards that require a responsible entity to implement plans, policies and procedure that it must develop pursuant to the CIP Reliability Standards	Version 2
7	86	The Commission adopts its CIP NOPR proposal and approves NERC's implementation plan and time frames for responsible entities to achieve auditable compliance.	CMEP
8	89	we direct the ERO to submit a work plan for Commission approval for developing and filing for approval the modifications to the CIP Reliability Standards that we are directing in this Final Rule	This compliance filing; and an implementation plan is filed with each submitted version of the standards
9	90	We direct the ERO, in its development of a work plan, to consider developing modifications to CIP-002-1 and the provisions regarding technical feasibility exceptions as a first priority, before developing other modifications required by the Final Rule.	TFE Filing

10	96	we direct the ERO to require more frequent, semiannual, self-certifications prior to the date by which full compliance is required	CMEP program and self-certifications
11	97	we adopt our CIP NOPR proposals that, while an entity should not be subject to a monetary penalty if it is unable to certify that it is on schedule, such an entity should explain to the ERO the reason it is unable to self-certify	CMEP, self-certification process
12	106	the Commission adopts the CIP NOPR proposals and directs NERC to modify the CIP Reliability Standards through the Reliability Standards development process to remove the first two Terms ["reasonable business judgment," and "acceptance of risk"], and develop specific conditions that a responsible entity must satisfy to invoke the "technical feasibility" exception	Version 2 and TFE Filing
13	128	the Commission directs the ERO to develop modifications to the CIP Reliability Standards that do not include this term. We note that many commenters, including NERC, agree that the reasonable business judgment language should be removed based largely on the rationale articulated by the Commission in the CIP NOPR.	Version 2
14	138	the Commission directs the ERO to modify the CIP Reliability Standards through its Reliability Standards development process to remove references to reasonable business judgment before compliance audits begin.	Version 2
15	150	The Commission, therefore, directs the ERO to remove acceptance of risk language from the CIP Reliability Standards.	Version 2
16	156	the Commission directs the ERO to develop through its Reliability Standards development process revised CIP Reliability Standards that eliminate references to acceptance of risk.	Version 2

17	178	directs the ERO to develop a set of conditions or criteria that a responsible entity must follow when relying on the technical feasibility exception contained in specific Requirements of the CIP Reliability Standards	TFE Filing
18	186	the Commission adopts its proposal in the CIP NOPR that technical feasibility exceptions may be permitted if appropriate conditions are in place.	TFE Filing
19	192	the Commission adopts the CIP NOPR proposal for a three step structure to require accountability when a responsible entity relies on technical feasibility as the basis for an exception. We address mitigation and remediation in this section and direct the ERO to develop: (1) a requirement that the responsible entity must develop, document and implement a mitigation plan that achieves a comparable level of security to the Requirement; and (2) a requirement that use of the technical feasibility exception by a responsible entity must be accompanied by a remediation plan and timeline for elimination the use of the technical feasibility exception.	TFE Filing
20	209	The Commission thus adopts its CIP NOPR proposal that use and implementation of technical feasibility exceptions must be governed by a clear set of criteria.	TFE Filing
21	211	direct the ERO to include approval of the mitigation and remediation steps by the senior manager (identified pursuant to CIP-003-1) in the course of developing this framework of accountability.	TFE Filing
22	212	the practical considerations pointed out by a number of the comments have convinced us to adopt an approach to the issue of external oversight different from the one originally	TFE Filing

		proposed.	
23	218	we direct the ERO to design and conduct an approval process through the Regional Entities and the compliance audit process.	TFE Filing
24	219	we direct NERC, in developing the accountability structure for the technical feasibility exception, to include appropriate provisions to assure that governmental entities that are subject to Reliability Standards as users, owners or operators of the Bulk-Power System can safeguard sensitive information.	TFE Filing
25	220	We direct the ERO to submit an annual report to the Commission that provides a wide-area analysis regarding use of the technical feasibility exception and the effect on Bulk-Power System reliability.	TFE Filing
26	221	we direct the ERO to control and protect the data analysis to the extent necessary to ensure that sensitive information is not jeopardized by the act of submitting the report to the Commission.	TFE Filing
27	222	we direct the ERO to develop a set of criteria to provide accountability when a responsible entity relies on the technical feasibility exceptions in specific Requirements of the CIP Reliability Standards.	TFE Filing
28	222	We direct the ERO to develop appropriate modifications, as discussed above.	TFE Filing
29	233	we direct the ERO to consult with federal entities that are required to comply with both CIP Reliability Standards and NIST standards on the effectiveness of the NIST standards and on implementation issues and report these findings to the Commission.	Ongoing discussions with Drafting Team Members from USBR, BPA, NIST; Development of Version 4
30	253	While we adopt our CIP NOPR proposal, we recognize that the ERO has already initiated	Guideline / Version 4

		a process to develop such guidance … leave to the EO's discretion whether to incorporate such guidance into the CIP Reliability Standard, develop it as a separate guidance document, or some combination of the two.	
31	254	direct the ERO to consider these commenter concerns [how to assess whether a generator or a blackstart unit is "critical" to Bulk-Power System reliability, the proper quantification of risk and frequency, facilities that are relied on to operate or shut down nuclear generating stations, and the consequences of asset failure and asset misuse by an adversary]when developing the guidance.	Guideline / Version 4
32	255	we direct either the ERO or its designees to provide reasonable technical support to assist entities in determining whether their assets are critical to the Bulk-Power System.	Unscheduled
33	257	we direct the ERO to consider this clarification [the meaning of the phrase "used for initial system restoration," in CIP-002-1, Requirement R1.2.4] in its Reliability Standards development process.	Guideline / Version 4
34	272	the Commission directs the ERO, in developing the guidance discussed above regarding the identification of critical assets, to consider the designation of various types of data as a critical asset or critical cyber asset.	Guideline / Version 4
35	272	The Commission directs the ERO to develop guidance on the steps that would be required to apply the CIP Reliability Standards to such data and to consider whether this also covers the computer systems that produce the data.	Guideline / Version 4
36	282	the Commission directs the ERO, through the Reliability Standards development	Guideline / Version 4

		process, to specifically require the consideration of misuse of control centers and control systems in the determination of critical assets	
37	285	we direct the ERO to consider the comment from ISA99 Team [ISA99 Team objects to the exclusion of communications links from CIP-002-1 and non-routable protocols from critical cyber assets, arguing that both are key elements of associated control systems, essential to proper operation of the critical cyber assets, and have been shown to be vulnerable – by testing and experience].	Version 4
38	294	The Commission adopts its CIP NOPR proposal and directs the ERO to develop, pursuant to its Reliability Standards development process, a modification to CIP-002-1 to explicitly require that a senior manager annually review and approve the risk-based assessment methodology.	Version 2
39	294	the Commission directs the ERO to develop a modification to CIP-002-1 to explicitly require that a senior manager annually review and approve the risk-based assessment methodology.	Version 2
40	322	The Commission adopts its CIP NOPR proposal to direct that the ERO develop through its Reliability Standards development process a mechanism for external review and approval of critical asset lists.	Version 4 (Note: proposed version 4 methodology obviates the need for external review0
41	329	the Commission directs the ERO, using its Reliability Standards development process, to develop a process of external review and approval of critical asset lists based on a regional perspective.	Version 4 (Note: proposed version 4 methodology obviates the need for

			external review0
42	333	we direct the ERO, in developing the accountability structure for the technical feasibility exception, to include appropriate provisions to assure that governmental entities can safeguard sensitive information	TFE Filing
43	355	the Commission directs the ERO to provide additional guidance for the topics and processes that the required cyber security policy should address.	Guideline
44	376	the Commission adopts its CIP NOPR proposal and directs the ERO to clarify that the exceptions mentioned in Requirements R2.3 and R3 of CIP-003-1 do not except responsible entities from the Requirements of the CIP Reliability Standards.	Version 4
45	381	The Commission adopts its CIP NOPR interpretation that Requirement R2 of CIP-003-1 requires the designation of a single manager who has direct and comprehensive responsibility and accountability for implementation and ongoing compliance with the CIP Reliability Standards	Version 2
46	386	The Commission adopts its CIP NOPR proposal and directs the ERO to develop modifications to Reliability Standards CIP-003-1, CIP-004-1, and/or CIP-007-1, to ensure and make clear that, when access to protected information is revoked, it is done so promptly.	Version 4
47	397	The Commission directs the ERO to develop modifications to Requirement R6 of CIP-003-1 to provide an express acknowledgment of the need for the change control and configuration management process to consider accidental consequences and malicious actions along with intentional changes.	Version 4 / Guideline

48	412	The Commission therefore directs the ERO to provide guidance, regarding the issues and concerns that a mutual distrust posture must address in order to protect a responsible entity's control system from the outside world.	Guideline
49	431	The Commission adopts the CIP NOPR's proposal and directs the ERO to develop a modification to CIP-004-1 that would require affected personnel to receive required training before obtaining access to critical cyber assets (rather than within 90 days of access authorization), but allowing limited exceptions, such as during emergencies, subject to documentation and mitigation.	Version 2
50	433	we direct the ERO to consider, in developing modifications to CIP-004-1, whether identification of core training elements would be beneficial and, if so, develop an appropriate modification to the Reliability Standard.	Version 4
51	434	The Commission adopts the CIP NOPR's proposal to direct the ERO to modify Requirement R2 of CIP-004-1 to clarify that cyber security training programs are intended to encompass training on the networking hardware and software and other issues of electronic interconnectivity supporting the operation and control of critical cyber assets.	Version 4
52	435	Consistent with the CIP NOPR, the Commission directs the ERO to determine what, if any, modifications to CIP-004-1 should be made to assure that security trainers are adequately trained themselves.	Version 4
53	443	The Commission adopts with modifications the proposal to direct the ERO to modify Requirement R3 of CIP-004-1 to provide	Version 2

		that newly-hired personnel and vendors should not have access to critical cyber assets prior to the satisfactory completion of a personnel risk assessment, except in specified circumstances such as an emergency.	
54	443	We also direct the ERO to identify the parameters of such exceptional circumstances through the Reliability Standards development process	Version 4
55	460	The Commission adopts the CIP NOPR proposal to direct the ERO to develop modifications to CIP-004-1 to require immediate revocation of access privileges when an employee, contractor or vendor no longer performs a function that requires physical or electronic access to a critical cyber asset for any reason (including disciplinary action, transfer, retirement, or termination).	Version 4
56	464	We also adopt our proposal to direct the ERO to modify Requirement R4 to make clear that unescorted physical access should be denied to individuals that are not identified on the authorization list, with clarification.	Version 4
57	473	The Commission adopts its proposals in the CIP NOPR with a clarification. As a general matter, all joint owners of a critical cyber asset are responsible to protect that asset under the CIP Reliability Standards. The owners of joint use facilities which have been designated as critical cyber assets are responsible to see that contractual obligations include provisions that allow the responsible entity to comply with the CIP Reliability Standards. This is similar to a responsible entity's obligations regarding vendors with access to critical cyber assets.	Version 4

58	476	we direct the ERO to modify CIP-004-1, and other CIP Reliability Standards as appropriate, through the Reliability Standards development process to address critical cyber assets that are jointly owned or jointly used, consistent	Version 4
59	496	The Commission adopts the CIP NOPR's proposal to direct the ERO to develop a requirement that each responsible entity must implement a defensive security approach including two or more defensive measures in a defense in depth posture when constructing an electronic security perimeter	Not scheduled
60	502	The Commission directs that a responsible entity must implement two or more distinct security measures when constructing an electronic security perimeter, the specific requirements should be developed in the Reliability Standards development process.	Not scheduled
61	502	The Commission also directs the ERO to consider, based on the content of the modified CIP-005-1, whether further guidance on this defense in depth topic should be developed in a reference document outside of the Reliability Standards.	Not scheduled / Guideline
62	503	The Commission is directing the ERO to revise the Reliability Standard to require two or more defensive measures.	Not scheduled
63	511	The Commission adopts the CIP NOPR's proposal to direct the ERO to identify examples of specific verification technologies that would satisfy Requirement R2.4, while also allowing compliance pursuant to other technically equivalent measures or technologies.	Version 4
64	525	The Commission adopts the CIP NOPR proposal to require the ERO to modify CIP-	Version 4

		005-1 to require logs to be reviewed more frequently than 90 days	
65	526	the Commission directs the ERO to modify CIP-005-1 through the Reliability Standards development process to require manual review of those logs without alerts in shorter than 90 day increments.	Version 4
66	526	The Commission directs the ERO to modify CIP-005-1 to require some manual review of logs, consistent with our discussion of log sampling below, to improve automated detection settings, even if alerts are employed on the logs.	Version 4
67	528	the Commission clarifies its direction with regard to reviewing logs. In directing manual log review, the Commission does not require that every log be reviewed in its entirety. Instead, the ERO could provide, through the Reliability Standards development process, clarification that a responsible entity should perform the manual review of a sampling of log entries or sorted or filtered logs.	Version 4
68	541	we adopt the ERO's proposal to provide for active vulnerability assessments rather than full live vulnerability assessments.	Version 4
69	542	the Commission adopts the ERO's recommendation of requiring active vulnerability assessments of test systems.	Version 4
70	544	the Commission directs the ERO to revise the Reliability Standard so that annual vulnerability assessments are sufficient, unless a significant change is made to the electronic security perimeter or defense in depth measure, rather than with every modification.	Version 4
71	544	we are directing the ERO to determine, through the Reliability Standards development process, what would	Version 4

		constitute a modification that would require an active vulnerability assessment	
72	547	we direct the ERO to modify Requirement R4 to require these representative active vulnerability assessments at least once every three years, with subsequent annual paper assessments in the intervening years	Version 4
73	560	the Commission directs the ERO to treat any alternative measures for Requirement R1.1 of CIP-006-1 as a technical feasibility exception to Requirement R1.1, subject to the conditions on technical feasibility exceptions.	TFE Filing / CMEP
74	572	The Commission adopts the CIP NOPR proposal to direct the ERO to modify this CIP Reliability Standard to state that a responsible entity must, at a minimum, implement two or more different security procedures when establishing a physical security perimeter around critical cyber assets.	Not scheduled
75	575	The Commission also directs the ERO to consider, based on the content of the modified CIP-006-1, whether further guidance on this defense in depth topic should be developed in a reference document outside of the Reliability Standards.	Not scheduled / Guideline
76	581	The Commission adopts the CIP NOPR proposal and directs the ERO to develop a modification to CIP-006-1 to require a responsible entity to test the physical security measures on critical cyber assets more frequently than every three years,	Version 4
77	597	Therefore, the Commission directs the ERO to eliminate the acceptance of risk language from Requirements R2.3 and R3.2.	Version 2
78	600	Commission therefore directs the ERO to revise Requirement R3 to remove the	Version 2 / TFE Filing

		acceptance of risk language and to impose the same conditions and reporting requirements as imposed elsewhere in the Final Rule regarding technical feasibility.	
79	609	We therefore direct the ERO to develop requirements addressing what constitutes a "representative system" and to modify CIP-007-1 accordingly. The Commission directs the ERO to consider providing further guidance on testing systems in a reference document.	Version 4 / Guideline
80	610	we direct the ERO to revise the Reliability Standard to require each responsible entity to document differences between testing and production environments in a manner consistent with the discussion above.	Version 4
81	611	the Commission cautions that certain changes to a production or test environment might make the differences between the two greater and directs the ERO to take this into account when developing guidance on when to require updated documentation to ensure that there are no significant gaps between what is tested and what is in production.	Version 4
82	619	The Commission adopts the CIP NOPR proposal with regard to CIP-007-1, Requirement R4. [The Commission proposed to direct the ERO to eliminate the acceptance of risk language from Requirement R4.2, and also attach the same documentation and reporting requirements to the use of technical feasibility in Requirement R4, pertaining to malicious software prevention, as elsewhere. The Commission discussed the issues of defense in depth, technical feasibility, and risk acceptance elsewhere in the CIP NOPR and applied those conclusions here. The Commission further proposed to direct the	Version 4 / not scheduled

		ERO to modify Requirement R4 to include safeguards against personnel introducing, either maliciously or unintentionally, viruses or malicious software to a cyber asset within the electronic security perimeter through remote access, electronic media, or other means]	
83	622	Therefore, the Commission directs the ERO to eliminate the acceptance of risk language from Requirement R4.2	Version 2
84	622	The Commission also directs the ERO to modify Requirement R4 to include safeguards against personnel introducing, either maliciously or unintentionally, viruses or malicious software to a cyber asset within the electronic security perimeter through remote access, electronic media, or other means, consistent with our discussion above	Version 4 / not scheduled
85	628	The Commission continues to believe that, in general, logs should be reviewed at least weekly and therefore adopts the CIP NOPR proposal to require the ERO to modify CIP-007-1 to require logs to be reviewed more frequently than 90 days, but leaves it to the Reliability Standards development process to determine the appropriate frequency, given our clarification below, similar to our action with respect to CIP-005-1	Version 4
86	629	The Reliability Standards development process should decide the degree to which the revised CIP-007-1 describes acceptable log sampling. The ERO could also provide additional guidance on how to create the sampling of log entries, which could be in a reference document.	Version 4 / guideline
87	633	The Commission adopts the CIP NOPR proposal to direct the ERO to clarify what it means to prevent unauthorized retrieval of	Version 4

		data from a cyber asset prior to discarding it or redeploying it.	
88	635	the Commission directs the ERO to revise Requirement R7 of CIP-007-1 to clarify, consistent with this discussion, what it means to prevent unauthorized retrieval of data.	Version 4
89	643	The Commission adopts its proposal to direct the ERO to provide more direction on what features, functionality, and vulnerabilities the responsible entities should address when conducting the vulnerability assessments, and to revise Requirement R8.4 to require an entity-imposed timeline for completion of the already-required action plan.	Not scheduled
90	651	We direct the ERO to revise Requirement R9 to state that the changes resulting from modifications to the system or controls shall be documented quicker than 90 calendar days.	Version 2
91	660	The Commission adopts the CIP NOPR proposal to direct the ERO to provide guidance regarding what should be included in the term reportable incident. … we direct the ERO to develop and provide guidance on the term reportable incident.	Guideline
92	661	the Commission directs the ERO to develop a modification to CIP-008-1 to: (1) include language that takes into account a breach that may occur through cyber or physical means; (2) harmonize, but not necessarily limit, the meaning of the term reportable incident with other reporting mechanisms, such as DOE Form OE 417; (3) recognize that the term should not be triggered by ineffectual and untargeted attacks that proliferate on the internet; and (4) ensure that the guidance language that is developed	Version 4 / Guideline

		results in a Reliability Standard that can be audited and enforced	
93	673	The Commission adopts the CIP NOPR proposal to direct the ERO to modify CIP-008-1 to require each responsible entity to contact appropriate government authorities and industry participants in the event of a cyber security incident as soon as possible, but, in any event, within one hour of the event, even if it is a preliminary report.	Version 4 / Guideline
94	676	the Commission directs the ERO to modify CIP-008-1 to require a responsible entity to, at a minimum, notify the ESISAC and appropriate government authorities of a cyber security incident as soon as possible, but, in any event, within one hour of the event, even if it is a preliminary report.	Version 4 /. Guideline
95	686	The Commission adopts the CIP NOPR proposal to direct the ERO to modify CIP-008-1, Requirement R2 to require responsible entities to maintain documentation of paper drills, full operational drills, and responses to actual incidents, all of which must include lessons learned.	Version 4
96	686	The Commission further directs the ERO to include language in CIP-008-1 to require revisions to the incident response plan to address these lessons learned.	Version 4
97	694	For the reasons discussed in the CIP NOPR, the Commission adopts the proposal to direct the ERO to modify CIP-009-1 to include a specific requirement to implement a recovery plan.	Version 4
98	694	We further adopt the proposal to enforce this Reliability Standard such that, if an entity has the required recovery plan but does not implement it when the anticipated event or conditions occur, the entity will not	Version 4

		be in compliance with this Reliability Standard.	
99	706	The Commission adopts, with clarification, the CIP NOPR proposal to direct the ERO to modify CIP-009-1 to incorporate use of good forensic data collection practices and procedures into this CIP Reliability Standard.	Not scheduled
100	710	Therefore, we direct the ERO to revise CIP-009-1 to require data collection, as provided in the Blackout Report.	Not scheduled
101	725	The Commission adopts, with modifications, the CIP NOPR proposal to develop modifications to CIP-009-1 through the Reliability Standards development process to require an operational exercise once every three years (unless an actual incident occurs, in which case it may suffice), but to permit reliance on table-top exercises annually in other years.	Not scheduled
102	731	The Commission adopts the CIP NOPR proposal to direct the ERO to modify Requirement R3 of CIP-009-1 to shorten the timeline for updating recovery plans.	Version 2
103	739	The Commission adopts the CIP NOPR proposal to direct the ERO to modify CIP-009-1 to incorporate guidance that the backup and restoration processes and procedures required by Requirement R4 should include, at least with regard to significant changes made to the operational control system, verification that they are operational before the backups are stored or relied upon for recovery purposes	Version 4
104	748	The Commission adopts the CIP NOPR proposal to direct the ERO to modify CIP-009-1 to provide direction that backup practices include regular procedures to ensure verification that backups are	Version 4

		successful and backup failures are addressed, so that backups are available for future use.	
105	757	Therefore, we will not allow NERC to reconsider the Violation Risk Factor designations in this instance but, rather, direct below that NERC make specific modifications to its designations.	VRF Filing(s)
106	759	Consistent with the Violation Risk Factor Order, the Commission directs NERC to submit a complete Violation Risk Factor matrix encompassing each Commission approved CIP Reliability Standard.	VRF Filing(s)
107	767	The Commission adopts the CIP NOPR proposal to direct the ERO to revise 43 Violation Risk Factors.	VRF Filing(s)

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Agenda
Cyber Security Order 706 SDT — Project 2008-06

December 15, 2009 | 8:00 AM to 5:30 PM EST
December 16, 2009| 8:00 AM to 5:00 PM EST

Arkansas Electric Cooperative Corporation
1 Cooperative Way
Little Rock, AR,

NOTE:
1. Agenda Times May be Adjusted as needed during the Meeting
2. Document Drafting Group Meetings May Not Have Access to Telephones and Ready-Talk

Proposed Meeting Objectives/Outcomes

- Receive an overview the CIP 002-4 document drafting progress;
- Review the NERC's proposed FERC Order workplan filing and milestones;
- Conduct a walk-through of the CIP 002-4 and identify lessons learned and any changes needed in the document(s) including: Cover memo, Comment Form, CIP 002, Guidance Document, and Controls Description and Sample;
- Identify remaining CIP 002-4 key issues and provide guidance to document drafting groups;
- Convene CIP 002-4 Document Drafting Groups;
- Review and refine Document Drafting Group products;
- Compile, review and refine the draft CIP 002-4 and related documents;
- Adopt the CIP-002-4 Documents for posting;
- Review CSO 706 SDT leadership transition and changes; and
- Review the 2010 Schedule and agree on next steps and assignments.

Draft Agenda

Tuesday	**December 15, 2009**
8:00 a.m.	Welcome and Opening Remarks- *Jeri Domingo Brewer, Phil Huff & John Lim* Roll Call; NERC Antitrust Compliance Guidelines
8:10	Review of Meeting Objectives, Agenda and Meeting Guidelines- *Bob Jones*
8:15	Overview of CSO 706 SDT Workplan- December 2009 to June, 2010- *Jeri Domingo Brewer*
8:20	Review of NERC Actions in Support of CSO 706 SDT and NERC Workplan Filing with FERC- *Gerry Adamski, NERC*

	SDT Discussion of Proposed Workplan
9:20	Overview of CIP 002-4 Strawman Draft Documents- *John Lim et al.*
9:30	Walk Through of CIP 002-4 Strawman Scenario-*Jackie Collett et al.*
10:30	*Break*
10:45	Reflections and Lessons Learned from Walk Through and Implications for the CIP 002 Draft
11:00	Run-through and Flag Key Remaining Issues in CIP Version 4 Strawman Documents
12:15	*Lunch*
12:45	Review of Remaining Issues and Proposal for Key Issues/Documents Drafting Groups
1:00	Key Issues/Documents Drafting Sub-Group Meetings
4:00	Drafting Sub-Group Reports and Identification of any Outstanding Issues and Drafting Assignments
5:30	*Recess (possible after dinner drafting assignments)*

Wednesday	**December 16, 2009**
8:00	Welcome, Agenda Review and Antitrust Guidelines- *Jeri Domingo-Brewer, Phil Huff, John Lim & Joe Bucierro* Facilitator review and SDT acceptance of November 16-19, 2009 Orlando SDT meeting summary
8:10	Update on Status of Version 3 CIP Standards, Implementation Plans, etc–*Scott Mix*
8:20	Update on other related cyber security initiatives- *SDT Members*
8:30	Reconvene SDT CIP 002-4 Document Drafting Sub-Groups *(as needed)*
10:30	*Break*
10:45	Draft Document Review and Consensus Testing on Any Key Remaining Issues *(as needed)*
12:00	*Working Lunch (compilation of refined inputs to CIP 002-4 documents)*
12:45	Review of CSO 706 SDT Leadership Changes
1:00	Draft CIP-002-4 and Guidance Document Review
3:00	*Break*
3:15	**Motion to Adopt Draft CIP-002-4 and Guidance Documents for Industry Posting**
3:45	Review and Agree on CIP 002-4 Next Steps and January- June 2010 Workplan and Schedule Preparation and Assignments for CIP 003-009 January Meeting
4:30	Discussion of 2010 Meeting Logistics and Locations, and SDT Membership • Meeting Evaluation
5:00	*Adjourn*

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

PROJECT 2008-06 CYBER SECURITY ORDER 706 SDT MEMBERS

1. Rob Antonishen	Ontario Power Generation
2**. Jeri Domingo-Brewer, Chair**	U.S. Bureau of Reclamation
3. Jim Brenton	ERCOT
4. Jackie Collett	Manitoba Hydro
5. Jay S. Cribb	Information Security Analyst, Southern Company Services
6. Joe Doetzl	Manager, Information Security, Kansas City Pwr. & Light Co.
7. Sharon Edwards	Duke Energy
8. Gerald S. Freese	Director, Enterprise Info. Security America Electric Pwr.
9**. Phillip Huff, Vice Chair**	Arkansas Electric Coop Corporation
10. Doug Johnson	Exelon Corporation – Commonwealth Edison
11. Frank Kim	Ontario Hydro
12. Rich Kinas	Orlando Utilities Commission
13. John Lim, Vice Chair	CISSP, Department Manager, Consolidated Edison Co. NY
14. David Norton	Entergy
15. Christopher A. Peters	ICF International
16. David S. Revill	Georgia Transmission Corporation
17. Scott Rosenberger	Luminant Energy
18. Kevin Sherlin	Sacramento Municipal Utility District
19. Jonathan Stanford	Bonneville Power Administration
20.Keith Stouffer	National Institute of Standards & Technology
21. John D. Varnell	Technology Director, Tenaska Power Services Co.
22.William Winters	Arizona Public Service, Inc.
Roger Lampilla	NERC
Scott Mix	NERC
Dave Taylor	NERC
Joe Bucciero	NERC/Bucciero Consulting, LLC
Robert Jones	FSU/FCRC Consensus Center
Hal Beardal	FSU/FCRC Consensus Center
Stuart Langton	FSU/FCRC Consensus Center

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

CSO 706 SDT VERSION 3 CIP AND VERSION 4 CIP 002 PROCESS

CIP Version 3 Key Steps/Schedule

1. *Post for Industry Comment 10-13-09 to 11-12-09*
2. **November 13 SDT Conference Call- Review of Industry Comments and Response**
3. **November 16, CSO 706 SDT Meeting in Orlando, Monday, 5:00 p.m.- through dinner- Response Document to Industry Comments**
4. **November 17**, Tuesday, CSO 706 SDT Meeting, Orlando, Complete and Adopt Response Document to Industry Comments
5. **November 20**, Wednesday, Post Response Document and Initiate Ballot
6. **November 30**, Monday *(after Thanksgiving)* Deadline for Votes and Industry Comments
7. **December 2, Wednesday, CSO 706 SDT - Conference Call- finalize Response document to Industry Comments**
8. **December 3- 13,** Recirculation Ballot
9. **December 16,** BoT Approval
10. **December 29, 2009,** FERC Filing

CIP 002-4 Key Steps/Schedule (October-December 2009)

1. **November 1:** Jackie Collett, Phil Huff, John Lim and John Varnell, the chairs of the 4 CIP 002 Subgroups will form the CIP 002 Strawman Drafting Group (SDG).
2. **November 1:** All CIP 002 "meta groups" and subgroups will forward to the Strawman Drafting Group their standards text drafts including any guidance language**.**
3. Joe Doetzl will coordinate the work of the Controls Drafting Group (CDG) members: Jim Brenton, Keith Stouffer, Bill Winters, Jon Stanford. They will produce several recommended sample controls to illustrate high/medium/low concepts in CIP 002 as well as recommendations on whether the SDT should request guidance from the Standards Committee on referencing a 'catalogue of security requirements', for circulation to the SDT **by Friday, November 13, 2009**
4. The SDG will prepare a strawman draft by **November 13, 2009** for review by the SDT in advance of November 16-19, 2009 SDT meeting
5. The SDT will utilize the strawman draft to organize its **November 16-19 meeting** and determine at the conclusion of the meeting if the SDT will continue to aim for the December 16th adoption of CIP 002 draft for posting for industry comment
6. **December 7, 3:00-4:30 p.m. est**. Previews of reviewed CIP 002 and related document drafts at a SDT conference call.
7. The SDT will refine and circulate a revised strawman Draft by Monday, December 14, 2009 for review at the **December 15-16** CSO706 SDT meeting in Little Rock
8. **December 15-16** will refine, finalize and adopt draft CIP 002-4 for posting to the industry for informal comments.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

CSO 706 SDT MEETING SCHEDULE
OCTOBER 2008–DECEMBER 2010
DEVELOPMENT OF CIP VERSION 2 AND NEW VERSION FRAMEWORK
OCTOBER 2008–JULY 2009

1. October 6–7, 2008 — Gaithersburg, MD Reviewed CIP-002-CIP-009, Agreed on Version 2 approach.
2. October 20–21 —Sacramento, CA CIP-002-CIP-009 Version 2 development
3. November 12–14, 2008 — Little Rock, AR CIP-002-CIP-009 Version 2 adoption for comment and balloting; CIP-002-CIP-009 New Version process reviewed.
4. December 4–5, 2008 — Washington D.C. CIP-002-CIP-009 Version 3 reviewed and debated, SDT member white "working" papers assigned, Technical Feasibility Exceptions white paper reviewed and refined.
5. January 7–9 — Phoenix, AZ, Reviewed Technical Feasibility Exceptions white paper**,** reviewed industry comments on CIP-002-CIP-009 Version 2 products — established small groups to draft responses, reviewed New Version white "working" papers.
January 15 — WebEx meeting(s) Small group drafted responses to industry Version 2 comments.
January 21 — WebEx meeting(s) Small group drafted responses to industry Version 2 comments.
6. February 2–4, 2009 — Phoenix, AZ Update on NERC Technical Feasibility Exceptions process**,** VSL process and SDT role**,** review of Version 3 White papers, strawman and principles**,** reviewed and adopted SDT responses to industry comments on Version 2 and Version 2 Product Revisions.
7. February 18–19, 2009 — Fairfax, VA Update on Version 2 process**,** NERC TFE process and VSL Team process; reviewed, discussed and refined Version 3 CIP-002 White papers, strawman, and principles.
8. March 10–11, 2009 — Orlando, FL Update on NERC TFE and VSL and VRF Team process and review and refine Version 3 CIP-002 Strawman Proposals
March 2–April 1, 2009 — 30-day Pre Ballot
Mid-March — NERC posts TFE draft Rules of Procedure for industry comment
March 30, 2009 — WebEx meeting(s) White Paper Drafting Team
April 1–10 — NERC Balloting on Version 2 Products
April 6, 2009 — WebEx meeting — White Paper Drafting Team
April 8, 2009 — WebEx meeting(s) — White Paper Preview- Full SDT Conference Call
April 11, 2009 — Version 2 Ballot Results (Quorum: 91.90% Approval: 84.06%) and Industry Comments
9. April 14–16, 2009 — Charlotte NC Update on NERC TFE process, VSL Team process and NERC Critical Assets Survey; agreed and adopted responses for Version 2 industry comments for recirculation ballot; reviewed and refined Version 3 whitepaper and consensus points and progress report to NERC Member Representative Committee (MRC) May meeting.
April 28 and May 6, 2009 — White Paper Drafting Team Meetings and WebEx
April 17–27, 2009 — Recirculation Results: Quorum: 94.37% Approval: 88.32%
May 5, 2009 — NERC MRC Meeting, Arlington, VA- SDT progress report.
10. May 13–14, 2009 — Boulder City NV Reviewed MRC presentation and further SDT refinement and discussion of the Version 3 White Paper.
June 8 and June 15, 2009 — Working Paper Drafting Team Meetings and WebEx

11. June 17–18, 2009 — Portland OR Further SDT refinement of the draft CIP Version 3 Working Paper(s), reviewed SDT development process for June-December 2009; discussed potential SDT subcommittee structure and deliverables.

- *June — WebEx meeting(s)*
- *Working Paper drafting group sessions including inputs from selected industry personnel to help establish BES categorization criteria*

CIP-002 DEVELOPMENT OF REQUIREMENTS, MEASURES, ETC. JULY-DECEMBER 2009

12. July 13–14, 2009 in Vancouver, B.C., Canada
SDT reviewed, refined, and adopted SDT Working Paper. SDT adopted its response to NERC for Interpretation of CIP-006-1. SDT reviewed and adopted a proposal for CIP-002 Subgroups and Deliverables and convened subgroup organizational meetings to develop work plans. SDT adopted 2010 Meeting Schedule.

- *July–August Interim Conference call meeting(s)*
- *CIP-002 Subgroup meetings*
- *CIP-002 Coordination Team meeting*
- *August 3–5, 2009 in Winnipeg, Manitoba* ***NERC Member Representative Committee****. Progress Report and presentation on new CIP Version 3 Working Paper-Concept- Reliability Standards on Cyber Security for MRC input.*

13. August 20–21, 2009 in Charlotte, NC. SDT reviewed and responded to MRC input on Working Paper/CIP-002 Concepts and convened SDT Subgroup and plenary meetings to develop CIP-002 requirements and "proof of concept" control (s).

- *July–September — 45-day Industry Comment Period on CIP-002 Concept Working Paper*
- *NERC Webinar- August–September Interim Conference Call meeting(s)*
- *CIP-002 Subgroup meetings (as ne*
- *CIP-002 Coordination Team meeting*

14. September 9–10, 2009 in Folsom, CA. SDT reviewed and considered industry comments on the Working Paper and CIP-002 concepts and their application to the subgroup work and addressed coordinating issues through joint subgroup meetings. SDT agreed on meeting dates and proposed locations for January–December 2010 September–October Interim WebEx meeting(s)

- *FERC Version 3 Urgent Action SDT conference call meetings*
- *CIP-002 Coordination Team meeting*

CIP VERSION 3 RESPONSE TO FERC ORDER, OCTOBER-DECEMBER, 2009

15. October 20–22, 2009 in Kansas City, MI. Reviewed new FERC Order and urgent action CIP Version 3 process; discussed key issues raised by SDT CIP 002 Subgroups, small group meetings and agreement on refinements to the CIP 002-009 schedule and drafting process for CIP 002-4.

- *October–November Drafting Team meeting(s)*
- *CIP-002 Coordination Team meeting*

16. November 16–19, 2009 in Orlando, FL

- SDT review, refine and adopt Version 3 "industry response" document.
- SDT plenary and drafting group session(s) — to draft, review and refine CIP-002-4 standard, requirements, measures and controls and related documents.
- November–December Interim Conference call meeting(s)
- Drafting teams as needed to finalize draft CIP 002-4 documents
- CIP-002 Coordination Team meeting
- *CIP 002-4 Drafting Team produces next draft based on Orlando Meeting input.*
- *December 2 CSO 706 SDT Version 3 Consideration of Comments Draft Conference Call*
- *December X, CSO 706 SDT CIP 002-4 Preview Conference Call*

17. December 15–16, 2009 in Little Rock AK

- SDT scenario "walk through" to test flow of CIP 002-4.
- SDT plenary and drafting group session(s) to review, refine, and agree on and adopt CIP-002 standard, requirements, measures and controls and related documents.
- Agree on initial posting of draft CIP-002 for industry review and comment.
- Agree on next steps and 2010 Workplan and schedule

REFINEMENT AND ADOPTION OF CIP-002 VERSION 4 AND DEVELOPMENT AND ADOPTION OF CIP STANDARDS (003-009)
JANUARY 2010–DECEMBER 2010

18. January 19-20–21-22 — Tue-PM- to Friday AM, Tucker, GA (GTC)

- SDT Work on Developing CIP 003-009 Strawman Drafts

19. February 17-18–19 —Wed--Thursday –Friday, Austin TX (ERCOT)

- SDT Reviews Industry Comments and Refines CIP 002 for posting for 45-day industry formal comment period.
- SDT continues CIP 003-009 Strawman Drafts

20. March 9–10-11 — Tuesday–Thursday, Phoenix, AZ (APS)

- SDT continues CIP 003-009 Strawman Drafts

21. April 13-14–15 — Tue-Wednesday–Thursday, Atlanta GA (Southern Co)

- SDT Reviews and Responds to Industry Comments, Refines and Adopts CIP 002 for balloting
- SDT posts a draft CIP 003-009 for informal industry comment.

22. May 11-12–13 — Tue-Wednesday–Thursday, Dallas TX (Luminant)

- SDT reviews Industry 1st Ballot Comments and Drafts Responses
- SDT reviews CIP 003-009 informal industry comments and refines the draft.

23. June 8-10- Tues, Wed. Thursday- (Sacramento)

- SDT refines CIP 003-009 and posts for 2nd round of informal industry comments and refines the draft.

24. July 13-14–15, Tue-Wednesday–Thursday, Pittsburgh, PA (CERT)

- SDT reviews CIP 003-009 informal industry comments and refines the draft.

25. August 10-11–12, Tue-Wednesday–Thursday- TBD

- SDT refines CIP 003-009 and posts for formal 45 day industry comment

26. September 7,8,9, Tues-Thurs. TBD (if needed)

27. Oct. 12-13–14, Tue-Wednesday–Thursday- TBD

- SDT Reviews and Responds to Industry Comments, Refines and Adopts CIP 002 for balloting

28. November 16-17–18, Tue-Wednesday–Thursday- TBD

- SDT reviews Industry 1st Ballot Comments and Drafts Responses

29. December 14-15–16, Tue-Wednesday–Thursday- TBD

SDT Consensus Guidelines
Adopted Unanimously, November 13, 2008, Little Rock AR
Cyber Security for Order 706 Standard Drafting Team

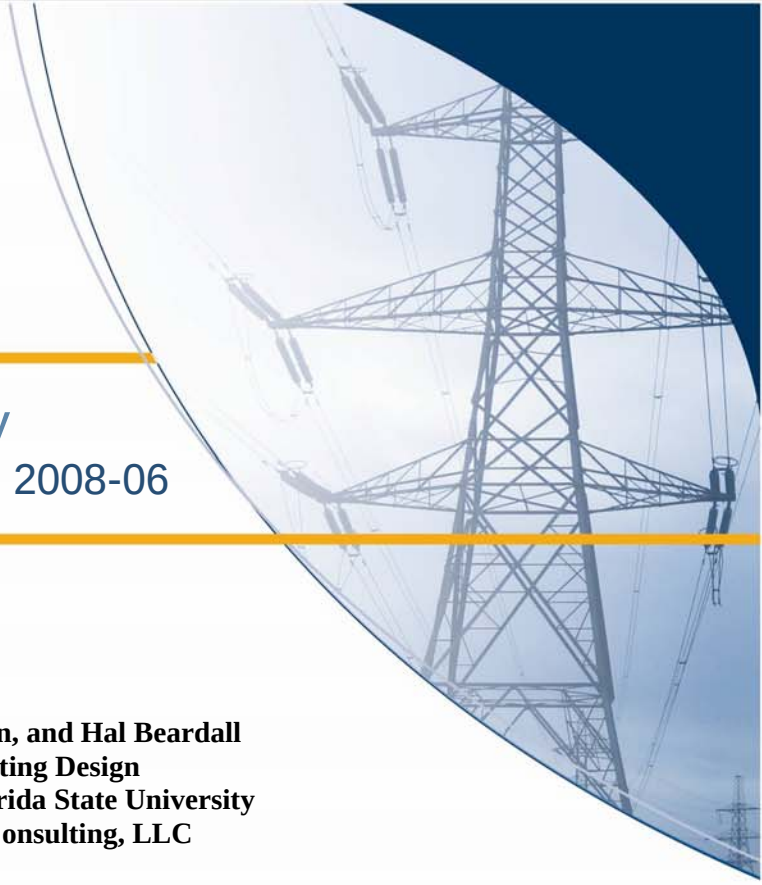
The Cyber Security for Order 706 Standard Drafting Team (Team) will seek consensus on its recommendations for any revisions to the CIP standards.
General consensus is a participatory process whereby, on matters of substance, the members strive for agreements which all of the members can accept, support, live with or agree not to oppose. In instances where, after vigorously exploring possible ways to enhance the members' support for the final package of recommended CIP revisions, and the Team finds that 100% acceptance or support of the members present is not achievable, final consensus recommendations will require at least 75% favorable vote of all members present and voting. This super majority decision rule underscores the importance of actively developing consensus throughout the process on substantive issues with the participation of all members. In instances where the Team finds that even 75% acceptance or support is not achievable, the Team's report will include documentation of any differences as well as the options that were considered for which there was greater than 50% support from the Team.

The Team will develop its recommendations using consensus-building techniques with the leadership of the Chair and Vice Chair and the assistance of the facilitators. Techniques such as brainstorming, consensus testing through rating and prioritizing approaches will be utilized. The Team's deliberation process will be conducted as a facilitated consensus-building process. Team members, NERC staff and facilitators will be the only participants seated at the table. Only Team members may participate in consensus rating or votes on proposals and recommendations. Observers/members of the public are welcome to speak when recognized by the Facilitator and all written comments submitted on the comment forms will be included in the Team and facilitators' summary reports.

The Team will make decisions only when a quorum is present. A quorum shall be constituted by at least 2/3's of the appointed members being present. The Team will utilize Robert's Rules of Order *(as per the NERC Reliability Standards Development Procedure)*, as modified by the Team's adopted procedural guidelines, to make and approve motions; however, the 75% supermajority voting requirement will supersede the normal voting requirements used in Robert's Rules of Order for decision making on substantive motions and amendments to motions. In addition, the Council will utilize their adopted meeting guidelines for conduct during meetings. The Council will make substantive recommendations using their adopted facilitated consensus-building procedures, and will use Robert's Rules of Order only for formal motions once a facilitated discussion is completed.
The presiding chair and/or facilitators for the SDT, in general, should use parliamentary procedures set forth in Robert's Rules of Order, as modified by Team's adopted procedural guidelines.

To enhance the possibility of constructive discussions as members educate themselves on the issues and engage in consensus-building, members agree to refrain from public statements that may prejudge the outcome of the Team's consensus process. In discussing the Team process with the media, members agree to be careful to present only their own views and not the views or statements of other participants and/or may direct such inquiries to the Team Chair and Vice Chair or the NERC Director of Standards. In addition, in order to provide balance to the Team process, members agree to represent and consult with appropriate industry interest groups.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION



16th Meeting Executive Summary

Cyber Security Order 706 SDT — Project 2008-06

December 15, 2009 | 8 a.m. to 5 p.m. EST
December 16, 2009 | 8 a.m. to 5 p.m. EST

Robert Jones, Stuart Langton, and Hal Beardall
Facilitation and Meeting Design
FCRC Consensus Center, Florida State University
Joe Bucciero, Bucciero Consulting, LLC

http://www.nerc.com/filez/standards/Project_2008-06_Cyber_Security.html

116-390 Village Blvd.
Princeton, NJ 08540
609.452.8060 | www.nerc.com

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Meeting Summary Contents

EXECUTIVE SUMMARY

On Wednesday morning, the Chair welcomed the members and Joe Bucciero conducted a roll call of members and participants in the room and on the conference call. After the Chair reviewed the meeting objectives, Mr. Bucciero reviewed with members the need to comply with NERC's Antitrust Guidelines. On Thursday morning, the SDT approved, without objection, the meeting summary for the November meeting in Orlando. Following lunch on Thursday, the SDT congratulated and applauded Jeri Domingo Brewer on her leadership role in chairing the team for the past 15 months and Phil Huff and John Lim presented her a plaque on behalf of the SDT in recognition of her leadership by example.

Gerry Adamski, NERC Director of Standards, reviewed with the team the NERC efforts to provide support for the team as they confront the challenge of completing the CIP in 2010. He offered that the new President of NERC has indicated that this is one of its most critical projects in the coming year.

He recounted that NERC had projected a two-year time frame for the project which will be realized if the SDT can complete its work by December 2010. He suggested that the SDT must demonstrate that CIP 002 Version 4 and the controls in CIP 003-009 will improve the current critical asset identification process and this has both technical requirements and political overtones.

Since the SDT November meeting in Orlando, NERC has identified a critical path to accomplish two things: a quality CIP 002-4 revision by June 2010 and the related set of security controls/requirements by the end of 2010. NERC has been working on how to put an optimal framework in place to allow the delivery on the expectations for the SDT. He noted a couple offline meetings with industry leaders and the SDT leadership have led to identifying NERC actions that can assist the Team. NERC met with trade associations collectively on November 30, 2009 to solicit their support and to build a mutual understanding of the technical and political complexity involved in the updating the CIP. In support of the SDT's meeting process, NERC has committed to implementing a comprehensive communication campaign and has secured additional support with Roger Lampila from Compliance and Dave Taylor and Howard Gugel from NERC Standards, in addition to Scott Mix's expertise, and introduced Lauren Koller from NERC who will assist and help Joe Bucciero on the ready talk and document displays. He noted that the Standards Committee met earlier in December and approved the use of an informal comment period followed by a formal 45-day comment period. He asked the Team to continue to help NERC understand what is needed to get the job done.

The Chair welcomed and introduced Barry Lawson with the National Rural Electric Cooperative Association (NRECA) and current chair of NERC's Critical Infrastructure Protection Committee (CIPC) and Allen Mosher representing the American Public Power Association (APPA) and vice chair of the NERC Standards Committee**.** They reviewed the letter sent to the Team by five trade associations including NRECA, the Edison Electric Institute, the American Public Power Association, the Electric Consumers Resource Council and the Electric Power Supply Association. They offered to provide any support that the trade association could in support of the industry's self regulatory model and industry developed standards. They asked the SDT to let them know what they can do to help. The Trade Associations agreed that:

- The Industry must seek to eliminate subjectivity as much as possible from both a technical and political standpoint.
- The SDT should identify the "brightest lines you can come up with".
- Trade associations are not suggesting how to do this. The current draft has made huge steps in the right direction.

- If we don't get the CIP standards right there will be real consequences for the Industry including a potentially reduced role in the development of these standards.
- The SDT's framework for the CIP appears sound and makes intuitive sense. Develop an asset classification approach that will make sense to the industry.
- The trade associations pledge to try to get our respective members to give early, responsive and constructive comments to the SDT on its drafts.

On behalf of the SDT, the chair noted appreciation for the work and efforts of NERC and the Trade Associations in assisting the SDT in its efforts to draw up a new CIP.

John Lim then provided an overview of the work undertaken and the changes made to the CIP 002-4 draft documents between Orlando and Little Rock by a drafting group comprised of John Lim, Jackie Collett, Phil Huff and John Varnell. These included the CIP 002, the Guidance Document, the Introduction and Comment Form and the Control examples. Dave Taylor noted that Howard Gugel from NERC will help the SDT get next products up to speed and be able to work with the SDT to answer any questions regarding format.

Jackie Collett provided an overview of the Pinecone Power "walk through" exercise. The SDT broke into two small groups and engaged in a "walk through" exercise. Following the break outs, the SDT reviewed reflections on lessons learned from the walk through in terms of implications for improving or clarifying the CIP 002 draft, including:

- Clarify how to define BES sub system in requirements and/or guidance
- Determine Appendix 2 requirement in standard
- Clarify blackstart units that change: How to address this in requirements? "blackstart capable"
- In terms of generating subsystems — define "Plant" — Units, combinations.
- R1 — "Identify + Categorize"? vs. Categorize.
- Keep cyber for R3? Not in R1 — rely on applying criteria.
- How to address "combinations" in the subsystems? Start with cyber systems first?
- Appendix #2 "Must Identify" a requirement with appendix.
- Careful we do not oversimplify categorization which may result in over protection — too many shortcuts could lead to incorrect conclusions.
- Need a full assessment without requiring more work than is necessary.
- We want to be sure nothing is missed — doesn't matter how it is defined if it is covered — then can choose to make it a subsystem but are not required to
- Give entities flexibility but careful don't leave an opportunity to game system by breaking systems into parts that stay below threshold for "high"
- Clarify something in R3 — identify and categorize all BES subsystems ….. that means identify every part of cyber system that has anything to do with awareness function — is that what we meant?

Following the Walk Through, the SDT reviewed the remaining issues and agreed to work in the following Drafting Groups on Wednesday afternoon to address issues raised in the "Walk-Through" and bring back clarifications and refinements for consideration by the SDT.

- Group #1 addressed Requirement #1and reviewed and produced agreement on how to address the R1 and appendix issues that had been raised in the walk through.
- Group #2 addressed Requirements #3 reviewed and produced agreement on how to address the R3 and appendix issues that had been raised in the walk through.

At the end of the day, the SDT reviewed progress and noted the following assignments:

- Issues of reliability functions— Phil Huff noted a plan to meet for dinner and resolve these issues and bring suggestions back tomorrow first thing tomorrow.
- Break into groups for document drafting (introduction and comment form; CIP 002-4; Guidance Document; Appendices; and Sample Controls.

Chair reminded the SDT that the goal is to ensure posting for informal industry review and the SDT should expect many suggestions back from industry. She also checked with the SDT to see if there were any red flags on proposed list of FERC specific directives in 706 since it will be part of the NERC filing at the end of December. The SDT concurred with the list.

On the second day John Lim reviewed with the SDT the revised definitions of terms used in standard and the SDT thoroughly discussed and reached consensus on issues in the definitions section.

Phil Huff led the SDT through a discussion of the changes to the standards sections R1, R2, R3 and R4. The SDT polled support for a couple of propositions including:

- **R-1. —** TPO requirements call for "annual" evaluation. SDT Poll support for reinstating the term "annual" in the standard for CIP-002-4 draft for industry comment: Yes — 8, No — 10. Won't reinstate "annual" for CIP 002-4 draft.
- **R4**.— Is the senior manager the right one for this role? If not, then does this requirement do much? The members ranked acceptability of the following options (multiple votes were permitted):
  - Remove it, address it elsewhere: 10 votes
  - Keep in R2 but with fuller definition: 9 votes
  - Keep it here as is: 7 votes
  - Remove here and keep in the comment form: 1 vote

  Members then offered the following preference polling *(only one vote for one of the 3 options)*
  - Remove it, address it elsewhere: 8
  - Keep in R2 but with fuller definition: 5
  - Keep it here as is: 1
- There is consensus of the importance of the issue and inclusion of the senior manager but less clear how best to do it.

The SDT then reviewed and refined the Compliance Section, the VSLs section and the Attachment documents.

On Thursday afternoon a motion was made and seconded to approve CIP 002-4 with identified and agreed upon changes. 16 members voted in favor, 0 members opposed and 1 member abstained.

Following a break, the SDT broke into separate "document" groups to harmonize the comment form and guidance document with the adopted CIP 002-4 (e.g. the Introduction and Comment Form and the Guidance Document). At the conclusion of the small group refinements to these documents the SDT reviewed the following key issues for the future (i.e. "parking lot")

- More detail on reliability functions to make operational — address "over protection" issues — map Requirement Function to thresholds
- "Controls" — "secure" defined — address in 003-009
- "BES Subsystem Impacts" define going forward (high/medium/low)
- 1.7, 1.11 & 1.15 — control center function issues)

The SDT Chair and Vice Chairs reviewed with the Team the work plan going forward including the need to make progress on the security controls (CIP 003-009) at the SDT's January meeting in Tucker, Georgia. The chair thanked Phil Huff for hosting the meeting and providing excellent food and facilities.

The SDT adjourned at 3:30 p.m. on December 16, 2009.

I. AGENDA REVIEW AND UPDATES

A. Agenda Review

On Tuesday morning, the Chair, Jeri Domingo-Brewer welcomed the members and Joe Bucciero conducted a roll call of members and participants in the room and on the conference call *(See appendix #2*). The Chair reviewed the meeting objectives and Bob Jones, facilitator, reviewed the proposed meeting agenda *(See appendix #1*). On the second day the SDT approved without objection the meeting summary for the November meeting in Orlando.

Mr. Bucciero reviewed the need to comply with NERC's Antitrust Guidelines *(See Appendix #3).* He urged the team and other participants in the process to carefully review the guidelines as they would cover all participants and observers. He urged all to avoid behaviors or appearance that would be anti-competitive nature and also reminded the group of the sensitive nature of the information under discussion.

Following lunch on Thursday, The SDT congratulated and applauded Jeri Domingo Brewer on her leadership role in chairing the Team for the past 15 months and Phil Huff and John Lim presented her a plaque on behalf of the SDT in recognition of her leadership by example. The Chair thanked the members for the acknowledgement and encouraged them to build on their work to date to get the job done by the end of 2010.

B. Review of NERC and Trade Association Actions in Support of CSO 706 SDT

Gerry Adamski, NERC Director of Standards, reviewed with the Team the NERC efforts to provide support for the team. He noted his admiration and appreciation for SDT commitment and dedication to this challenging task and that he believed it was Evident that all members are making a difference. He expressed his hope that the

Team could continue to move forward expeditiously with the task in the coming year. He offered that the new President of NERC has indicated that this is one of its most critical projects in the coming year.

He suggested that the Team will be challenged in addressing and finalizing CIP 002-4 while simultaneously developing CIP 003-009 addressing a significant portion of Order 706 directives. He reported that the Recirculation Ballot for Version 3 received 85.6% approval and that the NERC Board of Trustees was set on December 16 to approve version 3 and send on to FERC.

He recounted the "whirlwind of activities" over the past year and half and the call to action with respect to delivery of critical infrastructure standards. NERC had projected a two year time frame for the project which will be realized if the SDT can complete its work by December 2010. The SDT must demonstrate that CIP 002 Version 4 and the controls in CIP 003-009 will improve the current critical asset identification process and this has both technical requirements and political overtones.

Since the SDT November meeting in Orlando, NERC has identified a critical path to accomplish two things: a quality CIP 002-4 revision by June 2010 and the related set of security controls/requirements by the end of 2010. NERC has been working on how to put an optimal framework in place to allow the delivery on the expectations for the SDT. He noted a couple offline meetings with industry leaders and the SDT leadership have led to identifying NERC actions that can assist the Team. NERC met with trade associations collectively on November 30, 2009 to solicit their support and to build a mutual understanding of the technical and political complexity involved in the updating the CIP.

The Trade Associations are hoping the new CIP will provide clearer delineations in categorizing critical assets, i.e. "more bright line" determinations. The hope for is for producing a standard that is more objective than subjective and that provides an entity the understanding of which category their assets fall into.

In support of the SDT's meeting process, NERC has secured additional support with Roger Lampila from Compliance and Dave Taylor and Howard Gugel from NERC Standards, in addition to Scott Mix's expertise. Mr. Adamski noted that he has collected internal NERC comments on the current CIP 002-4 draft and will provide feedback to the SDT later at this meeting. He also introduced Lauren Koller from NERC who will assist and help Joe Bucciero on the ready talk and document displays.

The Standards Committee met earlier in December and approved the use of an informal comment period followed by a formal 45 day comment period. While comments are underway, NERC will be assembling the ballot pool.

NERC understands the new CIP will represent a sea-change and paradigm shift for the Industry and will require a comprehensive communication campaign. NERC will develop more formalized campaign. This was started in early December, 2009 by presenting to and working with the Operations and Planning Committee and CIPSE at their meetings. NERC will be holding a webinar- in early February 2010 with industry and will need the Team's help on this. In terms of the CIP 003-009, security controls framework for development, NERC is hoping to have a better sense following the January SDT meeting in Tucker. NERC wants to give adequate support so the SDT can get this job done with a quality product. He asked the Team to continue to help NERC understand what is needed and NERC will seek to put tools in your tool box to help you.

The Chair welcomed and introduced Barry Lawson with the National Rural Electric Cooperative Association (NRECA) and current chair of NERC's Critical Infrastructure Protection Committee (CIPC). He noted the five trade associations that signed the letter to the SDT including NRECA, the Edison Electric Institute, the American Public Power Association, the Electric Consumers Resource Council and

the Electric Power Supply Association. He addressed the SDT not as CIPCE chair but with his NRECA trade association hat. He made remarks to Operations Committee, Planning Committee and to CIPSE last week. He offered to provide any support that the trade association could in support of the industry's self regulatory model and industry developed standards. He noted that the work of SDT is being closely watched by FERC and Congress and that it is getting more attention than a normal SDT usually gets.

NERC has reached out to trade groups to help the SDT. He asked the SDT to let them know what they can do to help. He believes the Industry has to demonstrate that we can develop the CIP on expedited basis resulting in a clear and objective way that is easily auditable for both entities and the auditor. He offered the following points:

- We must seek to eliminate subjectivity as much as possible from both a technical and political standpoint.
- The SDT should identify the "brightest lines you can come up with".
- Trade associations are not suggesting how to do this. The current draft has made huge steps in the right direction.
- If we don't get the CIP standards right there will be real consequences for the Industry including a potentially reduced role in the development of these standards. More is at stake than simply a ballot that doesn't pass with sufficient Industry support. Draft legislation is already out there that points in this direction and we have to show that the Industry can get the job done with our self-regulatory model which may not always the prettiest, but it promises to produce the best results for reliability and security.
- Please continue your efforts- this team has put much time and effort into this so far. Getting CIP 002 right is critically important. Bold steps are needed.

The Chair then welcomed and introduced Allen Mosher representing the American Public Power Association (APPA)**.** Mr. Mosher noted he was wearing two hats in addressing the SDT: one as a national trade association representative; and another as vice chair of the NERC Standards Committee. He recounted the NERC Standards Committee's review and discussion regarding the SDT process modifications for an expedited schedule and noted they came to consensus in support of this approach because of the shared understanding that the Industry needs to move expeditiously in revising the CIP. Hopefully we will get to consensus with industry on the new CIP and the industry is confident that you are listening to their concerns and you have a plan of action to address them. The joint Trade Association letter demonstrates this. He then offered the following points:

- The SDT's framework for the CIP appears sound and makes intuitive sense. Develop asset classification that will make sense to the industry.
- The Standards Committee stands ready to help the SDT in this important effort.
- In terms of the trade associations, we pledge to try to get our respective members to give early, responsive and constructive comments to the SDT on its drafts. We can also help to get subject matter experts focused on this project. Both in January for reviewing the CIP 002-4 and further on in terms of security controls (CIP 003-009)
- Need to know up front of problems. Will motivate members to get those to the SDT as early as possible. Let's get the right solution for the CIP suite of standards.

On behalf of the SDT, the chair noted appreciation for the work and efforts of NERC and the Trade Associations in assisting the SDT in its efforts to draw up a new CIP.

SDT Member Comments:

- How much preparation will it take for industry to understand this new approach? Is leadership preparing the industry for added expenses these changes will require?
- Mr. Lawson responded that he was reaching out to electric cooperative leaders- explaining the reality of the situation, i.e. that more and stricter standards will require greater costs and investments. While they are not offering the SDT a blank check, they do want to see the connection with costs and increasing effectiveness. Will reach out to NREECA members to provide them with context about draft and encourage them submit comments (both pro and con) early.
- Mr. Mosher noted that the APPA envisions similar efforts with its members. There will undoubtedly be push back on increasing costs as budgets everywhere are tight. However, capital expenditures are needed as the status quo is not sustainable. Now it is not whether, rather what changes are needed.
- Concerned within industry- undercurrent of members- any increase in compliance risk no matter how good it may be for security is a tough issue. Concerned the industry may vote against a new CIP because of cost implications. We need an outreach effort to National Public Utilities Commissions- by NERC. Mitigating security risks should also minimize "compliance risks" This will cost more money.
- As a result of recent NERC spot checks, the industry and the SDT are gaining a new appreciation for importance of words and their interpretation in the standards.
- Concerned industry will throw this back on us.
- Mr. Mosher noted that Gerry Cauley new CEO for NERC has championed an ad hoc committee on results-based standards and may be interested in developing a new format for how standards are developed and presented. Moving away from the compliance focus on the "right document" to real security issues. The test should be does the effort accomplish the underlying goal and intent of requirements. That should suffice.
- Probably not bringing the results-based effort into this project. This will be an ongoing effort. It will be a cultural change in NERC and the Regions that this is sensible way to process.
- State commissions are important outreach audience for NERC.
- The Trade Associations will do their best to provide context and the consequences as well as the big picture to their members. Each entity will ultimately decide where they are on this. We can't tell them how to vote, but we can provide information to inform their vote.
- Emphasis on getting it right this time? How will you know if you met this goal? How will you convince the skeptic in DC if you meet this?
- What about trials or pilots with entities? Is this still an idea in play? Having some since you've hit target.
- No exact way to know if you have it right. If you address some of these concepts- more objective, clear, deterministic and auditable, that will get us there.
- A substantial list of "wrongs" can help focus on the right thing to do.

- Concern that Industry won't accept the CIP as proposed. The industry needs to understand the consequences. We will have only one shot at this. More true now than before.
- Mr. Adamski noted that NERC President, Gerry Cauley has said this is among the top 3 things NERC needs to do.
- Spot check experiences suggest that there may be an unreasonable level of detail applied to enforcing current standards.
- Approve an increase in scope while compliance level of detail currently applied.
- We have seen an undue level of detail in policy documentation for CIP 003-R1- policy must support the requirements. Regional auditor went through every R looking for that. "All" does not appear in the requirement. Auditor used that tact.
- CIP 002- R3- critical cyber assets- e.g. given assets used in access control.
- CIP 004 issue- haven't provided in format the auditor wanted to see. Spreadsheet wasn't completed. Had all the info. This is an e.g. of audit and compliance out of control.
- Consider challenging finding of the audit? We have that process. One way to bring to attention of regional entity, NERC and FERC. Maybe indicate a problem with a standard.
- Can change to focus of the audit and how performed through the Version 4. As rest of standards become auditably compliant. Been on 14 CIP spot checks. In some suggested entities should do a better job of correlating.
- Trade association could help show that industry has valuable assets and they are trying to protect them.
- Trade associations are working together. 12 associations are marching together, educating various committees, various senators. Meeting weekly in Washington.
- Our focus should be on drafting standards- making them better- not on managing compliance risk. Focus on where we can make standards as clear as possible.
- Thanks for the help given. And support provided.

II. CIP 002-4 STRAWMAN DRAFT DOCUMENTS

A. Overview of CIP 002-4 Strawman Draft Documents

John Lim provided an overview of the work undertaken and the changes made to the CIP 002-4 draft documents between Orlando and Little Rock by a drafting group comprised of John Lim, Jackie Collett, Phil Huff and John Varnell. These included the CIP 002, the Guidance Document, the Introduction and Comment Form and the Control examples.

Dave Taylor noted that Howard Gugel from NERC will help the SDT get next products up to speed and be able to work with the SDT to answer any questions regarding format.

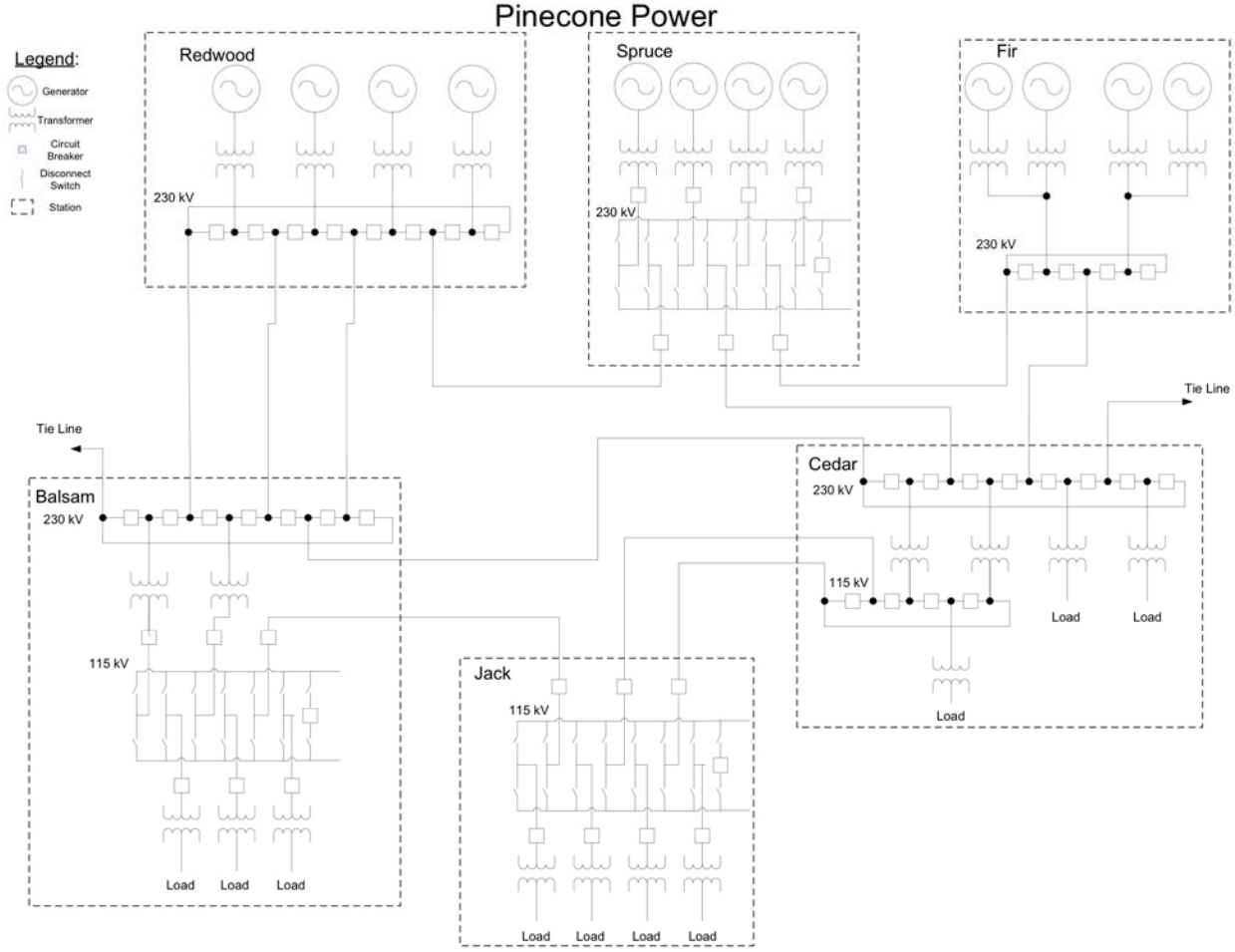
John summarized the following changes:

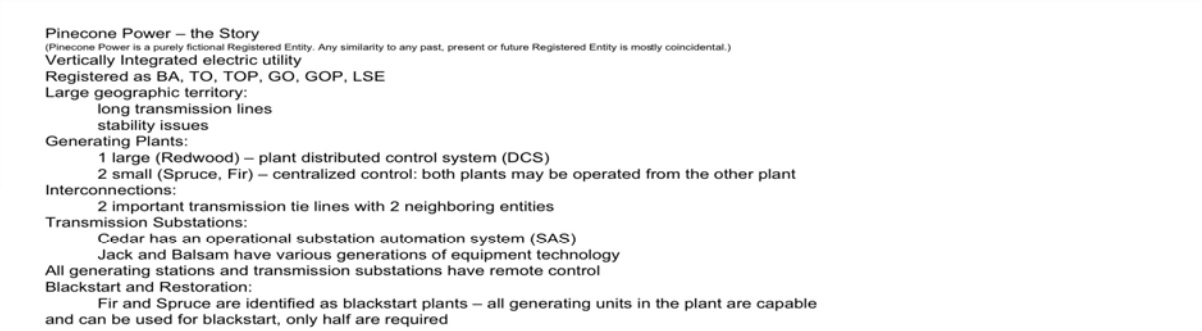
- A BES subsystem definition-
- Changed order of appendices. Harmonized- consistent use of terms.
- The list of the VSLs updated and some were put back in.

- The Guidance document has been refined and simplified with a 5-step process.
- We continue to need guidance in first two steps in categorizing BES subsystems.
- Agreed we will post as an "appendix" if ready.
- Highlights requirement. Tells the path to the development of the standards.
- Keith will be refining and cleaning up some examples for security controls as a stand alone document.

B. Walk-Through of CIP 002-4 Strawman Scenario

Jackie Collett provided an overview of the Pinecone Power "walk through" exercise.





Pinecone Power – the Story
(Pinecone Power is a purely fictional Registered Entity. Any similarity to any past, present or future Registered Entity is mostly coincidental.)
Vertically Integrated electric utility
Registered as BA, TO, TOP, GO, GOP, LSE
Large geographic territory:
long transmission lines
stability issues
Generating Plants:
1 large (Redwood) – plant distributed control system (DCS)
2 small (Spruce, Fir) – centralized control: both plants may be operated from the other plant
Interconnections:
2 important transmission tie lines with 2 neighboring entities
Transmission Substations:
Cedar has an operational substation automation system (SAS)
Jack and Balsam have various generations of equipment technology
All generating stations and transmission substations have remote control
Blackstart and Restoration:
Fir and Spruce are identified as blackstart plants – all generating units in the plant are capable and can be used for blackstart, only half are required

The SDT broke into two small groups and engaged in a "walk through" exercise that has been prepared by Jackie Collett, Dave Revill and other members. Following the breakouts, the SDT reviewed reflections on lessons learned from the walk through in terms of implications for improving or clarifying the CIP 002 draft.

1. **Possible Refinements to CIP-002-4**

- BES sub system definition - limitations <-> Reliability
- Clarify how to define BES sub system in requirements and/or guidance
- Determine Appendix 2 requirement in standard
- Clarify blackstart units that change - How to address this in requirements? "blackstart capable"
- Generating subsystems — define "Plant" — Units, combinations
- R1 — "Identify + Categorize"? vs. Categorize
- Keep cyber for R3? Not in R1 — rely on applying criteria
- How to address "combinations" in the subsystems? Start with cyber systems first?
- Appendix #2 "Must Identify" a requirement with appendix

2. **Key Issues — "Parking Lot" for Future Review**

- More detail on reliability functions to make operational — Address "Over Protection" issues — Map reliability functions to thresholds
- More specificity in reliability functions to allow entity to move description down in their operations — a cyber system may impact reliability but not the threshold — example a system

addressing operation awareness — make sure systems functions appropriately mapped to thresholds.

3. SDT Discussion Points from "Walk-Through"

- Did you identify the 7 generation subsystems? Some only came up with 6 but got to the right point. Will missing an interim step result in a severe impact?
- Goal is to categorize the cyber subsystems
- Careful we do not oversimplify categorization which may result in over protection — too many shortcuts could lead to incorrect conclusions
- Here is a cyber system — how many units does it impact - Look at megawatt total to set threshold of high-medium-low
- Think looking at units is the wrong path
- Break down to level of criteria you are evaluating — aggregation of megawatts at subsystem level— blackstarts would be at the unit level.
- Need a full assessment without requiring more work than is necessary
- Using generation subsystem across the board in the criteria — instead we may want to spell out generation subsystem or blackstart unit to make it clearer on to apply the criteria
- If pin down what we are talking about then replacing undefined subsystem with other terms that are undefined — new set of work to properly define and make sure each term properly used.
- We want to be sure nothing is missed — doesn't matter how it is defined if it is covered — then can choose to make it a subsystem but are not required to
- Give entities flexibility but careful don't leave an opportunity to game system by breaking systems into parts that stay below threshold for "high"
- No individual generator can determine full impact on system — that may require RC to determine but they will not want to do that task
- Clarify something in R3 — identify and categorize all BES subsystems ….. that means identify every part of cyber system that has anything to do with awareness function — is that what we meant?
- Every cyber system that performs that function should fall into one of the three categories, each with its own threshold
- How do you start — where do you get the list? Situational awareness is the universe of all cyber systems
- My take, we are saying you have to do the functions — which are BES cyber systems — every BES cyber system is at least a low based on the words we use here
- Maybe by extending the logic, you get around identifying subsystems — any system that can trigger specific levels
- Instead of starting with every cyber system — identify every cyber system that supports this BES subsystem

4. SDT Discussion of Next Steps in Drafting CIP 002-4

- Next steps in drafting?
- Build into R3 concept discussed in terms of the function of the BES subsystem
- Unclear where discussion of generation subsystem ended up — did not discuss transmission subsystems
- In criteria we can try to be more specific
- We may need to have very formal definitions we can put into the NERC glossary
- What is missing is what is the objective — should we try to introduce each requirement with the objective to help focus comments on what we are trying to do
- Can put that into the purpose statement to help clarify intent — that puts it into the standard — NERC has used those statements in the past to help in interpreting intent
- For the comment period, can we use statements as annotations to introduce a requirement?
- Scott read Maureen's revised purpose statement
- Members thought it sounded like she is trying to move to performance based standards, but this group may not be ready to do that given the limited time
- Adding more material may just draw comments on statements that will not be included in the end (relates to introducing requirement with intent comment)
- Suggesting a one-sentence introduction to clarify the intent and context of each requirement
- Could something be added to the comment form to set up the questions?
- Need more drafting input on appendix 2 — review the wording of the initial paragraph to avoid requirement language in the appendix

C. Remaining Issues

1. Small Group Work on Requirements # 1 and # 3.

Following the Walk Through, the SDT reviewed the remaining issues and agreed to work in the following Drafting Groups on Wednesday afternoon to address issues raised in the "Walk-Through" and bring back clarifications and refinements for consideration by the SDT.

- Group #1 Requirement #1 (*Jim Brenton, Jackie Collett, Keith Stouffer, Doug Johnson, Jeri Domingo Brewer, John Lim)* which reviewed and produced agreement on how to address the R1 and appendix issues raised in the walk through.
- Group #2: Requirement #3 drafting group (*Phil Huff, Jay Cribb, Frank Kim, Jon Stanford, Gerry Freese & Jeri Domingo Brewer)* How will this be understood- i.e. smaller unit is more secure than securing with a larger quantity. We are not trying to avoid protection; rather we are trying to determine how it affects the BES. Collectively assets may have a higher impact than one large asset.

At the end of the day, the SDT reviewed progress and noted the following assignments:

- Issues of reliability functions— Phil Huff noted a plan to meet for dinner and resolve these issues and bring suggestions back tomorrow first thing tomorrow.
- Break into groups for document drafting (introduction and comment form; CIP 002-4; Guidance Document; Appendices; and Sample Controls.

Chair reminded the SDT that the goal is to ensure posting for informal industry review and the SDT should expect many suggestions back from industry. She also checked with the SDT to see if there were any red flags on proposed list of FERC specific directives in 706 since it will be part of the NERC filing at the end of December. The SDT concurred with the list.

2. Definition of Terms

On the second day John Lim reviewed with the SDT the revised definitions of terms used in standard noting:

- #3 Bulk Electric System spelled out.
- generation subsystem turned from a bulleted list into a paragraph.
- transmission subsystem defined more specifically
- control system, second bullet added the qualifier "for the support of real-time operations"
- 7, 8 & 9 — changed to "BES" to be consistent — 9 adds Low BES impact

SDT Discussion of Proposed Changes to Definitions

- All the other bulleted lists turned into paragraphs — Is #9 the only bulleted list?
- #8 — does "medium" capture everything?
- High, medium and low are not intended to be used to capture categories but criteria — pulled from risk factors — be sure not to use definitions to apply categorization — does defining a term here make it apply in the standards?
- If leave it in then indicate how they are to assess the high, medium and low.
- Do we want them here in definitions versus in the attachment?
- Let the attachment determine rather than define them?
- Inclined to take it out of the definitions — this issue is even fluid at NERC — leave it in the attachment.
- Define here and reference the attachment? If put in to the standard, once adopted it goes into the glossary.
- Bring definition up to a higher level with the detail in the attachment?
- Is there an inconsistency between this and the mapping? What is wrong with this definition? Conflicts with the mapping, according to the definition here everything is high or medium, and nothing is low — everything affects the BES.
- Cannot read the bullets alone — have to read in context of lead-in language.
- All of them affect the system — the question is only how much they affect the system.

- Define BES impact — then categorize that with high, medium and low as degrees for measuring the impact.
- Suggestion changing "direct" to "adversely" in each bullet.
- Either simplify this or do not make missing one a high VSL — too complex to make it a high VSL if you miss one.
- High VSL is related to the importance of missing one rather than the complexity of the standard.
- Make sure we have the detail in each thing we are doing — make it too simple then people will complain it is ambiguous.
- Last sentence of Generation subsystem — confusing with a transmission issue — consider adding "... shared generation element …"
- What is a "generation element" — both generation and element are separate defined items — is this just the generator?
- Non-capital "generation" simply describes "Element" — the latter is a defined item, the former is not.
- Elements at a generation yard, etc. — clarify that we are not talking about something that doesn't spin.
- Is the last "or…" clause intended to capture something not already captured in the cyber system definition?
- Jackie Collett's revised definitions of Generation and Transmission Subsystems — review — it is a little wordy but it is more specific — included transmission substations in the later definition
- "Combinations of generation systems"? — not clear what that covers — could be more open than needed — need a qualifier for "combinations"
- Strike the last section of the first sentence — add "or" — should read "Generation plants or individual generation units … a transmission system."
- I don't understand the second sentence — how would it be applied?
- Combine the last two sections into a final separate sentence?
- Does generation plant mean everything inside the fence? Thought we had dropped that?
- Put in as part of the walk through review yesterday — the "or" gives the entity a choice
- Are elements in the second sentence already covered in the first? Or do we need the first sentence if the elements are covered in the second?
- In terms of the definition, is it redundant? Start with the second sentence?
- Concerned we may miss something if we take the first sentence out — would rather be redundant than miss something
- Transmission definition is closely parallel with generation — same issues — consider issues for both, move on for now and come back to this one.

3. Review of Changes to Standards Section

Phil Huff led the SDT through a discussion of the changes to the standards section.

- **R-1.** Purpose statement — shorter, more focused
- Identifying cyber security framework or the devices that require security?
- Consider just using the last paragraph of the previous definition version
- Up in the title — strike "identification and" — just categorizing, not identifying — remove "identification" in the purpose too
- Add "functions critical to the reliable operation" to the Purpose to be consistent
- Strike first set of words and start with "categorization" to make it a purpose statement rather than a requirement statement — start with "To categorize and document the BES …"
- #3 Applicability
- #4 Physical Facilities

  Insert "and are not under NRC cyber security regulations" at the end?
- Suggest not adding yet due to ongoing discussion of jurisdiction — balance of plant is still under NERC — following comment period the jurisdiction issue may be clarified — may get comments form nuclear guys.
- R1- Drop "serves" in first sentence "…BES subsystems provides a measure …"
- Add "...potential impact that its …"
- "Approved engineering evaluation" required? (in middle sentence) Method has to be approved but not every yearly evaluation is approved.
- Second sentence is long and wordy tighten up, along with the third sentence — if we can get agreement on the elements.
- Fiscal responsibility is with the owner — some facilities have multiple owners (by percentages) asking all owners to make the assessment?
- Who signs compliance? Operator not always the one who can ensure compliance — some plants have a contract operator — need to include "operators and owners" Owners should "ensure" — put them on the hook to make it happen.
- Reduce wording by striking "categorize all BES subsystems they own: and own …"
- The responsibility issue is a registration issue.
- Joint ownership issue is not new — how do we do this in the other standards? What is the language we used? We used to have a definition of "responsible entity" but stripped it out — the idea is be clearer about responsibility — spell out the entities in each requirement — some requirements may not be mapped to entities (?) — may have to go back through and clarify responsibilities
- R1 final sentence: "could affect" is too mushy, too uncertain
- Some want to put the "annual" requirement back in and some who want to take it out.

- TPO requirements call for "annual" evaluation. Need to make clear what we mean by "annual." The issue of "annual" appears in multiple places and on multiple projects. Need to be sure it is applied as part of review process — may want to wait for comments.
- **SDT Poll support for reinstating "annual" term in the standard for draft for comment: Yes — 8, No — 10. Won't reinstate for CIP 002-4 draft.**
- **R2-** Notification from generation to transmission side of the house a "high"?
- How does generation subsystem owner learn he has a high or medium? By definition or someone (reliability coordinator) tells him?
- Needs to be a clearer delineation of notice, and should be a "high" responsibility
- The owner has to determine through criteria, not the reliability coordinator who do not have any special ability in this area
- Look at attachment 1 — there are instances when owner operator will be notified — it is not just one or the other
- This is one of the places that industry has a problem — not enough of a bright line — owner/operator may not have enough data to assess
- "adjacent"? Replace with "connected to"? And specify the within 30 days is from R4?
- Adjacent is physical proximity — connected is the better word
- Add "…within 30 days of the approval date of the categorization …"
- Change "connected" to "directly interconnected"
- Why include "Senior Manager"? Addressed FERC directive. Need to look at the order — careful not to do more than is requested in the order.
- Is there a definition of "Senior Manager"?
- Why thirty days? Seems lengthy and arbitrary
- R4 already has the language of who approves — drop it here
- Is R4 necessary if we are dropping Senior Manager? Address when review that section.
- Suggest "within 30 days of the categorization" - 30 days is not too long to get ducks in a row.
- Violation risk factor should be "high".
- In R2 can we make it a "secured notification"? Define "secured"?
- Back to R1 to review revisions
- Do we have to list them all to add clarity to the definition? Add load serving entity and reliability coordinator.
- Need to go back and see what the functional model says — or post all and ask which entities do not belong — alternatively list all entities in 4.1 except NERC and Regional Entities
- Requiring reliability coordinator to assess others systems — goes back to ownership — reliability coordinator has no special skills to assess cyber security systems
- Can we change to cover own and operate?

- Is the control center considered a subsystem? If yes, as part of the BES subsystem, it is not clear hear where it is covered
- Put into the definition of control center that it may be a part of the BES subsystem
- In definition of BES Subsystem include "BES Facilities (i.e., Generation Subsystem, Transmission Subsystem, and Control Center)…"
- **R3**. Phil Huff reviewed revisions with the SDT
- 2nd sentence — do we need the final clause?
- Is our intent to identify or to categorize? Intentionally pulled "identify" out of R1 — are we being consistent?
- Remove "as those …" replace with "associated with" — also "Responsible Entities shall categorize" and put "… categorized in R1..."
- Planning function is both and internal and external — copy "… as part of the planning, including coordination with neighbors," from the R1 revision and use here too.
- Not requiring notification of our neighbors?
- Delete the final sentence? Not part of the security but better as part of control.
- Are we overloading the meaning of the term "planning" — we used it in sentence above with the normal NERC definition.
- Beginning of second sentence — Functional Entities and again in third and fourth sentences rather than Responsible Entities —
- Functional doesn't work here — need to go back to responsible.
- Need to capture changes in BES subsystems as well as BES cyber subsystems
- **R4**. Is the senior manager the right one for this role? If not, then does this requirement do much? Support removing.
- If remove, are we removing responsibility for person knowing what was happening.
- Despite the language in the FERC order paragraph 294, I think FERC would still want senior manager here explicitly because we have changed the process since their original request — I suggest leaving R4 in.
- Change "shall approve by written and dated signature" to match order "shall annually review and approve"
- The point was to establish a fiduciary duty to take responsibility and make a knowing effort to establish what was and what was not covered — now we have said everything is covered, but at three different levels.
- Approving additions or improvements to the system or annually reviewing the whole system?
- Ask in the comment form whether we need this requirement?
- Here we have prescribed the methodology — we responded to the order by changing the methodology.
- If we put it out as a question we need to get a response from FERC too

- FERC asked us to address regardless of the industry comment
- Leave it for industry comment and pose question for clarification with FERC
- Does senior manager necessary mean corporate office?
- This section is about categorizing assets, not putting in weak controls better addressed in 003-009
- My advice from other standards — if remove, better be sure you have a clear rational and suggestion of how it will be dealt with
- We need to be rethinking here and my concern is the senior manager shall is a weak control in the wrong place
- Intent of pulling senior manager into the process is to give it the attention it needs — establishes accountability as to what needs to be protected to big with — controls will be addressed next year
- This says the right thing, maybe in the wrong place, but pulling it out of here now will result in perception we are not addressing the issue
- Violent agreement on importance — question is where? It magically appears in R2 as a capitalized item without definition in R1.
- Three thoughts: any of these acceptable? (rather than one or the other).

  Members offer the following responses (multiple votes were permitted):

  - Remove it, address it elsewhere: 10 votes
  - Keep in R2 but with fuller definition: 9 votes
  - Keep it here as is: 7 votes
  - Remove here and keep in the comment form: 1 vote

  Members then offered the following preference polling *(only one vote of one of 3 options)*

  - **Remove it, address it elsewhere: 8**
  - **Keep in R2 but with fuller definition: 5**
  - **Keep it here as is: 1**
- There is consensus of the importance of the issue and inclusion of the senior manager but less clear how best to do it.
- Since removing it here now, need to clarify why
- Back up in R3- Strike "responsible entity shall" and rest of the last sentence. Still needs a tie back to R1 —

4. Review of the Revised Definitions for BES, Generation and Transmission Subsystems

- Still questions about discussions by nuclear industry and the impact on these definitions
- Definitions 7, 8 & 9 — High, Medium & Low
- Consider reorganizing the criteria based on H-M-L and by generation/transmission
- Remove "details provided in appendix 1" — put in above #7 — re-label as "attachment"

- Don't put that language in the definitions — it will be lost once adopted and moved into the glossary — each will stand alone in the glossary
- Not meant to be a part of the definition but rather to help clarify and explain for purposes of the comment period
- May need to consider for the next round given our time constraint today
- This doesn't include malicious use of the equipment, not just lost
- Doesn't matter if loss is by natural or malicious means — source of loss doesn't matter
- Perhaps include "misused"
- Need a more clear cut, declarative sentence
- These terms will be used independent of CIP 002
- Rewrite to be declarative: "BES Subsystems, that if destroyed….would have a severe….change #8 and #9 accordingly
- Concerned about "destroyed", etc. — concerned about availability — remove adjectives — doesn't matter how they are rendered unavailable — simply substitute "rendered unavailable"
- It is more than just availability — integrity matters too in cyber security
- Just looking at BES, not cyber security yet
- Need "misuse" — adds more than just availability — "that if misused, degraded or otherwise rendered unavailable…"
- Need to be describing the impact to the BES
- For now go with suggestion to go with previously adopted language — put the issue into the parking lot for future work

5. Compliance

- No changes were made to this section.

6. VSLs

- #1
- Made consist or conformed with discussions and changes made earlier today
- Still concerned with high impact given a severe VSL for not having categorized or mis-categorized
- Whole point in attachment and drawing bright lines is to limit auditor opinions on categorization
- Concern is with definition of subsystems
- We are only left with categorization — only have to categorize rather than identify subsystems
- In severe VSL — kill the phrase after "or" and put a period after "categorized" in all four levels?
- Just eliminate "identify" — retain the rest
- Should say has failed to start the process

- If you missed any single one by saying there are six subsystems and someone else says there are seven — am I then in severe VSL?
- Alternative: "The responsible entity has not categorized any BES subsystems it owns". Support for this language — Yes/13, No/1
- **#2**
- Too wordy — repeat high and medium impact at the beginnings and ends — could strike first half of each.
- Only two ways to miss — not notify or notify late
- **#4** — already removed

7. Attachments

- 1.3 — ok
- 1.8 — ok
- 1.15- Interchange coordinator, transmission service provider, load service provider, selling entity, etc. all have real time function responsibilities — none of them will be caught by 1.15?
- Can we expand 1.7, 1.10 or 1.11 to cover that omission — put control center functions into those three

8. Other Changes?

- What did we do with the requirement for VSL 2? Everyone agreed with concept just need appropriate language

D. Motion to approve CIP 002-4 with identified and agreed upon changes
Gerry Freese moved, John Varnell seconded

All in favor: **16** *(Frank Kim, Doug Johnson, Sharon Edwards, Gerry Freese, Jay Cribb, Keith Stouffer, Jon Stanford, Jim Brenton, John Lim, Jeri Domingo-Brewer, Phil Huff, Joe Doetzl, Rob Antonishen, John Varnell, Jackie Collett and Kevin Sherlin)*
Opposed: **0**
Abstain: **1** (Dave Norton)

E. Harmonizing the Comment Form and Guidance Documents

Following a break, the SDT broke into separate "document" groups to harmonize the comment form and guidance document with the adopted CIP 002-4:

- **Introduction and Comment Form**: (Frank Kim, Jay Cribb, Jon Stanford, Jim Brenton, Jeri Domingo-Brewer, John Lim, and Keith Stouffer, Jackie Collett, Dave Norton, John Varnell and Rob Antonishen)
- **Guidance Document**: (Phil Huff, Gerry Freese and Doug Johnson).

At the conclusion of the small group refinements to these documents the SDT reviewed the following key issues for the future (i.e. "parking lot")

- More detail on reliability functions to make operational — address "over protection" issues — map Requirement Function to thresholds
- "Controls" — "secure" defined — address in 003-009
- "BES Subsystem Impacts" define going forward (high/medium/low)
- 1.7, 1.11 & 1.15 — control center function issues)

IV. NEXT STEPS

The SDT Chair and Vice Chairs reviewed with the Team the work plan going forward including the need to make progress on the security controls (CIP 003-009) at the SDT's January meeting in Tucker, Georgia. The chair thanked Phil Huff for hosting the meeting and providing excellent food and facilities.

The SDT adjourned at 3:30 p.m. on December 16, 2009.

Appendix # 1— Meeting Agenda

NOTE:

1. Agenda Times May be Adjusted as Needed during the Meeting
2. Document Drafting Group Meetings May Not Have Access to Telephones and Ready-Talk

Proposed Meeting Objectives and Outcomes

- Receive an overview the CIP 002-4 document drafting progress
- Conduct a walk-through of the CIP 002-4 and identify lessons learned and any changes needed in the document(s).
- Review CIP 002-4 Key Issues and Provide Guidance to Document Drafting Groups
- Convene CIP 002-4 Document Drafting Groups
- Review and refine Document Drafting Group products
- Compile, review and refine the draft CIP 002-4 and related documents
- Adopt the CIP-002-4 Documents for Posting
- Review CSO 706 SDT leadership changes
- Review the 2010 Schedule and agree on next steps and assignments

Tuesday	**December 15, 2009**
8:00 a.m.	Welcome and Opening Remarks- *Jeri Domingo Brewer, Phil Huff & John Lim* Roll Call; NERC Antitrust Compliance Guidelines Facilitator review and SDT acceptance of November 16-19 Orlando SDT meeting summary
8:15	Review of Meeting Objectives, Agenda and Meeting Guidelines- *Bob Jones*
8:20	Review of SDT 706 Work plan- December- June, 2009- *Jeri Domingo Brewer*
8:50	Overview of CIP 002-4 Strawman Draft Documents, Format and Key Remaining Issues and Challenges- *John Lim et al.*
9:15	Walk Through of CIP 002-4 Strawman Scenario-*Jackie Collett, Dave Revill et al.*
10:30	*Break*
10:45	Reflections and Lessons Learned from Walk Through and Implications for the Draft
11:15	Run-through and Flag Key Remaining Issues in CIP Version 4 Strawman Documents
12:15	*Lunch*
12:45	Review of Remaining Issues and Proposal for Drafting Groups
1:00	Drafting Group Meetings
4:00	Drafting Group Reports and Identification of any Outstanding Issues and Drafting Assignments
5:30	*Recess*

Wednesday	**December 16, 2009**
8:00	Welcome and Agenda Review- *Jeri Domingo-Brewer, Phil Huff & John Lim*
8:10	Update on Status of Version 3 CIP—*Scott Mix*
8:15	Update on Technical Feasibility Exception (TFE) NERC Rules of Procedure —*Scott Mix*
8:20	Update on VSLs/VRFs- *Scott Mix*
8:25	Update on other related cyber security initiatives- *SDT Members*
8:30	Reconvene SDT CIP 002-4 Document Drafting Groups *(as needed)*

10:30	Break
10:45	Final Document Review and Consensus Testing on Resolution Key Remaining Issues
12:00	*Working Lunch (compilation of refined CIP 002 documents)*
12:45	Review of CSO 706 SDT Leadership Changes
1:00	Final Document Review and Consensus Testing on Resolution Key Remaining Issues
3:00	*Break*
3:15	Final Document Review and Motion to Adopt as Refined for Industry Posting
4:30	Review and Agree on CIP 002-4 Next Steps and January- June Work plan and Schedule • Meeting Evaluation
5:00	*Adjourn*

Appendix # 2 Attendees List

Attending in Person — SDT Members and Staff

1. Jeri Domingo-Brewer, Chair	U.S. Bureau of Reclamation
2. Jim Brenton	ERCOT
3. Jay S. Cribb	Information Security Analyst, Southern Company Services
4. Sharon Edwards	Duke Energy
5. Gerald S. Freese	Director, Enterprise Info. Security America Electric Pwr.
6. Phillip Huff, Vice Chair	Arkansas Electric Coop Corporation
7. Doug Johnson	Exelon Corporation — Commonwealth Edison
8. Frank Kim	Ontario Hydro
9. Rich Kinas	Orlando Utilities Commission (Wed)
10. John Lim, Vice Chair	CISSP, Department Manager, Consolidated Edison Co. NY
11. Jonathan Stanford	Bonneville Power Administration
12.Keith Stouffer	National Institute of Standards & Technology
Roger Lampila	NERC
Scott Mix	NERC
Dave Taylor	NERC
Howard Gugel	NERC
Lauren Koller	
Joe Bucciero	NERC/Bucciero Consulting, LLC
Robert Jones	FSU/FCRC Consensus Center
Hal Beardal	FSU/FCRC Consensus Center
Stuart Langton	FSU/FCRC Consensus Center
Gerry Adamski	NERC (Wed.)

SDT Members Attending via Ready Talk and Phone

13. Rob Antonishen	Ontario Power Generation (Thurs)
14. Jackie Collett	Manitoba Hydro (Wed/Thurs)
15. Joe Doetzl	Manager, Information Security, Kansas City Pwr. & Light Co. (Thurs.)
16. Rich Kinas	Orlando Utilities Commission (Wed.)
17. David Norton	Entergy (Wed. Thurs)
18. Kevin Sherlin	Sacramento Municipal Utility District (Wed. Thurs.)
19. John D. Varnell	Technology Director, Tenaska Power Services Co. (Wed. Thurs)

SDT Members Unable to Attend

Christopher A. Peters	ICF International
Scott Rosenberger	Luminant Energy
David S. Revill	Georgia Transmission Corporation
William Winters	Arizona Public Service, Inc. (Mon., Tues, Thurs)

Others Attending in Person

Alan Mosher	APPA
Barry Lawson	NRECA

Others Attending via WebEx and Phone

Rob Hardiman	Southern Company Transmission
Joseph Baxter	AECI
Justin Kelly	FERC
Justin Kelly	FERC
Michael Toecker	Burns and MacDonald Engineering
Bill Glynn	Westar Energy
Sam Merrell	Cert
Rob Wotherspoon	Orlando Utility Commission
Michael Fischette	LBWL
Laurel Moll	Orlando Utility Commission

Appendix # 4 — NERC Antitrust Compliance Guidelines

I. General

It is NERC's policy and practice to obey the antitrust laws and to avoid all conduct that unreasonably restrains competition. This policy requires the avoidance of any conduct that violates, or that might appear to violate, the antitrust laws. Among other things, the antitrust laws forbid any agreement between or among competitors regarding prices, availability of service, product design, terms of sale, division of markets, allocation of customers or any other activity that unreasonably restrains competition.

It is the responsibility of every NERC participant and employee who may in any way affect NERC's compliance with the antitrust laws to carry out this commitment.

Antitrust laws are complex and subject to court interpretation that can vary over time and from one court to another. The purpose of these guidelines is to alert NERC participants and employees to potential antitrust problems and to set forth policies to be followed with respect to activities that may involve antitrust considerations. In some instances, the NERC policy contained in these guidelines is stricter than the applicable antitrust laws. Any NERC participant or employee who is uncertain about the legal ramifications of a particular course of conduct or who has doubts or concerns about whether NERC's antitrust compliance policy is implicated in any situation should consult NERC's General Counsel immediately.

II. Prohibited Activities

Participants in NERC activities (including those of its committees and Subroups) should refrain from the following when acting in their capacity as participants in NERC activities (e.g., at NERC meetings, conference calls and in informal discussions):

- Discussions involving pricing information, especially margin (profit) and internal cost information and participants' expectations as to their future prices or internal costs.
- Discussions of a participant's marketing strategies.
- Discussions regarding how customers and geographical areas are to be divided among competitors.
- Discussions concerning the exclusion of competitors from markets.
- Discussions concerning boycotting or group refusals to deal with competitors, vendors or suppliers.

III. Activities That Are Permitted

From time to time decisions or actions of NERC (including those of its committees and Subgroups) may have a negative impact on particular entities and thus in that sense adversely impact competition. Decisions and actions by NERC (including its committees and Subgroups) should only be undertaken for the purpose of promoting and maintaining the reliability and adequacy of the bulk power system. If you do not have a legitimate purpose consistent with this objective for discussing a matter, please refrain from discussing the matter during NERC meetings and in other NERC-related communications.

You should also ensure that NERC procedures, including those set forth in NERC's Certificate of Incorporation and Bylaws are followed in conducting NERC business. Other NERC procedures that may be applicable to a particular NERC activity include the following:

- Reliability Standards Process Manual
- Organization and Procedures Manual for the NERC Standing Committees

- System Operator Certification Program

In addition, all discussions in NERC meetings and other NERC-related communications should be within the scope of the mandate for or assignment to the particular NERC committee or Subgroup, as well as within the scope of the published agenda for the meeting.

No decisions should be made nor any actions taken in NERC activities for the purpose of giving an industry participant or group of participants a competitive advantage over other participants. In particular, decisions with respect to setting, revising, or assessing compliance with NERC reliability standards should not be influenced by anti-competitive motivations.

Subject to the foregoing restrictions, participants in NERC activities may discuss:

- Reliability matters relating to the bulk power system, including operation and planning matters such as establishing or revising reliability standards, special operating procedures, operating transfer capabilities, and plans for new facilities.
- Matters relating to the impact of reliability standards for the bulk power system on electricity markets and the impact of electricity market operations on the reliability of the bulk power system.
- Proposed filings or other communications with state or federal regulatory authorities or other governmental entities.
- Matters relating to the internal governance, management and operation of NERC, such as nominations for vacant committee positions, budgeting and assessments, and employment matters; and procedural matters such as planning and scheduling meetings.

Any other matters that do not clearly fall within these guidelines should be reviewed with NERC's General Counsel before being discussed.

APPENDIX # 4 Meeting Schedule

OCTOBER 2008—DECEMBER 2010

DEVELOPMENT OF CIP VERSION 2 AND NEW VERSION FRAMEWORK
OCTOBER 2008—JULY 2009

1. October 6–7, 2008 — Gaithersburg, MD Reviewed CIP-002-CIP-009, Agreed on Version 2 approach.

2. October 20–21 —Sacramento, CA CIP-002-CIP-009 Version 2 development

3. November 12–14, 2008 — Little Rock, AR CIP-002-CIP-009 Version 2 adoption for comment and balloting; CIP-002-CIP-009 New Version process reviewed.

4. December 4–5, 2008 — Washington D.C. CIP-002-CIP-009 Version 3 reviewed and debated, SDT member white "working" papers assigned, Technical Feasibility Exceptions white paper reviewed and refined.

5. January 7–9 — Phoenix, AZ, Reviewed Technical Feasibility Exceptions white paper**,** reviewed industry comments on CIP-002-CIP-009 Version 2 products — established small groups to draft responses, reviewed New Version white "working" papers.

- January 15 — WebEx meeting(s) Small group drafted responses to industry Version 2 comments.
- January 21 — WebEx meeting(s) Small group drafted responses to industry Version 2 comments.

6. February 2–4, 2009 — Phoenix, AZ Update on NERC Technical Feasibility Exceptions process**,** VSL process and SDT role**,** review of Version 3 White papers, strawman and principles**,** reviewed and adopted SDT responses to industry comments on Version 2 and Version 2 Product Revisions.

7. February 18–19, 2009 — Fairfax, VA Update on Version 2 process**,** NERC TFE process and VSL Team process; reviewed, discussed and refined Version 3 CIP-002 White papers, strawman, and principles.

8. March 10–11, 2009 — Orlando, FL Update on NERC TFE and VSL and VRF Team process and review and refine Version 3 CIP-002 Strawman Proposals

- *March 2–April 1, 2009 — 30-day Pre Ballot*
- *Mid-March — NERC posts TFE draft Rules of Procedure for industry comment*
- *March 30, 2009 — WebEx meeting(s) White Paper Drafting Team*
- ***April 1–10 — NERC Balloting on Version 2 Products***
- *April 6, 2009 — WebEx meeting — White Paper Drafting Team*
- *April 8, 2009 — WebEx meeting(s) — White Paper Preview- Full SDT Conference Call*
- *April 11, 2009 — Version 2 Ballot Results (Quorum: 91.90% Approval: 84.06%) and Industry Comments*

9. April 14–16, 2009 — Charlotte NC Update on NERC TFE process, VSL Team process and NERC Critical Assets Survey; agreed and adopted responses for Version 2 industry comments for recirculation ballot; reviewed and refined Version 3 whitepaper and consensus points and progress report to NERC Member Representative Committee (MRC) May meeting.

- *April 28 and May 6, 2009 — White Paper Drafting Team Meetings and WebEx*
- *April 17–27, 2009 — Recirculation Results: Quorum: 94.37% Approval: 88.32%*

- *May 5, 2009 — NERC MRC Meeting, Arlington, VA- SDT progress report.*

10. May 13–14, 2009 — Boulder City NV Reviewed MRC presentation and further SDT refinement and discussion of the Version 3 White Paper.
June 8 and June 15, 2009 — Working Paper Drafting Team Meetings and WebEx

11. June 17–18, 2009 — Portland OR Further SDT refinement of the draft CIP Version 3 Working Paper(s), reviewed SDT development process for June-December 2009; discussed potential SDT subcommittee structure and deliverables.

- *June — WebEx meeting(s)*
- *Working Paper drafting group sessions including inputs from selected industry personnel to help establish BES categorization criteria*

CIP-002 DEVELOPMENT OF REQUIREMENTS, MEASURES, ETC. JULY-DECEMBER 2009

12. July 13–14, 2009 in Vancouver, B.C., Canada
SDT reviewed, refined, and adopted SDT Working Paper. SDT adopted its response to NERC for Interpretation of CIP-006-1. SDT reviewed and adopted a proposal for CIP-002 Subgroups and Deliverables and convened subgroup organizational meetings to develop work plans. SDT adopted 2010 Meeting Schedule.

- *July–August Interim Conference call meeting(s)*
- *CIP-002 Subgroup meetings*
- *CIP-002 Coordination Team meeting*
- *August 3–5, 2009 in Winnipeg, Manitoba **NERC Member Representative Committee**. Progress Report and presentation on new CIP Version 3 Working Paper-Concept- Reliability Standards on Cyber Security for MRC input.*

13. August 20–21, 2009 in Charlotte, NC. SDT reviewed and responded to MRC input on Working Paper/CIP-002 Concepts and convened SDT Subgroup and plenary meetings to develop CIP-002 requirements and "proof of concept" control (s).

- *July–September — 45-day Industry Comment Period on CIP-002 Concept Working Paper*
- *NERC Webinar- August–September Interim Conference Call meeting(s)*
- *CIP-002 Subgroup meetings (as ne*
- *CIP-002 Coordination Team meeting*

14. September 9–10, 2009 in Folsom, CA. SDT reviewed and considered industry comments on the Working Paper and CIP-002 concepts and their application to the subgroup work and addressed coordinating issues through joint subgroup meetings. SDT agreed on meeting dates and proposed locations for January–December 2010
September–October Interim WebEx meeting(s)

- *FERC Version 3 Urgent Action SDT conference call meetings*
- *CIP-002 Coordination Team meeting*

CIP VERSION 3 RESPONSE TO FERC ORDER, OCTOBER-DECEMBER, 2009

15. October 20–22, 2009 in Kansas City, MI. Reviewed new FERC Order and urgent action CIP Version 3 process; discussed key issues raised by SDT CIP 002 Subgroups, small group meetings and agreement on refinements to the CIP 002-009 schedule and drafting process for CIP 002-4.

- *October–November Drafting Team meeting(s)*
- *CIP-002 Coordination Team meeting*

16. November 16–19, 2009 in Orlando, FL

- SDT review, refine and adopt Version 3 "industry response" document.
- SDT plenary and drafting group session(s) — to draft, review and refine CIP-002-4 standard, requirements, measures and controls and related documents.
- November–December Interim Conference call meeting(s)
- Drafting teams as needed to finalize draft CIP 002-4 documents
- CIP-002 Coordination Team meeting
- *CIP 002-4 Drafting Team produces next draft based on Orlando Meeting input.*
- *December 2 CSO 706 SDT Version 3 Consideration of Comments Draft Conference Call*
- *December X, CSO 706 SDT CIP 002-4 Preview Conference Call*

17. December 15–16, 2009 in Little Rock AK

- SDT scenario "walk through" to test flow of CIP 002-4.
- SDT plenary and drafting group session(s) to review, refine, and agree on and adopt CIP-002 standard, requirements, measures and controls and related documents.
- Agree on initial posting of draft CIP-002 for industry review and comment.
- Agree on next steps and 2010 Work plan and schedule

Refinement and Adoption of CIP-002 Version 4 and Development and Adoption of CIP Standards (003-009)
January 2010–December 2010

18. January 19-20–21-22 — Tue-PM- to Friday AM, Tucker, GA (GTC)

- SDT Work on Developing CIP 003-009 Strawman Drafts

19. February 17-18–19 —Wed--Thursday –Friday, Austin TX (ERCOT)

- SDT Reviews Industry Comments and Refines CIP 002 for posting for 45-day industry formal comment period.
- SDT continues CIP 003-009 Strawman Drafts

20. March 9–10-11 — Tuesday–Thursday, Phoenix, AZ (APS)

- SDT continues CIP 003-009 Strawman Drafts

21. April 13-14–15 — Tue-Wednesday–Thursday, Atlanta GA (Southern Co)

- SDT Reviews and Responds to Industry Comments, Refines and Adopts CIP 002 for balloting
- SDT posts a draft CIP 003-009 for informal industry comment.

22. May 11-12–13 — Tue-Wednesday–Thursday, Dallas TX (Luminant)

- SDT reviews Industry 1st Ballot Comments and Drafts Responses
- SDT reviews CIP 003-009 informal industry comments and refines the draft.

23. June 8-10- Tues, Wed. Thursday- (Sacramento)

- SDT refines CIP 003-009 and posts for 2nd round of informal industry comments and refines the draft.

24. July 13-14–15, Tue-Wednesday–Thursday, Pittsburgh, PA (CERT)

- SDT reviews CIP 003-009 informal industry comments and refines the draft.

25. August 10-11–12, Tue-Wednesday–Thursday- TBD

- SDT refines CIP 003-009 and posts for formal 45 day industry comment

26. September 7,8,9, Tues-Thurs. TBD (if needed)

27. Oct. 12-13–14, Tue-Wednesday–Thursday- TBD

- SDT Reviews and Responds to Industry Comments, Refines and Adopts CIP 002 for balloting

28. November 16-17–18, Tue-Wednesday–Thursday- TBD

- SDT reviews Industry 1st Ballot Comments and Drafts Responses

29. December 14-15–16, Tue-Wednesday–Thursday- TBD

Appendix # 6 Trade Association Memorandum to SDT

December 10, 2009

TO: NERC CSO706 Critical Infrastructure Protection Standard Drafting Team

FROM: American Public Power Association, Edison Electric Institute, Electricity Consumers Resource Council, Electric Power Supply Association, and National Rural Electric Cooperative Association (the "Associations")

SUBJECT: Support for Expedited Revision of NERC Cyber-Security Standards

On behalf of our Associations, we want to express our support of efforts now under way by the CSO706 Standard Drafting Team to expedite development of a revised set of cyber-security reliability standards, including consideration of a tiered approach to the identification of bulk electric system ("BES") assets under CIP-002-4. We understand that assets within each BES tier will in turn be subject to a new suite of cyber-security controls developed under reliability standards CIP-003-4 through CIP-009-4.

As you know, Congress and the Executive Branch have identified cyber-security of the nation's critical infrastructures as essential to the protection of the public welfare, national security and national economic security. Therefore, NERC and the industry now have the opportunity to demonstrate the value of industry expert participation and the effectiveness of industry self-regulation by delivering a timely set of consensus critical asset identification parameters. The Associations believe a new, more systematic approach to asset classification will best ensure that BES assets are subject to the appropriate cyber-security protection controls that are commensurate with their importance to reliable operations and their vulnerability to cyber-security threats.

The Associations are committed to working with their members' executives and managers, to ensure that industry subject matter experts provide timely and constructive comments on the scheduled December 28, 2009 posting of Version 4 of CIP-002, and subsequent balloting. We recognize the difficulty of drafting during the holiday season, the tight time frame for conducting a thorough revision on matters involving complex technical issues, and the prospect that this process could invoke considerable tension and disagreement on a broad range of issues. However, we offer our support because we believe it is important that the industry reach consensus on CIP-002-4 during the next six months and deliver a full suite of cyber-security

standards for approval by the NERC Board of Trustees by the end of 2010. Consequently, it is imperative that the identification piece of the process starts well, and remains on track.

The Associations recognize that there may be several alternative approaches for defining applicability of the standards. If approved as reflected in the conceptual framework, the tiered approach to BES asset identification would be a significant departure from the current approach to critical asset and critical cyber-security asset identification. Reaching an industry consensus in support of a new conceptual framework and developing a clear, complete and enforceable set of reliability requirements on an aggressive timeline will be difficult at best. Implementing a new framework raises significant cost implications that must be addressed as well. However, given the importance of the role cyber-security plays in ensuring a safe and reliable electric system, the work of your drafting team is in our view a crucial NERC project.

Therefore, we offer our strong support for the expedited timeline and consideration of the tiered approach and to provide our encouragement for completing by the end of next year the critically important tasks you are performing. We are committed to providing whatever personnel and other resources and support needed to accomplish this goal.

Contact Persons:

Allen Mosher
American Public Power Association
(202) 467-2944
amosher@APPAnet.org

James P. Fama
Edison Electric Institute
(202) 508-5725
jfama@eei.org

John A. Anderson
Electricity Consumers Resource Council
(202) 682-1390
janderson@elcon.org

Jack Cashin
Electric Power Supply Association
(202) 349-0155
jcashin@epsa.org

Barry R. Lawson
National Rural Electric Cooperative Association
(703) 907-5781
barry.lawson@nreca.coop

Appendix #7 CIP-002-4 Template
FERC Specific directives from order 706:

Compiled by Scott Mix, NERC

The following table contains the status of all issues raised in the order that were either "direct"ed, specifically in the order, or "adopt"ed from the NOPR.

Note: Given the confusion over the SDT's inclusion of the change in CIP-008 ("Testing the Cyber Security Incident response plan does not require removing a component or system from service during the test") that the commission did not "direct", even though p 687 states: "In light of the comments received, the Commission clarifies that, with respect to full operational testing under CIP-008-1, such testing need not require a responsible entity to remove any systems from service," I did not include any issue that was not actively directed for change, such as those designated "should consider" or similar.

Issue #	Paragraph #	Text	Phase[1]
1	13	NERC is directed to develop a timetable for development of the modifications to the CIP Reliability Standards and, if warranted, to develop and file with the Commission for approval, a second implementation plan.	This compliance filing; and an implementation plan is filed with each submitted version of the standards
2	25	we direct NERC to address revisions to the CIP Reliability Standards CIP-002-1 through CIP-009-1 considering applicable features of the NIST framework.	Version 4
3	47	The Commission adopts the CIP NOPR approach regarding NERC and Regional Entity compliance with the CIP Reliability Standards.	Rules of Procedure statement
4	49	The Commission also adopts its CIP NOPR approach and concludes that reliance on the NERC registration process at this time is an appropriate means of identifying the entities that must comply with the CIP Reliability Standards	Compliance registry process
5	72	We adopt our proposal in the CIP NOPR that responsible entities must comply with the substance of a Requirement.	CMEP
6	75	we direct the ERO to develop modifications to the CIP Reliability Standards that require a responsible entity to implement plans, policies and procedure that it must develop pursuant to the CIP Reliability Standards	Version 2
7	86	The Commission adopts its CIP NOPR proposal and approves NERC's implementation plan and time frames for responsible entities	CMEP

[1] Schedule phases in this column mean one or more of the following:
- "Version 2" – complete in filed version 2
- "Version 4" – planned for next major version (12-18 months plus)
- "Guideline" – stand alone guidance started after corresponding requirement is determined
- "TFE Filing" – 2009 filing on TFE proposal and Appendix 4D to RoP
- "not scheduled" – beyond Version 4
- "CMEP" – part of an existing or ongoing compliance audit, self-report or other process
- "VRF Filing(s)" – one of several already-filed (or very soon to be filed in the case of Version 2) VRF and/or VSL filings

Phase may also be self-explanatory if not one of these entries

Issue #	Paragraph #	Text	Phase[1]
		to achieve auditable compliance.	
8	89	we direct the ERO to submit a work plan for Commission approval for developing and filing for approval the modifications to the CIP Reliability Standards that we are directing in this Final Rule	This compliance filing; and an implementation plan is filed with each submitted version of the standards
9	90	We direct the ERO, in its development of a work plan, to consider developing modifications to CIP-002-1 and the provisions regarding technical feasibility exceptions as a first priority, before developing other modifications required by the Final Rule.	TFE Filing
10	96	we direct the ERO to require more frequent, semiannual, self-certifications prior to the date by which full compliance is required	CMEP program and self-certifications
11	97	we adopt our CIP NOPR proposals that, while an entity should not be subject to a monetary penalty if it is unable to certify that it is on schedule, such an entity should explain to the ERO the reason it is unable to self-certify	CMEP, self-certification process
12	106	the Commission adopts the CIP NOPR proposals and directs NERC to modify the CIP Reliability Standards through the Reliability Standards development process to remove the first two Terms ["reasonable business judgment," and "acceptance of risk"], and develop specific conditions that a responsible entity must satisfy to invoke the "technical feasibility" exception	Version 2 and TFE Filing
13	128	the Commission directs the ERO to develop modifications to the CIP Reliability Standards that do not include this term. We note that many commenters, including NERC, agree that the reasonable business judgment language should be removed based largely on the rationale articulated by the Commission in the CIP NOPR.	Version 2
14	138	the Commission directs the ERO to modify the CIP Reliability Standards through its Reliability Standards development process to remove references to reasonable business judgment before compliance audits begin.	Version 2
15	150	The Commission, therefore, directs the ERO to remove acceptance of risk language from the CIP Reliability Standards.	Version 2
16	156	the Commission directs the ERO to develop through its Reliability Standards development process revised CIP Reliability Standards that eliminate references to acceptance of risk.	Version 2
17	178	directs the ERO to develop a set of conditions or criteria that a responsible entity must follow when relying on the technical feasibility exception contained in specific Requirements of the CIP Reliability Standards	TFE Filing
18	186	the Commission adopts its proposal in the CIP NOPR that technical feasibility exceptions may be permitted if appropriate conditions are in place.	TFE Filing
19	192	the Commission adopts the CIP NOPR proposal for a three step structure to require accountability when a responsible entity relies on technical feasibility as the basis for an exception. We address	TFE Filing

Issue #	Paragraph #	Text	Phase[1]
		mitigation and remediation in this section and direct the ERO to develop: (1) a requirement that the responsible entity must develop, document and implement a mitigation plan that achieves a comparable level of security to the Requirement; and (2) a requirement that use of the technical feasibility exception by a responsible entity must be accompanied by a remediation plan and timeline for elimination the use of the technical feasibility exception.	
20	209	The Commission thus adopts its CIP NOPR proposal that use and implementation of technical feasibility exceptions must be governed by a clear set of criteria.	TFE Filing
21	211	direct the ERO to include approval of the mitigation and remediation steps by the senior manager (identified pursuant to CIP-003-1) in the course of developing this framework of accountability.	TFE Filing
22	212	the practical considerations pointed out by a number of the comments have convinced us to adopt an approach to the issue of external oversight different from the one originally proposed.	TFE Filing
23	218	we direct the ERO to design and conduct an approval process through the Regional Entities and the compliance audit process.	TFE Filing
24	219	we direct NERC, in developing the accountability structure for the technical feasibility exception, to include appropriate provisions to assure that governmental entities that are subject to Reliability Standards as users, owners or operators of the Bulk-Power System can safeguard sensitive information.	TFE Filing
25	220	We direct the ERO to submit an annual report to the Commission that provides a wide-area analysis regarding use of the technical feasibility exception and the effect on Bulk-Power System reliability.	TFE Filing
26	221	we direct the ERO to control and protect the data analysis to the extent necessary to ensure that sensitive information is not jeopardized by the act of submitting the report to the Commission.	TFE Filing
27	222	we direct the ERO to develop a set of criteria to provide accountability when a responsible entity relies on the technical feasibility exceptions in specific Requirements of the CIP Reliability Standards.	TFE Filing
28	222	We direct the ERO to develop appropriate modifications, as discussed above.	TFE Filing
29	233	we direct the ERO to consult with federal entities that are required to comply with both CIP Reliability Standards and NIST standards on the effectiveness of the NIST standards and on implementation issues and report these findings to the Commission.	Ongoing discussions with Drafting Team Members from USBR, BPA, NIST; Development of Version 4
30	253	While we adopt our CIP NOPR proposal, we recognize that the ERO has already initiated a process to develop such guidance … leave to the EO's discretion whether to incorporate such guidance into the CIP Reliability Standard, develop it as a separate guidance document, or some combination of the two.	Guideline / Version 4
31	254	direct the ERO to consider these commenter concerns [how to assess whether a generator or a blackstart unit is "critical" to Bulk-	Guideline / Version 4

Issue #	Paragraph #	Text	Phase[1]
		Power System reliability, the proper quantification of risk and frequency, facilities that are relied on to operate or shut down nuclear generating stations, and the consequences of asset failure and asset misuse by an adversary]when developing the guidance.	
32	255	we direct either the ERO or its designees to provide reasonable technical support to assist entities in determining whether their assets are critical to the Bulk-Power System.	Unscheduled
33	257	we direct the ERO to consider this clarification [the meaning of the phrase "used for initial system restoration," in CIP-002-1, Requirement R1.2.4] in its Reliability Standards development process.	Guideline / Version 4
34	272	the Commission directs the ERO, in developing the guidance discussed above regarding the identification of critical assets, to consider the designation of various types of data as a critical asset or critical cyber asset.	Guideline / Version 4
35	272	The Commission directs the ERO to develop guidance on the steps that would be required to apply the CIP Reliability Standards to such data and to consider whether this also covers the computer systems that produce the data.	Guideline / Version 4
36	282	the Commission directs the ERO, through the Reliability Standards development process, to specifically require the consideration of misuse of control centers and control systems in the determination of critical assets	Guideline / Version 4
37	285	we direct the ERO to consider the comment from ISA99 Team [ISA99 Team objects to the exclusion of communications links from CIP-002-1 and non-routable protocols from critical cyber assets, arguing that both are key elements of associated control systems, essential to proper operation of the critical cyber assets, and have been shown to be vulnerable — by testing and experience].	Version 4
38	294	The Commission adopts its CIP NOPR proposal and directs the ERO to develop, pursuant to its Reliability Standards development process, a modification to CIP-002-1 to explicitly require that a senior manager annually review and approve the risk-based assessment methodology.	Version 2
39	294	the Commission directs the ERO to develop a modification to CIP-002-1 to explicitly require that a senior manager annually review and approve the risk-based assessment methodology.	Version 2
40	322	The Commission adopts its CIP NOPR proposal to direct that the ERO develop through its Reliability Standards development process a mechanism for external review and approval of critical asset lists.	Version 4 (Note: proposed version 4 methodology obviates the need for external review0
41	329	the Commission directs the ERO, using its Reliability Standards development process, to develop a process of external review and approval of critical asset lists based on a regional perspective.	Version 4 (Note: proposed version 4 methodology obviates the need for external review0
42	333	we direct the ERO, in developing the accountability structure for the	TFE Filing

Issue #	Paragraph #	Text	Phase[1]
		technical feasibility exception, to include appropriate provisions to assure that governmental entities can safeguard sensitive information	
43	355	the Commission directs the ERO to provide additional guidance for the topics and processes that the required cyber security policy should address.	Guideline
44	376	the Commission adopts its CIP NOPR proposal and directs the ERO to clarify that the exceptions mentioned in Requirements R2.3 and R3 of CIP-003-1 do not except responsible entities from the Requirements of the CIP Reliability Standards.	Version 4
45	381	The Commission adopts its CIP NOPR interpretation that Requirement R2 of CIP-003-1 requires the designation of a single manager who has direct and comprehensive responsibility and accountability for implementation and ongoing compliance with the CIP Reliability Standards	Version 2
46	386	The Commission adopts its CIP NOPR proposal and directs the ERO to develop modifications to Reliability Standards CIP-003-1, CIP-004-1, and/or CIP-007-1, to ensure and make clear that, when access to protected information is revoked, it is done so promptly.	Version 4
47	397	The Commission directs the ERO to develop modifications to Requirement R6 of CIP-003-1 to provide an express acknowledgment of the need for the change control and configuration management process to consider accidental consequences and malicious actions along with intentional changes.	Version 4 / Guideline
48	412	The Commission therefore directs the ERO to provide guidance, regarding the issues and concerns that a mutual distrust posture must address in order to protect a responsible entity's control system from the outside world.	Guideline
49	431	The Commission adopts the CIP NOPR's proposal and directs the ERO to develop a modification to CIP-004-1 that would require affected personnel to receive required training before obtaining access to critical cyber assets (rather than within 90 days of access authorization), but allowing limited exceptions, such as during emergencies, subject to documentation and mitigation.	Version 2
50	433	we direct the ERO to consider, in developing modifications to CIP-004-1, whether identification of core training elements would be beneficial and, if so, develop an appropriate modification to the Reliability Standard.	Version 4
51	434	The Commission adopts the CIP NOPR's proposal to direct the ERO to modify Requirement R2 of CIP-004-1 to clarify that cyber security training programs are intended to encompass training on the networking hardware and software and other issues of electronic interconnectivity supporting the operation and control of critical cyber assets.	Version 4
52	435	Consistent with the CIP NOPR, the Commission directs the ERO to determine what, if any, modifications to CIP-004-1 should be made	Version 4

Issue #	Paragraph #	Text	Phase[1]
		to assure that security trainers are adequately trained themselves.	
53	443	The Commission adopts with modifications the proposal to direct the ERO to modify Requirement R3 of CIP-004-1 to provide that newly-hired personnel and vendors should not have access to critical cyber assets prior to the satisfactory completion of a personnel risk assessment, except in specified circumstances such as an emergency.	Version 2
54	443	We also direct the ERO to identify the parameters of such exceptional circumstances through the Reliability Standards development process	Version 4
55	460	The Commission adopts the CIP NOPR proposal to direct the ERO to develop modifications to CIP-004-1 to require immediate revocation of access privileges when an employee, contractor or vendor no longer performs a function that requires physical or electronic access to a critical cyber asset for any reason (including disciplinary action, transfer, retirement, or termination).	Version 4
56	464	We also adopt our proposal to direct the ERO to modify Requirement R4 to make clear that unescorted physical access should be denied to individuals that are not identified on the authorization list, with clarification.	Version 4
57	473	The Commission adopts its proposals in the CIP NOPR with a clarification. As a general matter, all joint owners of a critical cyber asset are responsible to protect that asset under the CIP Reliability Standards. The owners of joint use facilities which have been designated as critical cyber assets are responsible to see that contractual obligations include provisions that allow the responsible entity to comply with the CIP Reliability Standards. This is similar to a responsible entity's obligations regarding vendors with access to critical cyber assets.	Version 4
58	476	we direct the ERO to modify CIP-004-1, and other CIP Reliability Standards as appropriate, through the Reliability Standards development process to address critical cyber assets that are jointly owned or jointly used, consistent	Version 4
59	496	The Commission adopts the CIP NOPR's proposal to direct the ERO to develop a requirement that each responsible entity must implement a defensive security approach including two or more defensive measures in a defense in depth posture when constructing an electronic security perimeter	Not scheduled
60	502	The Commission directs that a responsible entity must implement two or more distinct security measures when constructing an electronic security perimeter, the specific requirements should be developed in the Reliability Standards development process.	Not scheduled
61	502	The Commission also directs the ERO to consider, based on the content of the modified CIP-005-1, whether further guidance on this defense in depth topic should be developed in a reference document outside of the Reliability Standards.	Not scheduled / Guideline

Issue #	Paragraph #	Text	Phase[1]
62	503	The Commission is directing the ERO to revise the Reliability Standard to require two or more defensive measures.	Not scheduled
63	511	The Commission adopts the CIP NOPR's proposal to direct the ERO to identify examples of specific verification technologies that would satisfy Requirement R2.4, while also allowing compliance pursuant to other technically equivalent measures or technologies.	Version 4
64	525	The Commission adopts the CIP NOPR proposal to require the ERO to modify CIP-005-1 to require logs to be reviewed more frequently than 90 days	Version 4
65	526	the Commission directs the ERO to modify CIP-005-1 through the Reliability Standards development process to require manual review of those logs without alerts in shorter than 90 day increments.	Version 4
66	526	The Commission directs the ERO to modify CIP-005-1 to require some manual review of logs, consistent with our discussion of log sampling below, to improve automated detection settings, even if alerts are employed on the logs.	Version 4
67	528	the Commission clarifies its direction with regard to reviewing logs. In directing manual log review, the Commission does not require that every log be reviewed in its entirety. Instead, the ERO could provide, through the Reliability Standards development process, clarification that a responsible entity should perform the manual review of a sampling of log entries or sorted or filtered logs.	Version 4
68	541	we adopt the ERO's proposal to provide for active vulnerability assessments rather than full live vulnerability assessments.	Version 4
69	542	the Commission adopts the ERO's recommendation of requiring active vulnerability assessments of test systems.	Version 4
70	544	the Commission directs the ERO to revise the Reliability Standard so that annual vulnerability assessments are sufficient, unless a significant change is made to the electronic security perimeter or defense in depth measure, rather than with every modification.	Version 4
71	544	we are directing the ERO to determine, through the Reliability Standards development process, what would constitute a modification that would require an active vulnerability assessment	Version 4
72	547	we direct the ERO to modify Requirement R4 to require these representative active vulnerability assessments at least once every three years, with subsequent annual paper assessments in the intervening years	Version 4
73	560	the Commission directs the ERO to treat any alternative measures for Requirement R1.1 of CIP-006-1 as a technical feasibility exception to Requirement R1.1, subject to the conditions on technical feasibility exceptions.	TFE Filing / CMEP
74	572	The Commission adopts the CIP NOPR proposal to direct the ERO to modify this CIP Reliability Standard to state that a responsible entity must, at a minimum, implement two or more different security procedures when establishing a physical security perimeter around	Not scheduled

Issue #	Paragraph #	Text	Phase[1]
		critical cyber assets.	
75	575	The Commission also directs the ERO to consider, based on the content of the modified CIP-006-1, whether further guidance on this defense in depth topic should be developed in a reference document outside of the Reliability Standards.	Not scheduled / Guideline
76	581	The Commission adopts the CIP NOPR proposal and directs the ERO to develop a modification to CIP-006-1 to require a responsible entity to test the physical security measures on critical cyber assets more frequently than every three years,	Version 4
77	597	Therefore, the Commission directs the ERO to eliminate the acceptance of risk language from Requirements R2.3 and R3.2.	Version 2
78	600	Commission therefore directs the ERO to revise Requirement R3 to remove the acceptance of risk language and to impose the same conditions and reporting requirements as imposed elsewhere in the Final Rule regarding technical feasibility.	Version 2 / TFE Filing
79	609	We therefore direct the ERO to develop requirements addressing what constitutes a "representative system" and to modify CIP-007-1 accordingly. The Commission directs the ERO to consider providing further guidance on testing systems in a reference document.	Version 4 / Guideline
80	610	we direct the ERO to revise the Reliability Standard to require each responsible entity to document differences between testing and production environments in a manner consistent with the discussion above.	Version 4
81	611	the Commission cautions that certain changes to a production or test environment might make the differences between the two greater and directs the ERO to take this into account when developing guidance on when to require updated documentation to ensure that there are no significant gaps between what is tested and what is in production.	Version 4
82	619	The Commission adopts the CIP NOPR proposal with regard to CIP-007-1, Requirement R4. [The Commission proposed to direct the ERO to eliminate the acceptance of risk language from Requirement R4.2, and also attach the same documentation and reporting requirements to the use of technical feasibility in Requirement R4, pertaining to malicious software prevention, as elsewhere. The Commission discussed the issues of defense in depth, technical feasibility, and risk acceptance elsewhere in the CIP NOPR and applied those conclusions here. The Commission further proposed to direct the ERO to modify Requirement R4 to include safeguards against personnel introducing, either maliciously or unintentionally, viruses or malicious software to a cyber asset within the electronic security perimeter through remote access, electronic media, or other means]	Version 4 / not scheduled
83	622	Therefore, the Commission directs the ERO to eliminate the acceptance of risk language from Requirement R4.2	Version 2
84	622	The Commission also directs the ERO to modify Requirement R4 to include safeguards against personnel introducing, either maliciously	Version 4 / not scheduled

Issue #	Paragraph #	Text	Phase[1]
		or unintentionally, viruses or malicious software to a cyber asset within the electronic security perimeter through remote access, electronic media, or other means, consistent with our discussion above	
85	628	The Commission continues to believe that, in general, logs should be reviewed at least weekly and therefore adopts the CIP NOPR proposal to require the ERO to modify CIP-007-1 to require logs to be reviewed more frequently than 90 days, but leaves it to the Reliability Standards development process to determine the appropriate frequency, given our clarification below, similar to our action with respect to CIP-005-1	Version 4
86	629	The Reliability Standards development process should decide the degree to which the revised CIP-007-1 describes acceptable log sampling. The ERO could also provide additional guidance on how to create the sampling of log entries, which could be in a reference document.	Version 4 / guideline
87	633	The Commission adopts the CIP NOPR proposal to direct the ERO to clarify what it means to prevent unauthorized retrieval of data from a cyber asset prior to discarding it or redeploying it.	Version 4
88	635	the Commission directs the ERO to revise Requirement R7 of CIP-007-1 to clarify, consistent with this discussion, what it means to prevent unauthorized retrieval of data.	Version 4
89	643	The Commission adopts its proposal to direct the ERO to provide more direction on what features, functionality, and vulnerabilities the responsible entities should address when conducting the vulnerability assessments, and to revise Requirement R8.4 to require an entity-imposed timeline for completion of the already-required action plan.	Not scheduled
90	651	We direct the ERO to revise Requirement R9 to state that the changes resulting from modifications to the system or controls shall be documented quicker than 90 calendar days.	Version 2
91	660	The Commission adopts the CIP NOPR proposal to direct the ERO to provide guidance regarding what should be included in the term reportable incident. … we direct the ERO to develop and provide guidance on the term reportable incident.	Guideline
92	661	the Commission directs the ERO to develop a modification to CIP-008-1 to: (1) include language that takes into account a breach that may occur through cyber or physical means; (2) harmonize, but not necessarily limit, the meaning of the term reportable incident with other reporting mechanisms, such as DOE Form OE 417; (3) recognize that the term should not be triggered by ineffectual and untargeted attacks that proliferate on the internet; and (4) ensure that the guidance language that is developed results in a Reliability Standard that can be audited and enforced	Version 4 / Guideline
93	673	The Commission adopts the CIP NOPR proposal to direct the ERO to modify CIP-008-1 to require each responsible entity to contact appropriate government authorities and industry participants in the	Version 4 / Guideline

Issue #	Paragraph #	Text	Phase[1]
		event of a cyber security incident as soon as possible, but, in any event, within one hour of the event, even if it is a preliminary report.	
94	676	the Commission directs the ERO to modify CIP-008-1 to require a responsible entity to, at a minimum, notify the ESISAC and appropriate government authorities of a cyber security incident as soon as possible, but, in any event, within one hour of the event, even if it is a preliminary report.	Version 4 /. Guideline
95	686	The Commission adopts the CIP NOPR proposal to direct the ERO to modify CIP-008-1, Requirement R2 to require responsible entities to maintain documentation of paper drills, full operational drills, and responses to actual incidents, all of which must include lessons learned.	Version 4
96	686	The Commission further directs the ERO to include language in CIP-008-1 to require revisions to the incident response plan to address these lessons learned.	Version 4
97	694	For the reasons discussed in the CIP NOPR, the Commission adopts the proposal to direct the ERO to modify CIP-009-1 to include a specific requirement to implement a recovery plan.	Version 4
98	694	We further adopt the proposal to enforce this Reliability Standard such that, if an entity has the required recovery plan but does not implement it when the anticipated event or conditions occur, the entity will not be in compliance with this Reliability Standard.	Version 4
99	706	The Commission adopts, with clarification, the CIP NOPR proposal to direct the ERO to modify CIP-009-1 to incorporate use of good forensic data collection practices and procedures into this CIP Reliability Standard.	Not scheduled
100	710	Therefore, we direct the ERO to revise CIP-009-1 to require data collection, as provided in the Blackout Report.	Not scheduled
101	725	The Commission adopts, with modifications, the CIP NOPR proposal to develop modifications to CIP-009-1 through the Reliability Standards development process to require an operational exercise once every three years (unless an actual incident occurs, in which case it may suffice), but to permit reliance on table-top exercises annually in other years.	Not scheduled
102	731	The Commission adopts the CIP NOPR proposal to direct the ERO to modify Requirement R3 of CIP-009-1 to shorten the timeline for updating recovery plans.	Version 2
103	739	The Commission adopts the CIP NOPR proposal to direct the ERO to modify CIP- 009-1 to incorporate guidance that the backup and restoration processes and procedures required by Requirement R4 should include, at least with regard to significant changes made to the operational control system, verification that they are operational before the backups are stored or relied upon for recovery purposes	Version 4
104	748	The Commission adopts the CIP NOPR proposal to direct the ERO to modify CIP-009-1 to provide direction that backup practices include regular procedures to ensure verification that backups are	Version 4

Issue #	Paragraph #	Text	Phase[1]
		successful and backup failures are addressed, so that backups are available for future use.	
105	757	Therefore, we will not allow NERC to reconsider the Violation Risk Factor designations in this instance but, rather, direct below that NERC make specific modifications to its designations.	VRF Filing(s)
106	759	Consistent with the Violation Risk Factor Order, the Commission directs NERC to submit a complete Violation Risk Factor matrix encompassing each Commission approved CIP Reliability Standard.	VRF Filing(s)
107	767	The Commission adopts the CIP NOPR proposal to direct the ERO to revise 43 Violation Risk Factors.	VRF Filing(s)

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Agenda
Cyber Security Order 706 SDT — Project 2008-06

January 19, 2010 | 1:00 PM to 5:00 PM EST
January 20, 2010 | 8:00 AM to 5:00 PM EST
January 21, 2010 | 8:00 AM to 5:00 PM EST
January 22, 2010 | 8:00 AM to 3:00 PM EST

Georgia Transmission Corporation
2100 East Exchange Place
Tucker, GA

NOTE:
1. Agenda Times May be Adjusted as Needed during the Meeting
2. Drafting Group Meetings May Not Have Access to Telephones and

Proposed Meeting Objectives/Outcomes

- Review the CSO 706 SDT 2010 Workplan
- Receive update on the CIP 002-4 filing and review process lessons learned
- Receive updates on other related cyber security initiatives
- Receive a NERC update on implementing the CIP Communication Plan
- Review, discuss and test consensus for CIP guiding principles
- Review strawman documents, discuss and test consensus for CIP security controls approach, guidance, scope and applicability.
- Convene CIP Security Controls Drafting Groups
- Review Drafting Group Reports and Provide Feedback
- Agree on next steps and assignments

Draft Agenda

Tuesday	**January 19, 2009**
1:00 p.m.	Welcome and Opening Remarks- *Jeri Domingo-Brewer & Phil Huff* Roll Call; NERC Antitrust Compliance Guidelines Facilitator review and SDT acceptance of December 15-16, 2009 Little Rock SDT meeting summary
1:15	Review of Meeting Objectives, Agenda and Meeting Guidelines- *Bob Jones*
1:20	Review of CSO 706 SDT Workplan- January-June, 2010- *Stu Langton*
1:40	Update on CIP 002 Filing- Process Lessons Learned- *Joe Bucciero*

2:00	Other Updates on other related cyber security initiatives- *NERC Staff and SDT Members*
2:15	NERC Update on Implementing the CIP Communication Plan
2:30	Overview of Security Controls Strawman Documents and Drafting Group Process
2:	*Break*
3:00	Review, Rating and Consensus Testing of Principles
4:00	Review Strawman Security Controls Categories and Proposed Drafting Sub-Teams
4:30	Review and Consensus Testing of Sources for Controls
5:00	Review of Required Elements for Each Security Control
5:15	Member Drafting Sub-Teams Preference Survey
5:25	Review of Proposal for Wednesday Agenda and Drafting Groups
5:30	*Recess*

Wednesday	**January 20, 2010**
8:00	Welcome and Agenda Review- *Jeri Domingo-Brewer & Phil Huff*
8:10	Review of CIP Security Controls Drafting Template- *Scott Mix and Howard Gugel, NERC*
8:45	Review and Agree on Proposal for Drafting Security Controls and Sub Team Members
10:00	Convene Organizational Meetings of SDT Cyber Security Controls Sub Teams
12:00	*Working Lunch*
12:45	Reconvene SDT Cyber Security Controls Sub Teams
3:15 5	*Break*
3:0	Sub Team Organizational Reports, Requests and Needs and Full Team Feedback
4:50	Review Assignments and Thursday Agenda
5:00	*Recess*

Thursday	**January 21, 2010**
8:00	Welcome and Agenda Review- *Jeri Domingo-Brewer & Phil Huff*
8:15	Review any Drafting Group Requests/Needs
8:30	Reconvene SDT Cyber Security Controls Sub Teams
12:00	*Lunch*
	Reconvene SDT Cyber Security Controls Sub Teams
2:45	*Break*
3:00	Sub Team Reports and Full Team Feedback
4:50	Review Assignments and Friday Agenda
5:00	*Recess*

Friday	**January 22, 2010**
8:00	Welcome and Agenda Review- *Jeri Domingo-Brewer & Phil Huff*
8:15	Review any Drafting Group Requests/Needs
8:30	Reconvene SDT Cyber Security Controls Sub Teams
12:00	*Lunch*
12:30	Sub Team Reports and Full Team Feedback
2:30	Review and Agree on Next Steps for Developing Security Controls (CIP 003-009) and Work plan for February 2010 Meeting on CIP 002-4 Industry Comments
	Meeting Evaluation
3:00	*Adjourn*

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

PROJECT 2008-06 CYBER SECURITY ORDER 706 SDT MEMBERS

1. Rob Antonishen	Ontario Power Generation
2. Jeri Domingo-Brewer, Chair	U.S. Bureau of Reclamation
3. Jim Brenton	ERCOT
4. Jackie Collett	Manitoba Hydro
5. Jay S. Cribb	Information Security Analyst, Southern Company Services
6. Joe Doetzl	Manager, Information Security, Kansas City Pwr. & Light Co.
7. Sharon Edwards	Duke Energy
8. Gerald S. Freese	Director, Enterprise Info. Security America Electric Pwr.
9. **Phillip Huff, Vice Chair**	Arkansas Electric Coop Corporation
10. Doug Johnson	Exelon Corporation – Commonwealth Edison
11. Frank Kim	Ontario Hydro
12. Rich Kinas	Orlando Utilities Commission
13. John Lim, Chair	CISSP, Department Manager, Consolidated Edison Co. NY
14. David Norton	Entergy
15. Christopher A. Peters	ICF International
16. David S. Revill	Georgia Transmission Corporation
17. Scott Rosenberger	Luminant Energy
18. Kevin Sherlin	Sacramento Municipal Utility District
19. Jonathan Stanford	Bonneville Power Administration
20.Keith Stouffer	National Institute of Standards & Technology
21. John D. Varnell	Technology Director, Tenaska Power Services Co.
22.William Winters	Arizona Public Service, Inc.
Roger Lampilla	NERC
Scott Mix	NERC
Dave Taylor	NERC
Howard Gugel	NERC
Joe Bucciero	NERC/Bucciero Consulting, LLC
Robert Jones	FSU/FCRC Consensus Center
Hal Beardal	FSU/FCRC Consensus Center
Stuart Langton	FSU/FCRC Consensus Center

CSO 706 SDT MEETING SCHEDULE
JANUARY –DECEMBER 2010

REFINEMENT AND ADOPTION OF CIP-002 VERSION 4 AND DEVELOPMENT AND ADOPTION OF CIP STANDARDS (003-009)
JANUARY 2010–DECEMBER 2010

- ***SDT Security Controls Member Survey- December 30-January 6, 2010.***
- January 6- SDT Conference Call to Review Survey Results and Strawman Drafting Group
- January 11- SDT Strawman Drafting Group Conference Call
- January 14- SDT Strawman Drafting Group Conference Call

18. January 19-20–21-22 — Tues-1 PM- to Friday 3 PM, Tucker, GA (GTC)

- SDT reviews and refines security control drafting principles, strawman approach and subteams.
- SDT Security Controls Sub Teams begin drafting.

Interim Security Control Sub Team Conference Call Drafting Meetings

19. February 16, 17, 18 &19 —Tues-1 PM to –Friday 3 PM, Austin TX (ERCOT)

- SDT Reviews Industry Comments and Refines CIP 002-4 for posting for 45-day industry formal comment period.
- SDT Sub Team Progress Reports

Interim Security Control Sub Team Conference Call Drafting Meetings

20. March 9, 10, 11 & 12 — Tues-1 PM –Friday 3 PM, Phoenix, AZ (APS)

- SDT Security Control Sub Teams continue strawman drafts
- Review, Compile and Agree on an initial draft Security Controls Text

Interim Security Control Sub Team Conference Call Drafting Meetings

21. April 13, 14, 15 & 16 — Tues.-1 PM- Friday 3 PM, Atlanta GA (Southern Co)

- SDT Reviews and Responds to Industry Comments, Refines and Adopts CIP 002 for balloting
- SDT review and reach consensus on a draft CIP 003-009 for informal industry comment.

Interim Security Control Sub Team Conference Call Drafting Meetings

22. May 11-12–13 & 14 — Tues 1 PM- 3 PM Friday, Dallas TX (Luminant)

- SDT reviews Industry 1st Ballot Comments and Drafts Responses
- SDT reviews CIP Security Controls informal industry comments and refines the draft.

Interim Security Control Sub Team Conference Call Drafting Meetings

23. June 8-11- Tues- Fri. (Sacramento)

- SDT refines CIP Security Controls and posts for 2nd round of informal industry comments and refines the draft.

Interim Security Control Sub Team Conference Call Drafting Meetings

24. July 13-16, Tues-Fri., Pittsburgh, PA (CERT)

- SDT reviews CIP Security Controls informal industry comments and refines the draft.

Interim Security Control Sub Team Conference Call Drafting Meetings

25. August 10–13, Tues-Fri TBD

- SDT refines CIP 003-009 and posts for formal 45 day industry comment

Interim Security Control Sub Team Conference Call Drafting Meetings

26. September 7,8,9, Tues-Fri. TBD (if needed)

27. Oct. 12–15, Tues–Friday- TBD

- SDT Reviews and Responds to Industry Comments, Refines and Adopts CIP Security Controls for balloting

28. November 16–19, Tues-Fri - TBD

- SDT reviews Industry 1st Ballot Comments and Drafts Responses

29. December 14–17, Tues-Fri.- TBD

DEVELOPMENT OF CIP VERSION 2 AND NEW VERSION FRAMEWORK
OCTOBER 2008–JULY 2009

1. October 6–7, 2008 — Gaithersburg, MD Reviewed CIP-002-CIP-009, Agreed on Version 2 approach.

2. October 20–21 —Sacramento, CA CIP-002-CIP-009 Version 2 development

3. November 12–14, 2008 — Little Rock, AR CIP-002-CIP-009 Version 2 adoption for comment and balloting; CIP-002-CIP-009 New Version process reviewed.

4. December 4–5, 2008 — Washington D.C. CIP-002-CIP-009 Version 3 reviewed and debated, SDT member white "working" papers assigned, Technical Feasibility Exceptions white paper reviewed and refined.

5. January 7–9 — Phoenix, AZ, Reviewed Technical Feasibility Exceptions white paper**,** reviewed industry comments on CIP-002-CIP-009 Version 2 products — established small groups to draft responses, reviewed New Version white "working" papers.

January 15 — WebEx meeting(s) Small group drafted responses to industry Version 2 comments.

January 21 — WebEx meeting(s) Small group drafted responses to industry Version 2 comments.

6. February 2–4, 2009 — Phoenix, AZ Update on NERC Technical Feasibility Exceptions process**,** VSL process and SDT role**,** review of Version 3 White papers, strawman and principles**,** reviewed and adopted SDT responses to industry comments on Version 2 and Version 2 Product Revisions.

7. February 18–19, 2009 — Fairfax, VA Update on Version 2 process**,** NERC TFE process and VSL Team process; reviewed, discussed and refined Version 3 CIP-002 White papers, strawman, and principles.

8. March 10–11, 2009 — Orlando, FL Update on NERC TFE and VSL and VRF Team process and review and refine Version 3 CIP-002 Strawman Proposals

March 2–April 1, 2009 — 30-day Pre Ballot

Mid-March — NERC posts TFE draft Rules of Procedure for industry comment

March 30, 2009 — WebEx meeting(s) White Paper Drafting Team

April 1–10 — NERC Balloting on Version 2 Products

April 6, 2009 — WebEx meeting — White Paper Drafting Team

April 8, 2009 — WebEx meeting(s) — White Paper Preview- Full SDT Conference Call

April 11, 2009 — Version 2 Ballot Results (Quorum: 91.90% Approval: 84.06%) and Industry Comments

9. April 14–16, 2009 — Charlotte NC Update on NERC TFE process, VSL Team process and NERC Critical Assets Survey; agreed and adopted responses for Version 2 industry comments for recirculation ballot; reviewed and refined Version 3 whitepaper and consensus points and progress report to NERC Member Representative Committee (MRC) May meeting.

April 28 and May 6, 2009 — White Paper Drafting Team Meetings and WebEx

April 17–27, 2009 — Recirculation Results: Quorum: 94.37% Approval: 88.32%

May 5, 2009 — NERC MRC Meeting, Arlington, VA- SDT progress report.

10. May 13–14, 2009 — Boulder City NV Reviewed MRC presentation and further SDT refinement and discussion of the Version 3 White Paper.

June 8 and June 15, 2009 — Working Paper Drafting Team Meetings and WebEx

11. June 17–18, 2009 — Portland OR Further SDT refinement of the draft CIP Version 3 Working Paper(s), reviewed SDT development process for June-December 2009; discussed potential SDT subcommittee structure and deliverables.

- *June — WebEx meeting(s)*
- *Working Paper drafting group sessions including inputs from selected industry personnel to help establish BES categorization criteria*

CIP-002 DEVELOPMENT OF REQUIREMENTS, MEASURES, ETC. JULY-DECEMBER 2009

12. July 13–14, 2009 in Vancouver, B.C., Canada

SDT reviewed, refined, and adopted SDT Working Paper. SDT adopted its response to NERC for Interpretation of CIP-006-1. SDT reviewed and adopted a proposal for CIP-002 Subgroups and Deliverables and convened subgroup organizational meetings to develop work plans. SDT adopted 2010 Meeting Schedule.

- *July–August Interim Conference call meeting(s)*
- *CIP-002 Subgroup meetings*
- *CIP-002 Coordination Team meeting*
- *August 3–5, 2009 in Winnipeg, Manitoba **NERC Member Representative Committee**. Progress Report and presentation on new CIP Version 3 Working Paper-Concept-Reliability Standards on Cyber Security for MRC input.*

13. August 20–21, 2009 in Charlotte, NC. SDT reviewed and responded to MRC input on Working Paper/CIP-002 Concepts and convened SDT Subgroup and plenary meetings to develop CIP-002 requirements and "proof of concept" control (s).

- *July–September — 45-day Industry Comment Period on CIP-002 Concept Working Paper*
- *NERC Webinar- August–September Interim Conference Call meeting(s)*
- *CIP-002 Subgroup meetings (as ne*
- *CIP-002 Coordination Team meeting*

14. September 9–10, 2009 in Folsom, CA. SDT reviewed and considered industry comments on the Working Paper and CIP-002 concepts and their application to the subgroup work and addressed coordinating issues through joint subgroup meetings. SDT agreed on meeting dates and proposed locations for January–December 2010

September–October Interim WebEx meeting(s)

- *FERC Version 3 Urgent Action SDT conference call meetings*
- *CIP-002 Coordination Team meeting*

CIP VERSION 3 RESPONSE TO FERC ORDER, OCTOBER-DECEMBER, 2009

15. October 20–22, 2009 in Kansas City, MI. Reviewed new FERC Order and urgent action CIP Version 3 process; discussed key issues raised by SDT CIP 002 Subgroups, small group meetings and agreement on refinements to the CIP 002-009 schedule and drafting process for CIP 002-4.

- *October–November Drafting Team meeting(s)*
- *CIP-002 Coordination Team meeting*

16. November 16–19, 2009 in Orlando, FL

- SDT review, refine and adopt Version 3 "industry response" document.
- SDT plenary and drafting group session(s) — to draft, review and refine CIP-002-4 standard, requirements, measures and controls and related documents.
- November–December Interim Conference call meeting(s)

- Drafting teams as needed to finalize draft CIP 002-4 documents
- CIP-002 Coordination Team meeting
- *CIP 002-4 Drafting Team produces next draft based on Orlando Meeting input.*
- *December 2 CSO 706 SDT Version 3 Consideration of Comments Draft Conference Call*
- *December X, CSO 706 SDT CIP 002-4 Preview Conference Call*

17. December 15–16, 2009 in Little Rock AK

- SDT scenario "walk through" to test flow of CIP 002-4.
- SDT plenary and drafting group session(s) to review, refine, and agree on and adopt CIP-002-4 standard, requirements, measures and controls and related documents.
- Agree on initial posting of draft CIP-002-4 for industry review and comment.
- Agree on next steps and 2010 Workplan and schedule

- December 28, 2009 SDT Conference Call on CIP 002-4
- December 30, 2009 SDT Leadership Call- Security Controls Survey Draft

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Notes
Cyber Security Order 706 SDT — Project 2008-06

January 19, 2010 | 1:00 p.m. to 5:00 p.m. EST
January 20, 2010 | 8:00 a.m. to 5:00 p.m. EST
January 21, 2010 | 8:00 a.m. to 5:00 p.m. EST
January 22, 2010 | 8:00 a.m. to 5:00 p.m. EST

Adopted Unanimously by the SDT February 18, 2010

Robert Jones, Stuart Langton, and Hal Beardall
Facilitation and Meeting Design
FCRC Consensus Center, Florida State University

Joe Bucciero, Bucciero Consulting, LLC

http://www.nerc.com/filez/standards/Project_2008-06_Cyber_Security.html

116-390 Village Blvd.
Princeton, NJ 08540
609.452.8060 | www.nerc.com

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Meeting Summary Contents

EXECUTIVE SUMMARY

On Tuesday afternoon, the Chair, Jeri Domingo-Brewer welcomed the members and Joe Bucciero conducted a roll call of members and participants in the room and on the conference call. Mr. Bucciero reviewed the need to comply with NERC's Antitrust Guidelines. The Chair reviewed the meeting objectives and Bob Jones, facilitator, reviewed the proposed meeting agenda. On Thursday morning the SDT approved without objection the meeting summary for the December, 2009 meeting in Little Rock.

The Chair thanked members for their diligence, dedication and participation through the holidays to prepare the finalized draft of Version 3 of the CIP-002 to 009 Standards for balloting. Stuart Langton reviewed the SDT work plan, in particular the parallel effort of developing security controls while preparing Version 4 of the CIP-002 standard for posting for an informal comment period. The Chair noted this was her last meeting on the Team and that Jeff Hoffman from the Denver Office of the U.S. Bureau of Reclamation was being recommended to the NERC Standards Committee to serve as a member on the SDT. Joe Bucciero noted that Christopher Peters has submitted his resignation from the Team, and that Patrick Leon (Patricio Leon Alvarado) from Southern California Edison is also being recommended to serve as a member of the SDT. Mr. Bucciero noted there are two remaining open SDT member positions and invited members to talk with potential candidates and have them submit membership nomination forms.

Joe Bucciero provided an update on CIP 002 filing process and some reflections on lessons learned. He recounted that the NERC standards managers reviewed and discussed format and other changes to the standards following the SDT adoption of the CIP002-4 draft in Little Rock. Due to the press of the holidays and the FERC imposed deadline for posting, there was little time available to communicate with the SDT leadership and team members regarding the rationale for the NERC proposed changes. NERC agreed to withdraw many of the proposed text changes and submit them as comments during the informal comment period. Going forward, NERC has assigned Howard Gugel to the Team so he can improve coordination with NERC standards managers and provide direct format assistance in the Team's drafting process.

The Chair noted that yesterday Dave Norton circulated to the Team the release of a preliminary draft of the NIST Interagency Report (NISTIR) regarding the work of the Cyber Security Coordination Task Group (CSCTG) established to help define the cyber security requirements for the smart grid. The NISTIR document is planned to be finalized later this Spring. Keith Stouffer noted that there are over 300 people with seven working groups involved in the CSCTG. It will become a standing committee that is part of the Smart Grid Interoperability Panel (SGIP) that has been created by NIST as part of their work in response to EISA 2007. Keith also noted the draft NIST interoperability roadmap was recently released on January 19.

Gerry Adamski, director of NERC Standards noted he is working with the new NERC Communications Director, Carl Dombek and will share a draft plan with the Team later in the week. The Chair suggested that Carl Dombek be able to come to a future SDT meeting to brief the SDT and provide an update on the progress with implementing the communication plan. The Team agreed that the industry webinar addressing the draft CIP-002-4 standard should take place on February 3 from 1:00-3:00 p.m. EST to allow for industry feedback and questions on the new approach to this standard. SDT Vice-Chair, Phil Huff, agreed to serve as the contact for the Team's effort in developing the webinar materials, and Sharon Edwards and Jay Cribb will be the SDT presenters for the webinar.

On Tuesday morning, Scott Mix and Howard Gugel from NERC briefed the Team on the development of a security controls drafting template.

Phil Huff provided an overview of the SDT effort since Little Rock to develop a draft strawman including development of a security controls member survey created by the SDT leadership; a summary of the responses to the survey by 16 members compiled by the staff; a SDT conference call on January 6, 2010 to consider the member survey results and create and charge a drafting group; and two strawman drafting team meetings were assigned to develop a strawman document. The strawman document contained: Security Control Drafting Principles to provide guidance in drafting security controls and ensure more consistent outcomes among sub-teams; Security Control Groups having the relevant CIP 003-009 and NIST SP 800-53 families mapped including: Security Governance; Personnel and Training; Communication Protection; Physical Security; Systems Management; Incident Response; Recovery Plans; Access Control (Technical); Audit and Accountability; Configuration Management and System Lifecycle; Information Management; and Security Assessments.

Phil Huff noted that the first ten principles are drawn from NERC rules of procedure. The Team reviewed principles 11-15 and offered suggestions for refinements.

Phil Huff outlined the control group categories in the strawman draft. The Team reviewed the proposed six sub-teams in the strawman document including: Security Governance; Personnel and Physical Security; Operations Security; Recovery and Response; Access Control and Auditing; and Change Management, System Lifecycle and Information Management. On Tuesday morning sub-team preference forms were distributed to the members in the room and electronically to those participating via the Ready Talk conference facilities. Based on the preference form, the Sub-Teams were created.

Phil Huff reviewed the strawman guidance for the sub-groups. Following the initial Sub-Team reports on Wednesday, the Team discussed the implications for the ultimate standards/control format and for the further development of security controls in the context of CIP-002-4. On Thursday morning, the Team discussed whether the proposed "control group" format should be the organization for revising the current CIP 003-009 or just a starting point for the Team's work on security controls. The Team discussed the strengths and weaknesses of three choices going forward: using the current CIP Standards, the NIST SP 800-53 format, or the DHS security controls structure. Following the discussion, the Team considered and tested a fourth option of preparing the requirements first then determining the format going forward. Using the following 4-point acceptability scale, the Team decided to proceed first to create the requirements and controls and defer the format options review until having completed that task.

Prepare Requirements First, then Decide on Format

Acceptability Ranking Scale	***4** = acceptable, I agree*	***3** = acceptable, I agree with minor reservations*	***2** = not acceptable unless major reservations addressed*	***1** = not acceptable*	***AVG.***
	9	**6**	**0**	**1**	**3.3 of 4**

The Sub-Teams met on Wednesday morning and early afternoon and then reported their initial results on the review of selecting candidate controls from the DHS catalogue. The Sub-Teams met for a second time on Thursday morning and early afternoon to review security controls and begin exploring the drafting of requirements.

Prior to the second sub-team break-outs on Thursday morning, the Team agreed on a sub-team format for collecting information with the following columns:

1. SDT Team Name
2. Section #
3. Title
4. NERC Security Guidance
5. NERC CIP-2
6. NIST SP 800-53
7. CSO 706 SDT Applicable
8. SDT Comments
9. Validated 706 SDT Applicable (Yes/No)
10. Existing CIP Requirement Cross Reference
11. FERC Order 706 References (Paragraph #s)
12. Requirement Definition
13. Controls- High
14. Controls- Medium
15. Controls- Low
16. Applicability- Transmission
17. Applicability- Generation
18. Applicability- Control Centers

Over the three days the sub-teams met first to identify candidate DHS Security Controls and then to identify controls and draft requirements. The sub-teams and their members included:

1. Security Governance and Assessments *(Gerry Freese, Jon Stanford, Rich Kinas)*
2. Personnel and Physical Security. *(Doug Johnson, Rob Antonishen, Kevin Sherlin).*
3. Operations Security *(Jay Cribb, John Varnell, Jackie Collett & Jim Brenton)*
4. Recovery and Response *(Jeri Domingo Brewer, Jason Marshall, Joe Doetzl, Scott Rosenberger)*
5. Access Control and Auditing *(Sharon Edwards, Phil Huff and Jeff Hoffman)*
6. Change Management System Lifecycle and Information Management. *(Dave Revill, Keith Stouffer and Bill Winters)*

On Friday morning, following the sub-team reports, the Team offered reflections on the sub-team exercise. Following the sub-team reports, the facilitators presented and the Team reviewed and refined the next steps and assignments emerging from the meeting including steps for the Team as a whole, security control sub-team assignments, and steps in the CIP-002-4 review and refinement process.

Scott Mix presented a revised proposed schedule for CIP 002 and the security controls requirements *(See Appendix #5).* The Team liked the presentation in which the two efforts are put in parallel columns and shows the amount of work ahead.

Vice-Chair, Phil Huff reviewed some questions that the Team discussed for FERC/NERC meeting on January 28, 2010, including:

1) What expectations are there regarding coordination with the Smart Grid CSCTG (Cyber Security Coordination Task Group) product and how we use NIST SP 800-53/DHS Catalogue?
2) NIST SP 800-53 is an organizational risk management framework, which allows for tailoring and compensating controls. However, FERC Order 706 calls for extensive oversight for any exceptions. What are their thoughts on reconciling these seemingly conflicting objectives?
3) The process to make modifications to the Standards through a FERC Order is very resource intensive. Conversely, changes made prior to industry balloting are done with relative ease. Is it possible to have a process where the team can receive feedback from FERC prior to ballot?
4) To what degree can we remove or lessen prescriptive elements in the current CIP Standards where the risk reduction does not justify the consumption of industry resources?
5) Have we captured all of the directives from Order 706 in the filing made in December 2009?

He noted this was a working list which will be circulated for members to suggest additions in advance of the January 28 FERC/NERC meeting.

The facilitators noted that each sub-team should plan on meeting in the interim (between meetings) and on preparing and presenting at the February 2010 meeting in Austin a short progress report including key questions for presentation. The Austin meeting will primarily focus on refining CIP-002-4 in response to industry comments received from the informal comment period (ending February 12). NERC will try to have Maureen Long attend a portion of the Austin meeting (preferably on Thursday) to address the response and refinements of the CIP-002-4. The primary objective of the Austin Meeting is to have the Team reach agreement on CIP 002 as revised for posting for 45 day formal comment period.

On behalf of the SDT, Phil Huff thanked Jeri Domingo Brewer for her leadership over the past 16 months. Ms. Brewer acknowledged the opportunity to get to know the SDT members and noted the honor of having worked with them to produce excellent and timely outcomes. She urged the Team to continue to build on the foundation of trust and collegiality to complete the task assigned by December 2010.

Mr. Huff then thanked Dave Revill for hosting the meeting and providing excellent support for this critical meeting.

The SDT adjourned at 12:30 p.m. on January 22, 2010. Several sub-teams continued to meet following lunch on Friday afternoon.

MEETING SUMMARY

I. AGENDA REVIEW, WORKPLAN, UPDATES AND COMMUNICATION PLAN

A. Agenda Review

On Tuesday afternoon, the Chair, Jeri Domingo-Brewer welcomed the members and Joe Bucciero conducted a roll call of members and participants in the room and on the conference call *(See appendix #2*). The Chair reviewed the meeting objectives and Bob Jones, facilitator, reviewed the proposed meeting agenda *(See appendix #1*). On Thursday morning the SDT approved without objection the meeting summary for the December, 2009 meeting in Little Rock.

Mr. Bucciero reviewed the need to comply with NERC's Antitrust Guidelines *(See Appendix #3).* He urged the team and other participants in the process to carefully review the guidelines as they would cover all participants and observers. He urged all to avoid behaviors or appearance that would be anti-competitive nature and also reminded the group of the sensitive nature of the information under discussion.

The Chair thanked members for their diligence, dedication and participation through the holidays to get the draft finalized and ready for balloting. Stuart Langton reviewed the SDT work plan (*See Appendix # 5)* in particular the parallel effort of developing security controls while finalizing the CIP-002 draft for balloting.

The Chair noted this was her last meeting on the Team and that the Standards Committee was going to appoint Jeff Hoffman from the Denver Office of the U.S. Bureau of Reclamation to serve in her stead. Joe Bucciero noted that Christopher Peters had submitted his resignation from the Team. The Standards Committee has appointed Patrick Leon (Patricio Leon Alvarado) to the SDT from Southern California Edison, who has the lead for CIP NERC compliance in terms of their substations and also has considerable substation planning experience. He will join the Team at its Austin meeting. Mr. Bucciero noted there were two open spots and invited members to submit potential candidates.

B. Lessons Learned- CIP-002-4 Posting

Joe Bucciero provided an update on CIP 002 Filing process and some reflections on lessons learned. He noted that much has been learned since this Team was formed in the Fall of 2008. He recounted that the NERC standards managers following the SDT adoption of the CIP002-4 draft in Little Rock reviewed and discussed format and other changes to the standards but due to the press of the holidays and the deadline for posting did not adequately communicate to the SDT leadership and team members the rationale for proposed changes. NERC agreed to withdraw many of the proposed text changes and submit them as comments in the informal comment period.

Going forward, NERC has assigned Howard Gugel to the Team so he can improve coordination with NERC standards managers and provide direct format assistance in the Team's drafting process. Joe Bucciero agreed to circulate to the Team documents that lay out the new approach for standards drafting. Mr. Bucciero noted that NERC's leadership change with a new President stepping in was a factor.

Member Comments

- Going forward the Team will be struggling to get the documents to a point we can agree on them as a group – there may not be enough time for NERC staff review – may need to change the

process to allow for staff review and then committee review and agreement before it goes to ballot.
- We should not face this in the future since Howard will to help coordinate the issue to reduce the problem in the future

C. Cyber Security Initiatives Updates
The Chair noted that yesterday Dave Norton circulated to the Team the release of an intermediate draft smart grid work of the Cyber security coordination task group to be finalized later this Spring. Keith Stouffer noted that there are over 300 people with seven working groups. It specifies security standards at multiple points and is a list of requirements rather than baselines. Keith also noted the NIST roadmap for operability was also just released on January 19.

Member Comments
- Need to continue to coordinate between our group and theirs to be sure not developing incompatible requirements
- The Team may want to consider forming a task group looking specifically at the Smart Grid work to be sure our work is compatible and not at odds or creating issues.
- Add agenda item for Wed. or Thurs. for discussing how we can interact or interface with that group?
- Can we feed our work back to that task force as we move forward?
- Another item – critical cyber security identification guideline is now out for formal comment. This is a formal guideline development process, not a standards development process despite the similarities.
- U.S. nuclear plants – NERC needs to file version 2 implementation plan – how version 2 and 3 will be applied to nuclear plants – Commission says implement on same time line as version 1 – The order says future orders must include how nuclear plants are expected to apply

D. NERC Update on Implementing the CIP Communication Plan
Gerry Adamski, director of NERC Standards noted he is working with the new NERC Communications Director, Carl Dombek and will have a plan to share with the Team later in the week (*See Appendix #9)*. He noted the need to set a date for a CIP 002-4 webinar in early February. He noted that NERC is not expecting this Team can take the lead in developing and implementing a communications plan. The Chair suggested that Carl Dombek may be able to come to a future SDT meeting to brief and provide an update on progress with implementing the communication plan. The Team agreed the webinar should take place on February 3 from 1:00-3:00 p.m. EST to allow for industry questions. SDT Vice Chair, Phil Huff, agreed to serve as the contact for the Team's effort in developing the webinar materials. Sharon Edwards and Jay Cribb will be the SDT presenters.

E. Review of NERC's CIP Security Controls Drafting Template
On Tuesday morning, Scott Mix and Howard Gugel from NERC briefed the Team on the development of a security controls drafting template. Mr. Gugel noted that one key is for the Team to decide how much granularity they want to work with and suggested it will be easier to start with the broader high-medium-low categories. He also pointed to using a table format that would be referenced by each requirement. Other points made included:

- Requirement statements can be very short and simple: e.g. you shall implement passwords subject to attachment # 1. The entity looks in the attachment to determine if you are high, medium or low, then look at details for compliance. There remains a question as to whether compliance is assigned to a column or row versus to an individual cell in the table.
- Requirement could speak to applicability and the attachment would catalogue the controls.
- The example is divided just to indicate whether or not you need different types of controls for transmission, control centers, generation, etc. It also breaks it down to look at whether it is manned or not which may affect the mapping of controls needed.
- Third example is just "high BES impact" with granular of physical access, monitor physical access or logging physical access
- Control centers have a lot more for virus protection than a remote center – then break it down into transmission, production or control – don't need virus protection of a relay (though those with windows platform may need some)
- The Team should consider the VSLs as you are writing requirements – if not, there is a disconnect and you may find you did not write the requirements as clearly as you should have
- The proposed concept will work best for this Team and this is the direction overall NERC and the industry needs to be headed in. In addition it is easier to follow.

Member Comments

- Suggesting just one VSL level for each of the h-m-l categories? No – associated with each requirement is a set of VSLs
- Each violation has a risk factor – but this is not a one-to-one relationship.
- Do you have a prototype we can look at? Not yet.
- We need to look at the violation severity and have clear cut controls. 90% of the effort should then be aimed at highest level impact.
- If it is a high impact it needs to be protected. It should not be important to determine whether it is transmission or control center or other. It is the impact on the BES that is important.
- I like idea of doing the VSLs at the same time to allow us to fine tune the requirements and be sure they are auditable.
- This just shows how to map each requirement – may not have a direct tie to a VSL
- Are these several different models to use together or are we choosing one over the other?
- The concept is good – this might be useful once we decide which controls are in the buckets of h-m-l. Your suggestion makes implementation simpler.
- If you have a table do you still have just one requirement or does the table represent Sub-Requirements? This is an open question at this point
- Is there a NERC style guide for VSLs we should reference? There is but it does not assume the complexities of what we are looking at here.
- I think the VSLs need to be more granular than the requirements. VRFs should be easier to assign to impact levels than VSLs.

- We should consider creating a litmus test to use as we move forward.
- Should we count one miss the same as multiple misses of the requirement?

II. SECURITY CONTROLS AND THE STRAWMAN DOCUMENTS

A. Overview of Security Controls Strawman Document and Drafting Group Process

Phil Huff provided overview of the SDT effort since Little Rock to develop a draft strawman. This included a:

- Security controls member survey developed by the leadership in December, 2009;
- Summary of the responses by 16 SDT members compiled by staff, *(See Appendix # 6),*
- Full Team conference call on January 6, 2010 to consider the member survey results and create and charge a drafting group, and
- Strawman drafting team which met twice on January 11 and 14, 2010 to develop and bring a strawman document to this meeting for the Team's consideration.

He thanked the Team and the drafting team members for their responsiveness in completing the survey and developing a strawman document (*See Appendix #8).* The strawman document contains:

1. Security Control Drafting Principles to provide guidance in drafting security controls and ensure more consistent outcomes among sub-teams;
2. Security Control Groups having the relevant CIP 003-009 and NIST SP 800-53 families mapped including: Security Governance; Personnel and Training; Communication Protection; Physical Security; Systems Management; Incident Response; Recovery Plans; Access Control (Technical); Audit and Accountability; Configuration Management and System Lifecycle; Information Management; and Security Assessments
3. Drafting Sub-Teams based on the control families:

Team	Control Families
Security Governance	(1) Security Governance
Personnel and Physical Security Operations Security	(2) Personnel and Training, (4) Physical Security (3) Communication Protection, (5) Systems Management
Recovery and Response Access Control and Auditing	(6) Incident Response, (7) Recovery Plans , (12) Security Assessments (8) Access Control, (9) Audit and Accountability
Change Management, System Lifecycle and Information Management	(10) Configuration Management and System Lifecycle, (11) Information Management

4. Team assignments to determine the security controls within their assigned control families necessary to mitigate risk to the BES. Begin by taking the set of applicable Requirements from version 3 CIP Cyber Security Standards and reconcile with applicable NIST SP 800-53 security controls. Then incorporate additional sources where applicable to mitigate unacceptable risk to the BES functions. The initial work product should be a set of security controls with applicability to high, medium and low impact Cyber Systems and how specific FERC directives have been

addressed *(as indicated in Appendix A: FERC Directives from Order 706).* Additionally, for each security control:

- State how the security control reduces risk appropriate to the impact categorization *[Drafting principle 11]*
- State how an objective third party with knowledge or expertise in security can measure the control *[Drafting principle 4]*
- State the rationale for making changes from previous versions [*Drafting principle 12]*
- Denote the applicability to (1) Generation Subsystems, (2) Transmission Subsystems, and (3) Control Centers. Provide clarifications or enhancements where necessary to meet the security control objective in that environment *[3.2 acceptability among survey respondents]*.
- Denote the priority for the security control relative to the risk it mitigates (i.e. P1, P2, P3, None). *[SP800-53 introduced this in version 3, and it could help in developing VRFs and implementation plans]*
- Denote applicability for differing vulnerability and threat profiles.
- Write controls based on risk profile (as well as impact categorization)
- Denote applicability for general purpose vs. proprietary operating systems.

5. Security Controls for Impact Categories with basic premise that the cost to implement security controls should reflect the reduction of risk to the BES commensurate with the impact category. The industry as a whole should first focus on mitigating the greatest amount of risk.
6. NERC CIP/NIST SP 800-53 will serve as the baseline and SANS, ISO, DHS, and ISA-99 provide supplemental or amplifying guidance.

B. Drafting Principles

Phil Huff noted that the first ten principles are drawn from NERC rules of procedure. The Team reviewed 11-5 and offered the following suggestions.

11. Reduce Risk [**3.5 acceptability among survey respondents**] **–** Security controls reduce risk appropriately for applicable BES impact categories.

Member Comments and Suggestions

- Depend on an entities implementation? Yes, but assume that we will be making risk decision of what is minimum acceptable for reducing risk as we develop the standards.
- This one deals again with what is high, medium and low.
- Throwing around "risk" a lot – There is a complaint that we use "risk" but cannot qualify it, nothing to document what we are doing reduces "risk" – show me how it is a "risk"? How do we justify using the word if we cannot quantify it
- Same problem with #11 – current standards assume a positive benefit from any effort to reduce risk – in federal model you perform risk assessment and decide whether what you are doing is acceptable.
- Need to clarify the level of organizational risk that applies – but have to have an industry baseline and justification that this is appropriate and reduces risk as we understand it in the industry.
- What are the threats we trying to counter so we know what to put into place to address it
- As we identify a control, we must assume controls reduce risks?

- We cannot do a risk assessment for the whole industry.
- Discussing the outcomes of having controls – this may be the overarching goal, rather than a principle.
- May need to define "reduce risk" – what is the intent of the controls? Reducing risk may be an outcome
- The list is intended as measure of review of the draft products of each group.
- Under the survey the question asked if it would be appropriate to document how the controls reduces risk. That is covered in the next section
- Cannot prescribe controls and quantify specific results – it is the controls as a whole?
- My concern is with the word "reduce." Reducing from what? Have to have a starting point.
- Talking about overarching principles which is fine but on page 4 asking each group to begin with a statement of the risk and we may get back into the circular argument – need to establish and clarify why we are offering a control. We will need to have some reason why requiring the industry to do this.
- If we do this for every control, we may get bogged down given the 200+ items listed – may simply need the justification for a category of controls rather for than each individual control.
- We need sound reasoning for why we are or not including a security control.
- We need to be sure we are not expecting a control to reduce a high risk impact is also applicable to a low impact item too.
- Need a principle that we need appropriate controls that are applicable to a category – controls that are appropriate and applicable – rephrase the principle so as not to lose that thought?
- Is #11 the same as #14? Not the same, as #14 is intended to avoid all of the compliance effort being aimed at low levels.
- "Security controls shall be appropriate for applicable BES impact categories."
- "Security controls shall be commensurate with identified level of BES impact categories."
- As a guiding principle this is fine – the Team understands the intent of this principle.

12. **Change Documentation** [**3.3 acceptability among survey respondents**] – Changes from prior versions of CIP Standards have clear rationale. These include the following types of changes:
    a. Above and beyond the current standards
    b. Removal of requirements
    c. Major formatting changes.

Member Comments

- We cannot pass anything that doesn't give a roadmap from how to get from version 2 to 3 to 4 – if we drop something along the way we need to justify it.
- May want to test and get validation from NERC staff before finalizing – make this part of the communication plan? Note that staff cannot speak for the commission
- Industry will want to know why it appears we have gone from asking them to do 40+ things to 200+ things – may be the same or less total work even if more items.

13. **Reduce Administrative Overhead** [**Suggested principle**] **–** Administrative documentation kept to the minimum that is necessary to verify acceptable risk.

Member Comments

- How do you measure compliance? If you reduce documentation? NERC and regions may make up what you need. We should be all for reducing documentation, but we have to show compliance.
- Currently, you are out of compliance unless through documentation you can prove you are in compliance.
- Documentation needs to be rational but we probably cannot completely eliminate documentation.
- No matter how much documentation we have, it seems it is never enough to completely prove compliance – documentation is always subject to interpretation. We must make this more precise
- As worded the principle is what you want – have to have adequate documentation but not more than needed.
- Cut off the principle after "necessary"?
- Also federal performance audits actually improve security.

14. **Priority [Suggested Principle] –** Implementation and compliance with the Standards are prioritized according to BES risk. The industry should focus on mitigating the greatest risk (i.e. not spend the majority of our resources on the low-impact Cyber Systems).

Member Comments

- We can't just bite off little parts – adding priorities may be done differently depending on your processes.
- Priority built in already – is this going after impact levels rather than risk? Prioritize based on BES impact. Prioritizing could be handled through the implementation plan followed by a compliance plan.
- Need to just remove – already categorizing into high, medium, low – that set priorities, still have to get to the low too.
- Replace "risk" with "impact" – how do we focus on "high impact" to get most bang for the buck. It may important enough to do, but perhaps not important enough to test? Simply remove "and compliance" from the sentence?
- *(*Parking Lot item)* Can small entities leverage the work of others? Should we allow them to? Ballot body may be more amenable if we do this.
- What is the mechanism that allows them to do that since audits cannot be shared?
- These are principles for the Team to use moving forward, and are not for the industry: strike the second sentence?

15. **Minimize TFEs** [**Suggested principle**] **–** Security controls should minimize the need for TFEs

Member Comments

- What is the principle or goal? To eliminate TFEs? It is clear that the TFE process is broken – should be striving to eliminate the need for TFEs.
- TFEs were an end run on the requirements – reword standards to eliminate the need for an "end run."
- Allow for controls to mitigate and document for older equipment that cannot meet all the requirements – call it whatever you want.
- TFE is an existing term and process – eliminate the need for TFEs – replace with an effective exception process. We will still have a need for exceptions. Add compensating controls?
- TFE grants safe harbor from retroactive sanctions – can we write any exception without such retroactive protection? Are we constrained by the current process? This is a question for NERC.
- "Mitigating controls" vs. "Compensating controls" are very different terms.
- There may be a place for exceptions, but not the current TFE system that has been misused.
- Reasonable to expect there will need to be some exceptions – we cannot write a standard that will cover all possibilities.
- Issue is over the word "exception" rather than the concept or need for them. We know there will be instances where an entity cannot meet the letter of the standard – remember these standards are mandatory.

C. Control Group Categories

Phil Huff outlined the control group categories that the strawman draft proposed depicted below:

ID	Control Group	NERC Standard	NIST SP 800-53 Family
1	Security Governance	CIP-003 – R1, R2, R3;	Planning, Risk Assessment, Program Management
2	Personnel and Training	CIP-004 – R1, R2, R3	Awareness and Training, Personnel Security
3	Communication Protection	CIP-005 R1, R3	System and Communication Protection
4	Physical Security	CIP-006 R1 through R6	Physical and Environmental Protection
5	Systems Management	CIP-007 R2, R3, R4, R6	System and Information Integrity
6	Incident Response	CIP-008 R1 & R2	Incident Response
7	Recovery Plans	CIP-009 R1 through R5	Contingency Planning
8	Access Control (Technical)	CIP-003 R5; CIP-005 R2; CIP-007 R5; CIP 004 R4	Access Control, Identification and Authentication
9	Audit and Accountability	CIP-005 R5, CIP-007 R9	Audit and Accountability
10	Configuration Management and System Lifecycle	CIP-003 R6; CIP-007 R1, R7	Configuration Management, Maintenance, Media Protection, System and Services Acquisition
11	Information Management	CIP-003 R4	Access Control, Media Protection
12	Security Assessments	CIP-005 R4, CIP-007 R8	Security Assessment and Authorization

Member Comments

- Number 12, Security Assessment should be moved up as part of Security Governance (#1)? Yes.
- Access control in #11 different from that in #8? Access to information versus access to systems. Remove access control from #11 as both uses of term covered under CIP 003 R5 in #8.

D. Proposed Sub-Teams

The Team reviewed the proposed six sub-teams in the strawman document including: Security Governance; Personnel and Physical Security; Operations Security; Recovery and Response; Access Control and Auditing; and Change Management, System Lifecycle and Information Management. On Tuesday morning sub-team preference forms were distributed to the members in the room and electronically to those participating on ready-talk. *(See Appendix # 7 Preference Form results).*

Member Comments

- Recognize that the six categories may leave only a couple members per team among members physically present
- Consider combining access controls and operations security?
- Consider having members serve on more than one group? Especially any categories that may need coordination?
- How can we account for those with time available for the group and those who don't? Careful we don't end up with a group of three but none have sufficient time to complete the task.
- Several mappings or cross walks exist already.
- May need to review mapping together as a team to start, then break off to deal with sub-questions
- Would it be beneficial to go through DHS(?) catalogue rather than NIST SP 800-53?
- Mapping exercise? Pull up a control and ask if it is applicable?
- Should we be working toward identifying the plan or approach first?
- Would discussion of High/Medium/Low happen with the mapping discussion?
- What is in the CIP now generally is the high – pare down from there to identify medium – then low.
- We need to draw on varied experiences in the Team to draw conclusions and map the controls. We also need to develop a common understanding by drawing on the groups experience
- Why are we defending against any standard? We were asked to consider NIST, not defend from it?
- Trying to identify gaps and explain why we did not include a particular control or standard
- Simply need to explain why we did not include a type or group of controls
- NIST is a different way of doing things, not directly comparable with existing CIP standards.
- I agree they are different – but looking at different references for ideas that may improve coverage. We should not be looking to make wholesale changes if we don't have to.

E. Review of Required Elements for Each Security Control
Phil Huff reviewed with the Team the strawman guidance for the sub-groups.

Member Comments

- The strawman guidance on high/medium/low was intended to simply offer an example, and is not trying to write the control
- Use high category and pare down from there?
- High/Medium/Low may mean different things when looking at control center versus a transmission subsystem.
- Medium will be a tough category to define.

- E.g. Passwords. May want shorter passwords changed less often for low than for high. The requirement is to use passwords for authentication – do you define the complexity for the level of impact?
- Consider establishing a short succinct requirement and then look to the column and row in the attachment tied to the level of impact.

III. SECURITY CONTROLS FORMAT AND SUB-GROUPS

Following a mid-morning break on Wednesday, the Team reviewed sub-team assignments and then broke out into sub-teams to initially review the DHS catalogue of controls to determine the applicability of these controls to their sub-group categories. On Wednesday afternoon the sub-groups provided initial reports.

A. Initial Format Discussion

Following the reports the Team discussed the implications for the ultimate standards/control format and for the further development of security controls in the context of CIP-002-4.

Overall Comments following Initial Sub-Group Reports on Wednesday

- No equivalency requirements in this one. Looked at requirement and supplemental guidance.
- With a CIP requirement- take side by side. Look for what is different
- JS: FAQ- "access point" defines ESP. Providing traffic control in/out of ESP. Have to have fire wall. Access control-
- Access control and monitoring- on DHS- access control pp 93. Identification authentification of a use etc. for granting access to user. Combine and you have access, authorized access. 3 stages of the process.
- How IT/cyber security- access control. Without a NERC definition of "access control"
- "Network perimeter protection"- visuals upper management. "Guards, gates and guns"- physical and virtual perimeters to explain without jargon.
- Identification and authentification- problematic do not exist in any legacy or modern in any SCADA, ill defined. There will be lots of discussion around this issue. It is possible to authenticate and identify?
- Why no "access control" definition? Disappointed with small number of defined terms.
- Parking Lot issue: Access control.
- Remote access through an ESP. After spot audit. This is an important issue. We need to deal with universally understood concepts, understood the same way. Get away from concepts understood only by a drafting team.
- The problem may be who accepted it?
- NERC defined terms- if we put them in a reference document, they will not be part of the standard.
- Different approach – said yes to good ideas but recognize may be difficult to write a requirement – we did not look to see if already in the CIP, just whether it should be considered "high."

- Go back and agree on the criteria for high, medium, low and then repeat the review to categorize the ones identified by the sub teams.
- Should we have a first draft of the total bucket and then refine the issues? We can then use a standard template to redact high, medium, low.
- Take work done today through a next step to look at words surrounding the possible requirement
- Need to talk about format – how are we going to structure the requirements moving forward?
- Make a change to one standard it ripples through the others – can we make these stand alone? I need more information on how we are going to structure the standard to avoid tripping over each other in sub teams.
- Take one family – a smaller one – and develop a "proof of concept" for putting into a table to establish a template for the other larger families
- Collapsing to smaller number of requirements? Caution, the smaller the number of standards, the more likely we will be out of compliance with a standard.
- Out of compliance with a requirement, not just a standard?
- Agree we should work on one to establish the standard.
- Which one should we utilize?
- The Team should take the .1 in each DHS family as policy to be addressed in the Governance
- We will need to address when a control family crosses over multiple areas
- Need to work on getting requirements into a new format or framework – but collectively need to discuss how to construct the bucket. I.e. what is the control framework? What is preference and what builds clarity and understanding?
- If keeping CIP 003-009, do we keep the policies spread through each or pulled out into a separate stand alone
- May depend on who the target user of the document is – target to field, management, others?
- How do we address generation, transmission or control centers? One size does not fit all – they each have unique requirements – need to make it easy to look up transmission requirements for example.
- Think about the NERC development process and that you need to sell this to through the ballot process to the industry – start with existing and refine and modify from there – otherwise much more difficult to sell to industry
- Our drafting principles call for keeping it close to current structure.
- Page 3 of strawman has a suggested structure in the chart – current CIP003-009 into control groups.
- Small group meet after we adjourn to discuss and develop a starting point for tomorrow's discussion
- Also need to compile the "yes" and "maybe" from the sub teams
- Not suggesting throw the whole structure out but collect common policies together first – shouldn't worry about whether they map one-to-one with current structure – putting policies

together will help us sell to industry the changes – elevate policy and bucket the rest of the controls into appropriate sections

B. Consideration of Security Controls Format Options

On Thursday morning following the sub-groups' first round of meetings on Wednesday afternoon, the Team discussed whether the proposed "control group" format was being proposed as an organization for revising the current CIP 003-009 format or just a starting point for the Team's work. The Team discussed the choices going forward, initially identifying three: using the current CIP, the NIST SP 800-53 format or the DHS security controls structure.

Member comments

- Do we need to have some motion or vote to determine the form we are moving forward
- Need a good strong framework to build on – need to determine today what we will use as the structure – move the pieces around using the structure we have or create a new structure – we struggle with the existing structure – don't like the idea of just moving the deck chairs around – need to resolve and get it behind us
- Need to discuss strengths and weaknesses of each and may need to recognize that option that is not favored may still have an element we want to incorporate
- The Team was called together to fix problems identified by FERC. We need to fix those with the tools available including NIST – order did not call for a change in structure – people are familiar with it and likely to vote in favor – go recognize and go to the relevant R and then the table to understand how to comply – logical layout that is familiar to the industry.
- All of our programs are written in the format to comply with this format.
- Look at existing documentation and how it relates to current model – may be a burden to many to adjust to a new model without any clear payback.
- There will be a significant impact on documentation for any of the options. Yes, have an investment of time and resources in the existing CIP, but we should look at the next 3-5 year result. All of the models under consideration will require a major rewrite.
- Whatever we come up with needs to better than what we have no matter what the format – concern is that the substance is easy to understand and follow regardless of the format
- Are we going to stick with the h-m-l format? Be prepared if comments are universally against that format.
- Expect, like the past, that comments will be across the spectrum of support-nonsupport
- What is "better"? Building a house before we know what type of house we want.
- "Better" means concise, easy to understand and to implement.
- We identified about 90 security controls yesterday – if we have a new access control will we will have to add it in several places producing duplication?
- I assumed the twelve control groups were to be used to help distribute the new items into the current format – this would fix problems without creating new ones
- Stay with current structure or move to a functional model –satisfied with current model or ready to move on to something else?

- Discussed this issue before – writing the standards more like NIST is just one option – rewriting the current standards is not off the table.
- The issue is not NIST versus the current CIP structure. The question is does the current structure work or not. If not, what can we do to improve it? There may be resistance to change, but our task is to make the process better – "we can not keep the system as is and just move the deck chairs around."
- Difference between structure and organization – keep the current structure and the topical references? Same titles and thought processes?
- Yes the topics stay the same but the meat within may change – make the changes fit within that
- With CIP002 not sure fits with the old structures organization
- Where does the functional strawman fit? A new CIP-010 or in the existing CIP 003-009 structure?
- Preferably the latter

Option #1- Current CIP-003-009

Strengths

- Current structure allows industry to meet their respective needs.
- Industry understands system.
- Some industry concerned that proposed CIP002 is turning the world upside down – may need a hybrid to get the industry buy-in and acceptance

Weaknesses

- The current policy mixes enterprise wide policies and technical controls – confusion in implementation
- Number of TFEs and interpretation requests are indicative of some of the issues/problems with the current CIP.
- Focus on compliance versus performance assurance – some are focused solely on compliance and documentation, not measurable improvement in security.
- Core problem with current organization – topics are okay – but cannot understand and implement because we have moved away from commonly understood industry terms – key is in CIP005 and concept of perimeter and security enforcement mechanism.

Member Comments

- Are we here to fix the system or to change the terms of art?
- Keep the discussion on the structure – if task is to reword the current structure we could have done that long ago – are we tasked with redeveloping the standards for the industry or not
- Here to write a new standard or not?
- Not advocating keeping current structure as is – suggesting start with CIP 003-009 and reorganize as needed while keeping basic structure, can still have new Requirements – functional controls would fall into a table pointed to

- For existing structure option, will this allow us to still move things around? Yes, in particular to adjust for CIP 002. The table(s) still have to be tied to a standard.

Option #2- DHS standard

Strengths
- DHS leverages the work already done by the industry.

Weaknesses
- If move away from current structure, logistic issue of retiring all the current standards and start with CIP010 – for a couple of years there is potential for confusion – can keep current system and cross reference.

Member Comments
- Do we need to move away for question of documentation and talk about the technical difficulties of implementation?
- Where does electronic perimeter for a system begin and end? Left with an organization-by-organization determination of what and how to implement and hope you pass the audit – equipment out in the field what type of protection does it need – have to create things that do not exist today in order to comply for an audit.
- Cannot measure art – just because a group creates a strawman does not mean it is the right structure or just a pile of hay – security perimeter was created in 2002 at the request of FERC – our CIP-002 changes focus and sets the basis for h-m-l standard to bring focus of resources on the high.

Option #3- Strawman Approach

Strengths
- The strawman doesn't completely abandon the system understood by the industry – we identified 53 more controls yesterday – the strawman will accommodate the large number of new additions.
- The strawman offers a more logical grouping – not necessarily the final format –
- Group should not lose sight of the fact the strawman drafting group proposed and eleven-group structure.
- Talking about structure only, not content – the change shouldn't matter if it is easier to understand and implement – it is the substance not the structure that should matter.
- This format does leverage industries work and is not a radical change.

Weaknesses
- The more cross referencing you have, the greater opportunity for confusion – get caught in a repeating loop or circular logic –

Option #4- Prepare Requirements First, then Determine Format

The facilitators suggested an acceptability ranking of the three options. Several members suggested a fourth option which the Team tested.

Member Comments

- Can we right the requirements first, then find the model that fits them – I don't know what the right model is until I know what the parts are – a fourth option?
- Core issue is whether we stick with current structure or look for something different
- Prepare Requirements first?
- Don't know enough yet to know what structure we need
- Still too much unknown at this point – hopefully out of the drafting effort to develop requirements and controls will give us better idea of which format works best.
- Defer the format question until after drafting requirements. The Team will return to this by the end of March meeting

Prepare Requirements First, then Decide on Format

Acceptability Ranking Scale	***4** = acceptable, I agree*	***3** = acceptable, I agree with minor reservations*	***2** = not acceptable unless major reservations addressed*	***1** = not acceptable*	***AVG.***
	9	**6**	**0**	**1**	**3.3 of 4**

As a result of strong support for preparing the requirements first, the Team decided not to rank the acceptability of three options.

C. Subgroup Meetings and Reports

The Sub-groups met on Wednesday morning and early afternoon and then reported their initial results on the review of selecting candidate controls from the DHS catalogue. The Sub-groups met for a second time on Thursday morning and early afternoon to review security controls and begin exploring the drafting of requirements.

Prior to the second sub-team break-outs, the Team agreed on a sub-team format for collecting information with the following columns:

19. SDT Team Name
20. Section #
21. Title
22. NERC Security Guidance
23. NERC CIP-2
24. NIST SP 800-53
25. CSO 706 SDT Applicable
26. SDT Comments
27. Validated 706 SDT Applicable (Yes/No)
28. Existing CIP Requirement Cross Reference
29. FERC Order 706 References (Paragraph #s)
30. Requirement Definition

31. Controls- High
32. Controls- Medium
33. Controls- Low
34. Applicability- Transmission
35. Applicability- Generation
36. Applicability- Control Centers

1. Security Governance and Assessments *(Gerry Freese, Jon Stanford, Rich Kinas)*

a. First Break Out- Identifying Candidate DHS Security Controls

- Note that the DHS doesn't call out "document" something such as CIP does
- Does in other areas
- In this area we may need to add "document" where appropriate
- Either cover globally as an opening statement or try to address where needed
- Cannot have implied documentation – must be called for in specific requirements – but should call for documentation where needed
- Do you have to document how you plan to document compliance?
- Assurance frameworks – federal standards referenced
- Excluded 2.2.5 and 2.2.6 – why?
- This has a federal slant to it – not that you shouldn't cover third parties but it is covered earlier in the standard – if write correctly then you can cover the third party situations in other areas
- DHS catalogue has a federal flavor and context
- Under NERC policy you cannot enforce on a third party except contractually
- Statute disallows you requiring a third party compliance – NERC cannot come in and obligate a vendor to follow requirements – NERC can only audit the registered entity
- Question mark by 2.7.1 – hard to put into CIP context and put into a requirement – the planning requirement in DIP is only implied –
- Concept of planning is good but coordinating between physical security and cyber security is very difficult
- Good placeholder item about how to deal with this one
- Know what is wrong but not sure how to fix it – strategic planning for security is a good idea, especially at a regional level – but need to be realistic, logical and not burdensome to individual entities – may fall outside these standards
- Can't write a standard to a functional model that does not exist yet – maybe CIP 10 is regional security coordination – make sure we are not creating work to create work – how do you craft requirement so they can be measured and audited for compliance? – but this idea into the parking lot for later consideration
- 2.17.4 – no? may want to parking lot "best practices" as a guidance document – agree it is not a requirement question

- If something is in the standards today then we were suppose to be reluctant to pull it out – is that true across the board – appears here that we may be pulling out items already in the standards
- Second to last column in the appendix has the CIP standards reference – need to gut check whether a few of these are included as topics rather than in intent of the requirement – needs a critical eye with as needed explanation as to why it is pulled out
- Vulnerability assessments included in several places – wording may not be the same – some of these no's should not be completely discounted – example is 2.17.2 and 2.18.4
- 2.18.11 and 2.1812 cover the issue
- risk management? Can only protect 90% - not writing controls to defeat your adversary – are we doing it justice if we throw it out
- reducing risk to an acceptable level to manage
- security control someone is looking for new threats and addressing them in a different way than we do today.
- That is part of risk management and risk decisions
- Is there a way to address risk management through the requirements? Put into the parking lot: a way to role risk management framework into the CIP requirements
- 2.18.6-10 are out
- 2.19.1??
- creating a whole new entity or beauracracy? – federal entities already have this – can we address this outside the federal context – parking lot: entity controls or common controls across entities
- there is a role for a forward looking plan – not sure how you audit or measure it
- can this be part of the assessment phase?
- 2.19.3??
- federal context this is identified – seems like a good idea – not sure how it applies to the private context; how it would look
- may have issues of measurement and enforcement – may be a good business practice but not in the requirements – same may be true of 2.19.2 –
- push back on "senior manager" from industry and this is even more prescriptive
- 2.19.5 already captured in CIP 002 – so it is a "no" here – it is here but only as a federal mandated response to specific legislation –

b. 2nd Break Out- Identifying Controls and Drafting Requirements

- Went through controls again but did not cross walk with CIP – will look back through CIP once have initial set
- Kept "organization" rather than "responsible entity"
- Reviewed requirement definitions – may have to adjust language to fit CIP

- 2.2.1-.3 pulled up into 2.1.1 language
- 2.2.4 belongs in the response section
- 2.7.1 – said no as is – 2.7.2 develop a security plan – not much changed from DHS – if we keep ESP then need to go back and reference here
- Did not include change to BES cyber system.
- Enterprise architecture? May not want that concept – the concept was a response to Federal law – left here until we determine if and how we want to address across other areas too
- the controls in this case are the requirements
- 2.7.10 – plan update
- May need to be prescriptive here using the table
- 2.17.1 – changed to NO and removed as too cumbersome – noted as a "?" in the first pass – not much benefit and anticipate huge push back from industry – difficult to monitor or test
- 2.18.5 – control system connections – difficult to take federal concept into the CIP/BES mind set – many vendors require a connection into your system to service their equipment – may need some assurance at both ends – should at a minimum document the relationship exists
- This is a mutual distrust, defend against friend and foe – that is where the concept of ESP comes in
- Opening a hole to a vendor
- Discussed as a team and pushed the issue over to security operations.
- 2.18.2 moved up above
- 2.191 captured in global policy
- 2.19.2 removed as too directive – may damage most organizations in terms of accountability
- 2.19.3 removed
- Figured out the first requirement – looked primarily at the DHS catalogue but making adjustments to language as needed
- Policy that addresses issues out of CIP002
- Assuming .1 requirements are being put into a policy section of CIP 003 – went through 2.1 and listed the policy and the sub-policy under it
- Also reviewed NIST language to see if it works in CIP context
- Illustrative example in 2.7.1 – document to explain a document? A policy that points to a program that may not exist?
- Thinking we may need to take this out – current words has a federal only context
- Do we change the CIP requirement?
- Look at 2.2.2 – high level policy set out in 2.2.1 – if leave this one in as a requirement may be adding layers of bureaucracy – this may be an opportunity to clarify, simplify and make it more implementable

- Eliminated some sub areas identified yesterday
- Tidy up and scope DHS language. Go back later and look at existing CIP- and drafts and lift all the ".1"s up.
- Instead of "Organization" will use Registered Entity (RE) consistently.
- The Sub-Team requested that Dave Norton join their team. Chair and Vice Chair also suggest checking with John Lim to see if he might join when he returns.

2. Personnel and Physical Security. *(Doug Johnson, Rob Antonishen, Kevin Sherlin).*

a. First Break Out- Identifying Candidate DHS Security Controls

- Covering DHS 2.8 Operations Security; 2.11 awareness training; 2.4 Physical security; 2.10 system maintenance; and 2.14 System integrity
- How should we pick up current CIP requirements that have no equivalency in this section? "Leadership" e.g. doesn't belong in CIP 003. How to ensure these get captured.
- "The designated manager" is a generic reference.
- Exceptions- CIP requirements- no explicit treatment of this in the DHS.
- Does this go in governance?
- 706 order- define- "parameters of exceptional circumstances" needs to go somewhere? Back in Governance?
- Factor in outstanding interpretations for current CIP standards.
- Reassessed the validity of the DHS judgment on CIP- couple dropped, with a couple back in.
- Some in other groups? E.g. ".1" policies
- Got to one requirement- personal screening. Looking to draft less on the how and more on the what.
- Principle: Wording of standards- similar wording in both- conceptually equivalent. Stick with old CIP wording where possible unless 706 requires otherwise.
- Principle- keep the detail level of the current CIP.
- Consistent with Access Control.
- Shortening up requirements.
- 2 ways to write requirement. The responsible entity shall have a program …consistent with state, federal. (consisting of placed somewhere else).
- Howard G:
- All go in the requirement, unless there are going to be differences between H/M/L and environments.
- FERC says improve the reliability standards.

- By adopting the standards, we said this is acceptable for reliability. For making less restrictive.
- E.g. if we were to scrap 7-year refresh. Or change to 10 years, we would need a compelling reason. Change to 5, i.e. strengthen it and you will be fine.
- FERC just approved TFE filing but requires a compliance filing. Within 90 days. Put those 2

b. 2nd Break Out- Identifying Controls and Drafting Requirements

- Started working on personnel security and training (2.3 DHS). Started with CIP and noted where changes made and suggested additions.
- They have some of the FERC order items in the mix.
- We will need to go into the determination high/med/low ahead.
- Need to get into the Physical security side. (2.4 DHS).
- 2.11- awareness training and training before access.
- Sub-team will get with the Access Control and Auditing Sub-Team.

3. Operations Security *(Jay Cribb, John Varnell, Jackie Collett & Jim Brenton)*

a. First Break Out- Identifying Candidate DHS Security Controls

The sub-team started with the following example to see what requirement drafting might entail (*E.g.*2.8.7)

1. The RE shall insure that all BES Cyber System component are within an Electronic Security Perimeter.
2. The RE shall manage the ESP gozintas and gozoutas (insert table to define "manage" at the different impact levels/environments).

E.g.

Ports /services enumation	H	M X	L X	CC/Gen/Tran
Strong Auth. For Remote Interactive Access	H	M X	L	

- Boundary protection 2.8.7
- 2 requirements. make sure everything in boundary and manage that boundary.
- What does "manage" mean at that level? Take sub Rs in 005 and put down left side of table.

Member Comments

- PH Defined ESP around crucial cyber assets- in CIP 002- boundary access control into and out of the cyber system.
- Why define a boundary? Need to know what is coming in going out.
- **2.8.7** talks about identifying a boundary.

- **I**s there a need of providing a glossary of new terms we should use as we write these requirements?
- If concepts roughly the same, use the "term"- Re-define to take out the CCA.
- CIP is tied around CCAs? Do CCAs have to be inside it? Boundary at DHS is generic. It isn't tied to asset, category or definition.
- If not ESP, (or use electronic security boundary) looking at this as more of a concept.
- Boundary "protection" is a function- critical cyber assets and a boundary around them, or perimeter.
- CIP tied to assets vs. federal concept of compliance. Problem with "electronic boundary" is that it constrains compliance.
- Think of "network boundaries"
- There is no standard in industry as to what an ESP is. Industry grappled with this one.

b. 2nd Break Out- Identifying Controls and Drafting Requirements

- The Sub-team met with the Access Control and Auditing group to coordinate and clarify which sub-team would deal with the access control issues in security operations.
- R1 and R3. Controls 2.87
- Drafted 5 requirements and added rows to the chart.
- High level –general ideas for requirements.
- Sub-requirements in R1 are definitional matters. Sub-team started a list of definitions, e.g. access points defined.
- #2- needs to scope this one as it represents a whole new concept.
- Sub-team is reworking R1, 4 and 5. They are a mess today. The Sub-team will make more succinct.
- Security systems- access control, monitoring. Some are monitoring more than 1 system.
- Are there auditing issues in R4 and R5?
- Went through R1 and R3 in CIP 005 and came up with five requirements with all components within the ESP and all Access Points are identified
- Need much more definition to Electronic Security Perimeter
- Also Remote Interactive Access
- Systems within the ESP are part of the Cyber System (R1.4 and 1.5)
- Monitor and log all access through an ESP Access Point
- Caution – security monitoring systems may monitor or protect more than one BES cyber system
- 1.4 and 1.5 look like monitoring systems – may need to coordinate with Auditing sub team
- Add summary description to document proposed changes

- May want to build a related glossary – be sure we are using the terms consistently across all the sections

4. Recovery and Response *(Jeri Domingo Brewer, Jason Marshall, Joe Doetzl, Scott Rosenberger)*

a. First Break Out- Identifying Candidate DHS Security Controls

- Validation of CIP and cross-reference and evaluate 706 whether there were paragraphs directed changes to these standards/requirements.
- "Continuity of operations" DHS- much broader.
- CIP- recovery and incidence of response. Overlap with other reliability standards.
- Clarify who and what this applies to
- Training in CIP 004 may take care of this training.
- Incident handling-look to FERC 706 paragraph.
- Looking at requirements next.

b. 2nd Break Out- Identifying Controls and Drafting Requirements

- Continuity of operations – part of critical business function practice –
- CIP 008 and 009 are straightforward
- Incident response: there are some elements regarding training, those pieces may need to remain in personnel training but overlap we need to discuss
- In the physical section there was a section on location of physical assets – does that fit more in your section?
- Much of the requirements are straightforward and will not require significant rewrites
- High impact- to low impact
- Federal government concept of "vital records" relates to continuity of service/operations. Requires more comprehensive planning than CIP.
- Incident response
- Training requirements- regarding recovery and response. Not clear whether these stay in this section vs. group responsible for training
- Physical section addresses choice of physical location of assets.
- Scott Rosenburger will take the lead from here on this section along with Joe Doetzl.

5. Access Control and Auditing *(Sharon Edwards, Phil Huff and Jeff Hoffman)*

a. First Break Out- Identifying Candidate DHS Security Controls

- Assumed the table and decisions apply to high impact only
- "Yes" means we will look at it further, not necessarily adopt in whole
- Account Management- 2.15.3- side-by-side CIP and DHS comparison.
- E.g. deleted #9 DHS side.

- Cross-referenced to existing CIP language.
- This should be incorporated into CIP #7 "specifically authorizing and monitoring the use of guest/anonymous accounts.
- Helpful to see what Jay's team did.
- E.g. periodic review- line items that could be put into a table format.
- Got through 1 out of 15 controls on our plate. Time is needed for this.
- Separation of duties? Cannot be done in some cases
- Looking at separating administrative from security duties
- That is a best practice, and should not be a requirement subject to possible fines
- Original intent was to have two people to verify an action by separating or limiting the scope of respective roles, Turn into a recommended practice, not a requirement
- Need to go back through the items in gray – assumed they were already in the CIP, but need to review them further

b. 2nd Break Out- Identifying Controls and Drafting Requirements

- Sub-Team focused on understanding the process and walked through one in detail – then divided up the rest for further work
- Identified changes to CIP
- Concerned that the current language allows organizational approval rather than specific individual. However, that allows for different organizational structures.
- CIP says "designate" rather than "authorized" – the former is more rigorous
- If CIP is the master language – having trouble putting into a master spreadsheet designed to address DHS requirements
- Need to modify the table to note CIP language not covered by DHS catalogue – add a row to each family
- End of presentation-- governance question.
- Clarify the meaning of "appropriate approvals."
- This is hard issue in terms of DHS and CIP.
- In the Federal context, this is shown by testing. It is built into the system as a performance framework and life cycle maturity.
- CIP- granular language- is this a weak compensation for a more mature control?
- What happens to a documentation step?
- Approval by "Designated personnel"
- Separately requires a list of who are the authorizing individuals.

6. **Change Management System Lifecycle and Information Management.** *(Dave Revill, Keith Stouffer and Bill Winters)*

a. First Break Out- Identifying Candidate DHS Security Controls

- Didn't get to 706 yet. Next task after cracking requirements language.
- Got through 1 family. 3 requirements left in. Removed 2-3 had yes on yesterday but on further review.
- 2.5.1 punted to the governance group.
- Requirement- policy 1.2.5.1, 2.5. 4, Acquisitions (dropped 252 and 253).
- E.g. 2.5.4 The organization develops security functional requirements specifications and documentation requirements for the BES cyber system acquisitions.

b. 2nd Break Out- Identifying Controls and Drafting Requirements

- 5 families (12-15 in each family)
- Sub-team has got through 1st family.
- First 3 controls of 2nd family (maybe an overlap with maintenance)
- When equivalency- the harmonization exercise takes more time.
- Configuration and change management
- System life cycle (not much overlap)
- Information mgt.- tough family regardless-
- 2.5.7 User installed software. Said yes initially. Really turned out more about authorizing to install. Since this is already managed through configuration change management process approval, we changed this to No.
- DHS-less concern about saying things multiple times unlike CIP.
- 2.6.1-policy will be handled by the Governance Sub-Team.
- Baseline configuration. - Mitre report and mapping from DHS catalogue. Suggested including in CIPS. Sub-Team didn't agree with that.
- Control written.

D. Final Reflections on the Sub-Team Output

On Friday morning, following the sub-team reports, the Team offered reflections on the sub-team exercise.

- Where does spreadsheet end up – is it proof we considered or is it just and internal document – may need to be careful in the comments
- Initially this should be just an internal documentation of the Team's discussion and agreements.

- Suggest more is better since we do not know its future – unlikely to be filed with a regulator but not sure how much justification we need in a text formatted future filing – also may be circulated as email to + list which makes it virtually public
- Don't think I need to justify why a DHS does not fit in CIP – "considered" as requested.
- May want a little more detail than just "too cumbersome" for our own use a few months down the road.
- Denote and label this document as a "working draft."

IV. NEXT STEPS

On Friday morning following the Sub-Team reports, the facilitators presented and the Team reviewed and refined the next steps and assignments emerging from the meeting:

A. Next Steps- SDT

1. Revise the Strawman based on Tucker outcomes- Phil and circulate to SDT
2. Get the overall SDT schedule/work plan out ASAP consistent with adopted NERC schedule (Scott Mix and Bob Jones)
3. Members provide comments early next week on draft Webinar materials to Jay/Sharon(by Tuesday/Wed)
4. Members provide questions to Joe B for FERC/NERC consideration at Jan 28 meeting by Jan 26. Joe will send around info on phone link up etc. Members consider participating.
5. Feb 3 Webinar- members encouraged to participate. Jay and Sharon lead.
6. Draft Tucker Summary circulated to SDT by end of Jan.

B. Sub-Team Assignments

1. Sub-teams will request today or ASAP assistance from Howard, Scott or Joe in their meetings and set their meetings and coordinate with Joe
2. Get the sub team master schedule from next week to Austin out ASAP. NERC will help resource these in terms of ready talk. (Joe B coordinates)
3. Recovery and Response- Jeri will send to Scott R. draft and join the first conference call meeting.
4. Prepare progress reports and any key questions for presentation in Austin on Friday morning.

C. CIP 002-4 Review

1. 'Ugly Dump" of raw comments from Industry on February 9th or 10th to be sent to the team (Scott Mix).
2. Informal Industry Comments due by Close of Business Friday February 12, 2010.
3. Meeting in Phoenix. 1 p.m. Tues- Feb 16 (15 is holiday) through noon on Friday February 19.
4. Draft Compilation and organization of comments and to be sent out over weekend. Feb 13 or 14 (John Lim and Scott Mix).
5. Full and small group review of comments and consideration of changes to CIP 002-4.
6. Agreement on CIP 002 as revised for posting for 45 day at conclusion of Austin meeting.

D. Work plan and Schedule Review

Scott Mix presented a revised proposed schedule for CIP 002 and the security controls requirements *(See Appendix #5).* The Team liked the presentation in which the two efforts are put in parallel columns and shows the amount of work ahead.

E. FERC/NERC Workshop Questions
Phil Huff reviewed some questions that the Team discussed for FERC meeting next week including:

1) What expectations are there regarding coordination with the Smart Grid CSCTG (Cyber Security Coordination Task Group) product and how we use NIST SP 800-53/DHS Catalogue?
2) NIST SP 800-53 is an organizational risk management framework, which allows for tailoring and compensating controls. However, FERC Order 706 calls for extensive oversight for any exceptions. What are their thoughts on reconciling these seemingly conflicting objectives?
3) The process to make modifications to the Standards through a FERC Order is very resource intensive. Conversely, changes made prior to industry balloting are relatively cheap. Is it possible to have a process where the team can receive feedback from FERC prior to ballot?
4) To what degree can we remove or lessen prescriptive elements in the current CIP Standard where the risk reduction does not justify the consumption of industry resources?
5) Have we captured all of the directives from order 706 in the filing from December?

He noted this was a working list which will be circulated for members to suggest additions to in advance of the January 28 FERC/NERC workshop.

F. Sub-Team Organization and Next Steps
Joe Bucciero will be soliciting from each Sub-Team their meeting schedules to produce a master Sub-Team schedule from this meeting to Austin. He noted that Ready talk will be made available to the Sub-Teams so they can review and share documents.

The facilitators noted that each Sub-Team should plan on preparing and presenting short progress reports and key questions for presentation at the Austin meeting which will primarily focus on refining CIP-002-4 in response to industry comments. NERC will try to get Maureen Long to the Austin meeting on Thursday to be available to address the response and refinements of the CIP-002-4. The Team needs to reach agreement on CIP 002 as revised for posting for 45 day period.

Phil Huff on behalf of the SDT thanked Jeri Domingo Brewer for her leadership over the past 16 months. Ms. Brewer acknowledged the opportunity to get to know the SDT members and noted the honor of having worked with them to produce excellent and timely outcomes. She urged the Team to continue to build on the foundation of trust and collegiality to complete the task assigned by December 2010.

Mr. Huff then thanked Dave Revill for hosting the meeting and providing excellent support for this critical meeting.

The SDT adjourned at 12:30 p.m. on January 22, 2010. Several Sub-Teams continued to meet following lunch on Friday afternoon.

Appendix # 1— Meeting Agenda

NOTE:
1. Agenda Times May be Adjusted as Needed during the Meeting
2. Drafting Group Meetings May Not Have Access to Telephones and

Proposed Meeting Objectives/Outcomes

- Review the CSO 706 SDT 2010 Work plan
- Receive update on the CIP 002-4 filing and review process lessons learned
- Receive updates on other related cyber security initiatives
- Receive a NERC update on implementing the CIP Communication Plan
- Review, discuss and test consensus for CIP guiding principles
- Review strawman documents, discuss and test consensus for CIP security controls approach, guidance, scope and applicability.
- Convene CIP Security Controls Drafting Groups
- Review Drafting Group Reports and Provide Feedback
- Agree on next steps and assignments

Draft Agenda

Tuesday **January 19, 2009**

1:00 p.m. Welcome and Opening Remarks- *Jeri Domingo-Brewer & Phil Huff*
Roll Call; NERC Antitrust Compliance Guidelines
Facilitator review and SDT acceptance of December 15-16, 2009 Little Rock SDT meeting summary
1:15 Review of Meeting Objectives, Agenda and Meeting Guidelines- *Bob Jones*
1:20 Review of CSO 706 SDT Work plan- January-June, 2010- *Stu Langton*
1:40 Update on CIP 002 Filing- Process Lessons Learned- *Joe Bucciero*
2:00 Other Updates on other related cyber security initiatives- *NERC Staff and SDT Members*
2:15 NERC Update on Implementing the CIP Communication Plan
2:30 Overview of Security Controls Strawman Documents and Drafting Group Process
3:00 Review, Rating and Consensus Testing of Principles
4:00 Review Strawman Security Controls Categories and Proposed Drafting Sub-Teams
4:30 Review and Consensus Testing of Sources for Controls
5:00 Review of Required Elements for Each Security Control
5:15 Member Drafting Sub-Teams Preference Survey
5:25 Review of Proposal for Wednesday Agenda and Drafting Groups
5:30 *Recess*

Wednesday **January 20, 2010**

8:00 Welcome and Agenda Review- *Jeri Domingo-Brewer & Phil Huff*
8:10 Review of CIP Security Controls Drafting Template- *Scott Mix and Howard Gugel, NERC*
8:45 Review and Agree on Proposal for Drafting Security Controls and Sub Team Members

10:00	Convene Organizational Meetings of SDT Cyber Security Controls Sub Teams
12:45	Reconvene SDT Cyber Security Controls Sub Teams
3:0	Sub Team Organizational Reports, Requests and Needs and Full Team Feedback
4:50	Review Assignments and Thursday Agenda
5:00	*Recess*

Thursday	**January 21, 2010**
8:00	Welcome and Agenda Review- *Jeri Domingo-Brewer & Phil Huff*
8:15	Review any Drafting Group Requests/Needs
8:30	Reconvene SDT Cyber Security Controls Sub Teams
	Reconvene SDT Cyber Security Controls Sub Teams
3:00	Sub Team Reports and Full Team Feedback
4:50	Review Assignments and Friday Agenda
5:00	*Recess*

Friday	**January 22, 2010**
8:00	Welcome and Agenda Review- *Jeri Domingo-Brewer & Phil Huff*
8:15	Review any Drafting Group Requests/Needs
8:30	Reconvene SDT Cyber Security Controls Sub Teams
12:30	Sub Team Reports and Full Team Feedback
2:30	Review and Agree on Next Steps for Developing Security Controls (CIP 003-009) and Work plan for February 2010 Meeting on CIP 002-4 Industry Comments
	Meeting Evaluation
3:00	*Adjourn*

Appendix # 2 Attendees List

Attending in Person — SDT Members and Staff

1. Rob Antonishen	Ontario Power Generation (Thurs)
2. Jeri Domingo-Brewer, Chair	U.S. Bureau of Reclamation
3. Jim Brenton (Wed-Fri.)	ERCOT
4. Jackie Collett	Manitoba Hydro (Wed/Thurs)
5. Jay S. Cribb	Information Security Analyst, Southern Company Services
6. Sharon Edwards	Duke Energy
7. Gerald S. Freese	Director, Enterprise Info. Security America Electric Pwr.
8. Phillip Huff, Vice Chair	Arkansas Electric Coop Corporation
9. Doug Johnson	Exelon Corporation – Commonwealth Edison
10. David S. Revill	Georgia Transmission Corporation
11. Jonathan Stanford	Bonneville Power Administration
12.Keith Stouffer	National Institute of Standards & Technology
13. John D. Varnell	Technology Director, Tenaska Power Services Co. (Wed. Thurs)
Roger Lampilla	NERC
Scott Mix	NERC
Howard Gugel	NERC
Gerry Adamski (Tues)	NERC
Joe Bucciero	NERC/Bucciero Consulting, LLC
Robert Jones	FSU/FCRC Consensus Center
Hal Beardal	FSU/FCRC Consensus Center
Stuart Langton	FSU/FCRC Consensus Center

SDT Members Attending via Ready Talk and Phone

14. Joe Doetzl (Wed)	Manager, Information Security, Kansas City Pwr. & Light Co. (Thurs.)
15. Frank Kim (Thurs)	Ontario Hydro
16. Rich Kinas (Wed/Thurs)	Orlando Utilities Commission (Wed.)
17. David Norton	Entergy (Wed.
18. Scott Rosenberger (Wed)	Luminant Energy
19. Kevin Sherlin (Tues-Fri)	Sacramento Municipal Utility District (Wed. Thurs.)
20. William Winters (Wed-Thurs)	Arizona Public Service, Inc.

SDT Members Unable to Attend

1. John Lim, Chair	CISSP, Department Manager, Consolidated Edison Co. NY

Others Attending in Person

Jeff Hoffman	USBR
John Falsey	EMMT
Jason Marshall	Midwest ISO

David Van Winkle	GTC

Others Attending via WebEx and Phone

Rob Hardiman	Southern Company Transmission
Joseph Baxter	AECI
Justin Kelly	FERC
Justin Kelly	FERC
Michael Toecker	Burns and MacDonald Engineering
Bill Glynn	Westar Energy
Sam Merrell	Cert
Rob Wotherspoon	Orlando Utility Commission
Michael Fischette	LBWL
Laurel Moll	Orlando Utility Commission

Appendix #3

Meeting Evaluation Feedback for Inclusion in Team Meeting Summary

The SDT members used the following 0-to-10 scale in evaluating the meeting: 0 means totally disagree and 10 means totally agree. This reflects 12 member responses.

1. Please assess the overall meeting.

8.00 The agenda packet was very useful.
8.14 The Ready Talk document display and the audio were effective
9.40 The quality of the meeting facility was good.
8.50 The objectives for the meeting were stated at the outset.
8.33 Overall, the objectives of the meeting were fully achieved.

Was each of the following meeting objectives fully achieved?

8.50 Review the CSO 706 SDT 2010 Work plan
7.88 Receive update on the CIP 002-4 filing and review process lessons learned
8.71 Receive updates on other related cyber security initiatives
8.00 Receive a NERC update on implementing the CIP Communication Plan
8.63 Review, discuss and test consensus for CIP drafting principles
8.50 Review straw man documents, discuss and test consensus for CIP security controls approach, including drafting sub-teams, sources for controls and required elements for each security control.
9.50 Convene CIP Security Controls Sub-Teams
9.43 Review Sub-Team Reports and Provide Feedback
8.75 Agree on next steps and assignments

2. Please tell us how well you believe the Team engaged in the meeting.

7.63 The Chair and Vice Chair provided leadership and direction to Team and Facilitators
8.89 The Facilitators made sure the concerns of all members were heard.
8.63 The Facilitators made sure the concerns of all participants were heard.
7.63 The Facilitators helped clarify and summarize issues.
7.25 The Facilitators helped members build consensus.
7.63 The Facilitators helped us arrange our time well.

3. What is your level of satisfaction with what was achieved at the meeting?

7.44 Overall, I am very satisfied with the results of the meeting.
7.80 Overall, the design of the meeting agenda was effective.
8.70 I was very satisfied with the services provided by the Facilitators.
7.90 I am satisfied with the outcome of the meeting.
6.89 I am satisfied with the progress we are making as a Team.
8.80 I know what the next steps following this meeting will be.
8.80 I know who is responsible for the next steps.

4. Other comments (use other side)

What did we achieve?

- We decided not to meet the schedule by not saying we will do other stuff besides fix existing structure.

What are our biggest challenges going forward?

- Timetable.
- Time/resources.

What suggestions do you have for making the Team more productive?

- Get the members to express their concerns in a more productive manner.
- Read out loud FERC ORDER 706!

Appendix # 4 — NERC Antitrust Compliance Guidelines

I. General

It is NERC's policy and practice to obey the antitrust laws and to avoid all conduct that unreasonably restrains competition. This policy requires the avoidance of any conduct that violates, or that might appear to violate, the antitrust laws. Among other things, the antitrust laws forbid any agreement between or among competitors regarding prices, availability of service, product design, terms of sale, division of markets, allocation of customers or any other activity that unreasonably restrains competition.

It is the responsibility of every NERC participant and employee who may in any way affect NERC's compliance with the antitrust laws to carry out this commitment.

Antitrust laws are complex and subject to court interpretation that can vary over time and from one court to another. The purpose of these guidelines is to alert NERC participants and employees to potential antitrust problems and to set forth policies to be followed with respect to activities that may involve antitrust considerations. In some instances, the NERC policy contained in these guidelines is stricter than the applicable antitrust laws. Any NERC participant or employee who is uncertain about the legal ramifications of a particular course of conduct or who has doubts or concerns about whether NERC's antitrust compliance policy is implicated in any situation should consult NERC's General Counsel immediately.

II. Prohibited Activities

Participants in NERC activities (including those of its committees and Subgroups) should refrain from the following when acting in their capacity as participants in NERC activities (e.g., at NERC meetings, conference calls and in informal discussions):

- Discussions involving pricing information, especially margin (profit) and internal cost
- information and participants' expectations as to their future prices or internal costs.
- Discussions of a participant's marketing strategies.
- Discussions regarding how customers and geographical areas are to be divided among competitors.
- Discussions concerning the exclusion of competitors from markets.
- Discussions concerning boycotting or group refusals to deal with competitors, vendors or suppliers.

III. Activities That Are Permitted

From time to time decisions or actions of NERC (including those of its committees and Subgroups) may have a negative impact on particular entities and thus in that sense adversely impact competition. Decisions and actions by NERC (including its committees and Subgroups) should only be undertaken for the purpose of promoting and maintaining the reliability and adequacy of the bulk power system. If you do not have a legitimate purpose consistent with this objective for discussing a matter, please refrain from discussing the matter during NERC meetings and in other NERC-related communications.

You should also ensure that NERC procedures, including those set forth in NERC's Certificate of Incorporation and Bylaws are followed in conducting NERC business. Other NERC procedures that may be applicable to a particular NERC activity include the following:

- Reliability Standards Process Manual
- Organization and Procedures Manual for the NERC Standing Committees
- System Operator Certification Program

In addition, all discussions in NERC meetings and other NERC-related communications should be within the scope of the mandate for or assignment to the particular NERC committee or Subgroup, as well as within the scope of the published agenda for the meeting.

No decisions should be made nor any actions taken in NERC activities for the purpose of giving an industry participant or group of participants a competitive advantage over other participants. In particular, decisions with respect to setting, revising, or assessing compliance with NERC reliability standards should not be influenced by anti-competitive motivations.

Subject to the foregoing restrictions, participants in NERC activities may discuss:

- Reliability matters relating to the bulk power system, including operation and planning matters such as establishing or revising reliability standards, special operating procedures, operating transfer capabilities, and plans for new facilities.
- Matters relating to the impact of reliability standards for the bulk power system on
- electricity markets, and the impact of electricity market operations on the reliability of the bulk power system.
- Proposed filings or other communications with state or federal regulatory authorities or other governmental entities.
- Matters relating to the internal governance, management and operation of NERC, such as nominations for vacant committee positions, budgeting and assessments, and
- employment matters; and procedural matters such as planning and scheduling meetings.

Any other matters that do not clearly fall within these guidelines should be reviewed with NERC's General Counsel before being discussed.

APPENDIX # 5
MEETING SCHEDULE
JANUARY –DECEMBER 2010

Preliminary, Draft, Unofficial Schedule for CIP-002-4

CIP-002 Task	CIP 2 Milestone Date	Week-of	Date	CIP-003 -- CIP-009 Task
		1/18/10		SDT Meeting - Work on requirement language
		1/25/10		sub-team meetings
		2/1/10		sub-team meetings
Informal Comment Period closes	2/12/10	2/8/10		sub-team meetings
SDT Meeting - React to comments		2/15/10		
Post for 45-day formal comment; form ballot pool	2/25/10	2/22/10		sub-team meetings
		3/1/10		sub-team meetings
		3/8/10		SDT Meeting - Work on requirements
		3/15/10		post initial unofficial draft (aid in CIP-002 ballot process)
		3/22/10		sub-team meetings
Initial Ballot start	4/2/10	3/29/10		sub-team meetings
		4/5/10		sub-team meetings
Initial ballot close; SDT Meeting - respond to comments	4/12/10	4/12/10		
		4/19/10		sub-team meetings
Recirc Ballot start	4/30/10	4/26/10		sub-team meetings
		5/3/10		sub-team meetings
Recirc ballot close; SDT meeting - respond to comments	5/10/10	5/10/10		
Re-recirc ballot start	5/16/10	5/17/10		sub-team meetings
Re-recirc ballot close; BoT Approval	5/25/10	5/24/10		sub-team meetings
File with Regulators	5/31/10	5/31/10		sub-team meetings
		6/7/10		SDT Meeting - Work on requirements
		6/14/10		
		6/21/10		
		6/28/10		
		7/5/10		
		7/12/10		SDT Meeting
		7/19/10		
		7/26/10		
		8/2/10		

OCTOBER 2008–JULY 2009

1. October 6–7, 2008 — Gaithersburg, MD Reviewed CIP-002-CIP-009, Agreed on Version 2 approach.

2. October 20–21 —Sacramento, CA CIP-002-CIP-009 Version 2 development

3. November 12–14, 2008 — Little Rock, AR CIP-002-CIP-009 Version 2 adoption for comment and balloting; CIP-002-CIP-009 New Version process reviewed.

4. December 4–5, 2008 — Washington D.C. CIP-002-CIP-009 Version 3 reviewed and debated, SDT member white "working" papers assigned, Technical Feasibility Exceptions white paper reviewed and refined.

5. January 7–9 — Phoenix, AZ, Reviewed Technical Feasibility Exceptions white paper**,** reviewed industry comments on CIP-002-CIP-009 Version 2 products — established small groups to draft responses, reviewed New Version white "working" papers.

- January 15 — WebEx meeting(s) Small group drafted responses to industry Version 2 comments.
- January 21 — WebEx meeting(s) Small group drafted responses to industry Version 2 comments.

6. February 2–4, 2009 — Phoenix, AZ Update on NERC Technical Feasibility Exceptions process**,** VSL process and SDT role**,** review of Version 3 White papers, strawman and principles**,** reviewed and adopted SDT responses to industry comments on Version 2 and Version 2 Product Revisions.

7. February 18–19, 2009 — Fairfax, VA Update on Version 2 process**,** NERC TFE process and VSL Team process; reviewed, discussed and refined Version 3 CIP-002 White papers, strawman, and principles.

8. March 10–11, 2009 — Orlando, FL Update on NERC TFE and VSL and VRF Team process and review and refine Version 3 CIP-002 Strawman Proposals

March 2–April 1, 2009 — 30-day Pre Ballot

Mid-March — NERC posts TFE draft Rules of Procedure for industry comment

March 30, 2009 — WebEx meeting(s) White Paper Drafting Team

April 1–10 — NERC Balloting on Version 2 Products

April 6, 2009 — WebEx meeting — White Paper Drafting Team

April 8, 2009 — WebEx meeting(s) — White Paper Preview- Full SDT Conference Call

April 11, 2009 — Version 2 Ballot Results (Quorum: 91.90% Approval: 84.06%) and Industry Comments

9. April 14–16, 2009 — Charlotte NC Update on NERC TFE process, VSL Team process and NERC Critical Assets Survey; agreed and adopted responses for Version 2 industry comments for recirculation ballot; reviewed and refined Version 3 whitepaper and consensus points and progress report to NERC Member Representative Committee (MRC) May meeting.

April 28 and May 6, 2009 — White Paper Drafting Team Meetings and WebEx

April 17–27, 2009 — Recirculation Results: Quorum: 94.37% Approval: 88.32%

May 5, 2009 — NERC MRC Meeting, Arlington, VA- SDT progress report.

10. May 13–14, 2009 — Boulder City NV Reviewed MRC presentation and further SDT refinement and discussion of the Version 3 White Paper.

June 8 and June 15, 2009 — Working Paper Drafting Team Meetings and WebEx

11. June 17–18, 2009 — Portland OR Further SDT refinement of the draft CIP Version 3 Working Paper(s), reviewed SDT development process for June-December 2009; discussed potential SDT subcommittee structure and deliverables.

- *June — WebEx meeting(s)*
- *Working Paper drafting group sessions including inputs from selected industry personnel to help establish BES categorization criteria*

CIP-002 DEVELOPMENT OF REQUIREMENTS, MEASURES, ETC. JULY-DECEMBER 2009

12. July 13–14, 2009 in Vancouver, B.C., Canada
SDT reviewed, refined, and adopted SDT Working Paper. SDT adopted its response to NERC for Interpretation of CIP-006-1. SDT reviewed and adopted a proposal for CIP-002 Subgroups and Deliverables and convened subgroup organizational meetings to develop work plans. SDT adopted 2010 Meeting Schedule.

- *July–August Interim Conference call meeting(s)*
- *CIP-002 Subgroup meetings*
- *CIP-002 Coordination Team meeting*
- *August 3–5, 2009 in Winnipeg, Manitoba **NERC Member Representative Committee**. Progress Report and presentation on new CIP Version 3 Working Paper-Concept- Reliability Standards on Cyber Security for MRC input.*

13. August 20–21, 2009 in Charlotte, NC. SDT reviewed and responded to MRC input on Working Paper/CIP-002 Concepts and convened SDT Subgroup and plenary meetings to develop CIP-002 requirements and "proof of concept" control (s).

- *July–September — 45-day Industry Comment Period on CIP-002 Concept Working Paper*
- *NERC Webinar- August–September Interim Conference Call meeting(s)*
- *CIP-002 Subgroup meetings (as ne*
- *CIP-002 Coordination Team meeting*

14. September 9–10, 2009 in Folsom, CA. SDT reviewed and considered industry comments on the Working Paper and CIP-002 concepts and their application to the subgroup work and addressed coordinating issues through joint subgroup meetings. SDT agreed on meeting dates and proposed locations for January–December 2010
September–October Interim WebEx meeting(s)

- *FERC Version 3 Urgent Action SDT conference call meetings*
- *CIP-002 Coordination Team meeting*

CIP VERSION 3 RESPONSE TO FERC ORDER, OCTOBER-DECEMBER, 2009

15. October 20–22, 2009 in Kansas City, MI. Reviewed new FERC Order and urgent action CIP Version 3 process; discussed key issues raised by SDT CIP 002 Subgroups, small group meetings and agreement on refinements to the CIP 002-009 schedule and drafting process for CIP 002-4.

- *October–November Drafting Team meeting(s)*
- *CIP-002 Coordination Team meeting*

16. November 16–19, 2009 in Orlando, FL

- SDT review, refine and adopt Version 3 "industry response" document.
- SDT plenary and drafting group session(s) — to draft, review and refine CIP-002-4 standard, requirements, measures and controls and related documents.
- November–December Interim Conference call meeting(s)
- Drafting teams as needed to finalize draft CIP 002-4 documents
- CIP-002 Coordination Team meeting
- *CIP 002-4 Drafting Team produces next draft based on Orlando Meeting input.*
- *December 2 CSO 706 SDT Version 3 Consideration of Comments Draft Conference Call*
- *December X, CSO 706 SDT CIP 002-4 Preview Conference Call*

17. December 15–16, 2009 in Little Rock AK

- SDT scenario "walk through" to test flow of CIP 002-4.
- SDT plenary and drafting group session(s) to review, refine, and agree on and adopt CIP-002-4 standard, requirements, measures and controls and related documents.
- Agree on initial posting of draft CIP-002-4 for industry review and comment.
- Agree on next steps and 2010 Work plan and schedule
- December 28, 2009 SDT Conference Call on CIP 002-4
- December 30, 2009 SDT Leadership Call- Security Controls Survey Draft

Appendix #6
MASTER SDT SURVEY RESPONSES FOR DEVELOPMENT OF CYBER SECURITY CONTROLS
(Updated Jan 12 2010)

16 SDT Member Respondents: **Rob Antonishen, Jim Brenton, Jackie Collett, Jay Cribb, Joe Doetzl, Sharon Edwards, Phil Huff, Doug Johnson, John Lim, Dave Norton, Chris Peters, Dave Revill, Scott Rosenberger, Kevin Sherlin, John Varnell, William Winters**

SDT Members Unable/No Response: Jeri Domingo-Brewer, Gerald Freese, Frank Kim, Rich Kina; Jonathan Stanford, Keith Stouffer
Industry Respondents: Thomas M. Overman, Boeing

NOTES:
1. This survey, developed by the SDT Chair and Vice Chairs over the holidays, is divided into 4 sections: Guiding Principles; Security Control Approaches; Security Control Guidance; and Security Control Scope/Documents and Applicability. It was sent to the Team on Wednesday, December 30 with a deadline of noon, January 5.
2. Within each section the statements/proposals are listed from "most acceptable" to "less acceptable based on an averaging of the member "acceptability ranks for each statement. Member comments and pros/cons are also included.
3. A SDT Sub-Team, made up of interested SDT member volunteers, will take these survey results following the January 6 SDT conference call and create a strawman document for review by the full team in advance of the in advance of the Jan 19-22 SDT meeting in Tucker, Georgia.

Interest in participating in a temporary SDT drafting group and able to commit to drafting documents and participating in up to two conference call meetings between January 6 and January 15 to produce draft strawman proposals for the development of security controls that will be reviewed by the SDT in Tucker?

Yes: **Jim Brenton, Jay Cribb, Joe Doetzl, Sharon Edwards, Phil Huff, Doug Johnson, Kevin Sherlin, John Varnell,**

No: John Lim *(Not available most of January)* Dave Revill, *(I would like to, but I can't make the time commitment necessary during those 2 weeks. I would like to participate as some sort of alternate when time allows if possible.)* Rob Antonishen (*Sorry – just don't have the time…I'm even getting pushback to 4 day meetings…)* Chris Peters, Scott Rosenberger (Team, I am interested but am sorry that I will not be able to dedicate the additional time with the current job requirements. I am working to get the appropriate staff added to lighten this load but that will take some time. Thanks**),** Jackie Collett, Dave Norton, William Winters

Yes- Thomas M. Overman, Boeing

SECTION 1: DRAFT STRAWMAN GUIDING PRINCIPLES FOR THE DEVELOPMENT OF SECURITY CONTROLS

A. **In developing security controls, the SDT will seek to minimize overlap, duplication, and reduce complexity of the requirements and controls.**

Acceptability Ranking Scale	***4** = acceptable, I agree*	***3** = acceptable, I agree with minor reservations*	***2** = not acceptable unless major reservations addressed*	***1** = not acceptable*	***Average Rank***
	12	**3**	**0**	**0**	**3.8**

Comments:

- Common sense.
- **It may be necessary to duplicate some items/sections to provide simplicity.**
- Who can argue against that? It's a source of much confusion in the current set of standards where all sorts of related things are split across standards and have different implementation plans and timeframes. We've got to stay away from that.

B. **In developing security controls, the SDT will document the security objective to be achieved for each security control to aid in future interpretations.**

Acceptability Ranking Scale	***4** = acceptable, I agree*	***3** = acceptable, I agree with minor reservations*	***2** = not acceptable unless major reservations addressed*	***1** = not acceptable*	***Average Rank***
	10	**6**	**0**	**0**	**3.6**

Comments:

- The emphasis should be on documenting the appropriate controls. If the SDT is diverting into documenting all of these items, it may take time away from the primary objective of documenting the controls. Some of these, i.e., reduction of risk to the BES functions, if done, may be follow-up items. Care should be taken to ensure that identifying and documenting appropriate controls is the priority.
- I don't disagree with this. However, I believe that if the security objective isn't already clear from the language in the requirement, then perhaps we didn't do a very good job writing the requirement.
- *THIS WILL ALSO HELP THE TEAM TO MEASURE THE VALIDITY OF THE OBJECTIVE AND WHETHER OR NOT THE SECURITY CONTROL ACHIEVES IT.*
- *This would be very nice to have though not essential. We should use a standardized framework if pursued to aid in standardized objectives (such as ISO,NIST)*
- If we are too narrow in defining our security objectives, we may not be able to provide enough flexibility for the future security landscape.
- This seems mandatory – isn't this what a requirement is all about? If we are doing 'what' and now 'how' standards then this is basic. It seems that ALL we would state is the security objective to be achieved and going beyond that means we have dropped into 'how' standards.

C. **In developing security controls, the SDT will document how each security control (and enhancement) reduces the risk to the BES functions appropriate to the impact categorization.**

Acceptability Ranking Scale	***4** = acceptable, I agree*	***3** = acceptable, I agree with minor reservations*	***2** = not acceptable unless major reservations addressed*	***1** = not acceptable*	***Average Rank***
	9	**5**	**1**	**0**	**3.5**

Comments:

- The emphasis should be on documenting the appropriate controls. If the SDT is diverting into documenting all of these items, it may take time away from the primary objective of documenting the controls. Some of these, i.e., reduction of risk to the BES functions, if done, may be follow-up items. Care should be taken to ensure that identifying and documenting appropriate controls is the priority.
- I am not sure how this will benefit us in the long run. I think our time would be better spent writing guidance for controls.
- Again, I have the same reservations as for question A. Any such documentation will have to exist outside the standard as (it is my understanding) that standards should not provide the rationalization, only the requirements and measures.
- *THIS MAY BE DIFFICULT TO DOCUMENT, BUT WE SHOULD AT LEAST AVOID INCORPORATING CONTROLS SIMPLY BECAUSE THEY ARE LISTED SOMEWHERE ELSE.*
- *Another nice to have and should be tied to standardized objectives*
- Not sure how we will do this and what value it will provide, while not releasing potential sensitive information.
- I think this goes to Gerry Cauley's remarks that he's made several times recently – how every requirement ought to be tied back to how it improves or preserves BES reliability. If we can't do this, then we have no business making it a requirement in a mandatory BES Reliability standard. If we can't do this, then we are doing security for security's sake and we've taken our eyes off the goal.

D. **In developing security controls, the SDT will consider how compliance can be demonstrated.**

Acceptability Ranking Scale	***4** = acceptable, I agree*	***3** = acceptable, I agree with minor reservations*	***2** = not acceptable unless major reservations addressed*	***1** = not acceptable*	***Average Rank***
	11	**2**	**3**	**0**	**3.5**

Comments:

- I agree that we should "consider" how compliance can be demonstrated, but that is not our primary goal. This is only acceptable if time allows. We may not have time to document compliance measurement. Some other items such as ensuring that appropriate controls are identified are more important as a responsibility of the drafting team.
- The purpose of the standard is to provide better reliability through proper cyber security posture. I am strongly opposed with any type of standard/controls that will eventually lead to a "checkbox" audit mentality. A proper understanding of the intent of the controls should lead to an adequate understanding on how to achieve compliance, while still providing the flexibility necessary in the IT security field to keep the standard in line with current technologies and practices.
- *I AGREE COMPLIANCE SHOULD BE CONSIDERED, BUT A FRAMEWORK THAT ALLOWS COST-EFFECTIVE RISK-REDUCTION IS MORE IMPORTANT THAN ONE THAT EASILY DEMONSTRATES COMPLIANCE.*
- *How will this be addressed in light of reports of auditors not using the measures section of the standard?*
- Since these are mandatory and enforceable standards, this is mandatory for us. We MUST have it clear in the standard with bright lines how an entity knows they are compliant with the requirement and how they will be measured. Anything less is unacceptable in this environment. These are not 'suggestions' or 'good ideas', these are mandatory, auditable, and enforceable. They must have clarity in this area.

E. **In developing security controls, the SDT will set forth and document clear rationales for changes made to the current Version 3 CIP 003-009 and how it protects current investments in security.**

Acceptability Ranking Scale	***4** = acceptable, I agree*	***3** = acceptable, I agree with minor reservations*	***2** = not acceptable unless major reservations addressed*	***1** = not acceptable*	***Average Rank***
	7	**8**	**1**	**0**	**3.4**

Comments:

- The emphasis should be on documenting the appropriate controls. If the SDT is diverting into documenting all of these items, it may take time away from the primary objective of documenting the controls. Some of these, i.e., reduction of risk to the BES functions, if done, may be follow-up items. Care should be taken to ensure that identifying and documenting appropriate controls is the priority.
- I don't disagree with doing this. However, I believe that it is not our burden to provide rationalization for every change that is made to the standards. I believe that it is already well documented that changes are necessary
- Pertaining to the development of security controls any revised CIP 003-009 will, in my opinion, be a significant rewrite of the current (version 3) standard. I am concerned about the effort that will be incurred by any direction that requires either rationalization or justification of any changes or deviations from the current standard.
- *We will have to address the requirements of order 706 as well and should seek to clarify when a change is driven from this order vs. our attempt to make things better*
- While I agree that the industry needs to understand how their previous efforts are not wasted, this effort should not significantly consume our time and effort to get the standards finished.
- If timeframe is such a crucial issue, we may not have time for this. I expect that the changes to current requirements would either provide needed flexibility based on environment (field vs. data center, etc) or go beyond a current weak requirement – neither of which would need a lot of documentation of how it protects current investments in security. I don't see us doing anything that tears down the 'Security 101' that has been built with the current CIP standards.

SDT MEMBER COMMENTS

- I agree with many of the items above, but I'm not sure we should really focus on those as being our *principles*. Several of them seem to be more task-oriented than truly fundamental principles that we should fall back on in the drafting of our security controls.
- *Fundamentally I believe these principles should be in place for the development of CIP3-CIP9V4+, though I am not sure there is time to include all this in the draft strawman if the time target is for the Jan meeting,*

OTHER SUGGESTED DRAFT GUIDING PRINCIPLES

- In developing security controls, the SDT will seek to eliminate the necessity for Technical Feasibility Exceptions (TFE's) though proper development of controls and defining appropriate applicability of those controls.
- In developing security controls, the SDT will seek to eliminate or at least GREATLY reduce the need for a TFE process.

  Comments: We should never write a technically infeasible requirement. That is an oxymoron. They should all be scoped to feasible situations only.
- In developing security controls, the SDT will seek to reduce the compliance documentation and audit burden on the lower impact systems.

  Comments: If the industry has to focus much if not most of its resources on tracking and documenting compliance on the vastly higher quantity lower impact assets, we will have harmed security and BES reliability. The entire point of CIP-002 and classifying impact is so that we can FOCUS on the higher impact systems.

OTHER COMMENTS

Thomas M. Overman, Boeing

First make a distinction between Requirements and Controls. Some overlapping controls are OK (even good), but conflicting requirements are not good. The CIP is likely to remain the only Cyber Security Standard with regulatory authority. Therefore it may be necessary for the CIP to take a lead, or possibly to have requirements contrary to Cyber Security documents which do not have the same regulatory authority. The CIP must address known conflicts if any must remain.

Additional Principles

- In developing security controls, the SDT must draft threat vectors against which certification and accreditation must be judged.
- The SDT seek to minimize overlap, duplication, and reduce complexity of the requirements and controls.
- There may have to be a classified annex to address threat scenarios from a national perspective.

SECTION 2: DRAFT STRAWMAN SECURITY CONTROL APPROACHES

This section lists possible approaches in starting to develop the security controls. This will guide the team's decisions on how to divide into sub-teams and which security control catalogue to begin with.

A. Begin with the current CIP-003 to 009 requirements review and document the applicable Order 706 directives and review any new ways to combine and select those NIST SP 800-53 controls that should be used in a new CIP set of controls.

+++++ Pros- Strengths +++++	------- Cons- Weaknesses --------
• Industry is familiar with current organization	• Requirements may require significant overhaul.
• Preserves investment in compliance management frameworks (significant)	• We may end up with a product similar to past CIP.
• Preserves investment in investments in current controls	• 800-53 not measurable for penalties
• Utilizes industry effort to date.	• Highly defined controls give a black hat a list of things not to do.
• Leverages existing approved standards	• Very time consuming with little value
• Meet objectives of FERC Order 706	• Possibility of missing areas that are currently not addressed.
• Finite target	• **Personally, I'd like to see 006 be removed from the "cyber" set and migrated to a new (CIP-010?) standard that would address requirements for ALL BES assets, regardless of their cyber nature. This is not**
• Addresses the Order 706 in a concrete, easy to demonstrate method.	
• Maintaining the current structure provides a clear path for	

utilities to migrate to a new standard. • Potentially allows for maximum reuse of efforts by the industry • Will be seen as evolutionary rather than revolutionary. • Aligns with 706 intent • Simplifies CIP document structure • Organized CIP Standards into Control families • *Preserves current investment possibly* • *Identified changes as required by FERC* • Starts with something the entire team is familiar with (CIP Standards). • Order 706 directives apply directly to CIPs • Meets overall principle of preserving CIP V1-3 investment • Industry familiarity • Provides a roadmap for the industry from the current controls to the new controls • Provides a cross reference to Order 706 to ensure everything is addressed • Builds on previous work • Helps focus on Order 706	**inconsistent as the current CIP-001 in Sabotage Reporting is not cyber in nature.** • Significant time and resource commitments • *May not provide a holistic and new approach* • *Easier for industry to understand* • Many current requirements need major overhaul. • May be limited by NIST 800-53 • May be seen as more of the same

Acceptability Ranking Scale	***4** = acceptable, I agree*	***3** = acceptable, I agree with minor reservations*	***2** = not acceptable unless major reservations addressed*	***1** = not acceptable*
	7	**7**	**2**	**0**

Avg. =3.3

Other Comments- Thomas M. Overman, Boeing

- Pros- Strengths= Good starting approach to phase into the more rigorous controls. Allows evolving and refining requirements rather than taking an entirely new approach (which would cause unnecessary industry churn.
  Cons- Weaknesses=CIP should also reference and synchronize with NIST 800-82 (Industrial Control System Security)
  In general, NERC CIP should address not only security processes/procedures, but also high-level technical requirements (without dictating technical solutions).

B. Begin with the current CIP-003 to 009 requirements divided into the security functions presented by the NERC Cyber Security Standards Education Team in 2006[1], review and document the applicable Order 706 directives, and review any new ways to combine and select those NIST SP 800-53 controls that should be used in a new CIP set of controls.

+++++ Pros- Strengths +++++	------- Cons- Weaknesses --------
• Used as a training concept. • N/A • This is going to occur somewhat anyway as we compare the current requirements to the NIST control families. • I am familiar with SET functions and support • Grouped into logical security functions similar to NIST 800-53, but in a way that the industry is familiar with. • Easier to incorporate 800-53 controls and prevent cross-references between Standards (or control families) • *I'm sure there are some* • Starts with something the entire team is familiar with (CIP Standards). • Could help eliminate overlap of requirements • Could better group requirements	• Security functions in training has no industry vetting • Not a recognized standard framework • Significant overlap with more recognized standards • I am not specifically familiar with the "security functions presented by the NERC CS Education Team in 2006…" • Would take some education for the team to understand exactly what rely on this NERC material means. • 800-53 not measurable for penalties • Highly defined controls give a black hat a list of things not to do • Time? • Can not comment as I am not familiar with this material • Don't understand the difference between A and B • *More difficult for the industry to understand*

[1] 2006 Cyber Security Standards Workshop Training Materials (Not Available on the NERC Website)

			• Unable to comment on the security function model – not available • Document not available. Can't rank this one • I do not personally know what the security functions presented were and do not have a copy to work from • Lack of familiarity with referenced work	
Acceptability Ranking Scale	***4** = acceptable, I agree*	***3** = acceptable, I agree with minor reservations*	***2** = not acceptable unless major reservations addressed*	***1** = not acceptable*
	2	**6**	**6**(Education)	**0**

Avg. =2.7

C. Begin with the current NIST 800-53 publication, incorporate the current CIP-003 to 009 Standard, and review and document the applicable Order 706 directives.

+++++ Pros- Strengths +++++	------- Cons- Weaknesses --------
• Comprehensive (though not entirely applicable) • Familiar to Federal agencies • Satisfies congressional agenda to utilize NIST approach • Best solution to meet FERC Order 706 • Current NIST 800-53 would provide a solid template to develop the standard from. • Will provide a mature model that should ensure covering all required areas • *Standards based* • Existing set of security controls • NIST controls written at what seems an appropriate level for broad applicability • Politically correct answer (Congress, etc) • Based on a known (800-53) body of work	• A large number of non-applicable requirements • Too general for application to Control Systems • Not enforceable in the current compliance model • This implies that everything in NIST 800-53 will become part of future NERC Cyber Security standards. I did not think the team had agreed to this concept. • 800-53 not measurable for penalties • Highly defined controls give a black hat a list of things not to do • May end up requiring the most amount of modifications to entities existing CIP programs • Deviating from the current structure of the CIP standards will make it difficult, timely and costly for utilities to migrate to a new standard. • May be seen as "throwing out the baby with the bath water" by the Industry, • While this effort would demonstrate adherence to the 706 Order, a significant restructure will undoubtedly introduce NEW areas that FERC will have issue with, and may result in a new Order as significant as the current 706 Order. • The NIST standard is not designed as an audit/enforcement standard, and as such may not be the best style to use for a reliability standard • This is a massive undertaking that the SDT is not organized to achieve. • Several controls assume an enterprise security architecture which would be difficult to demonstrate in the NERC compliance program. • *Does not preserve current investment* • Not all team members are familiar with 800-53 (learning curve) • Industry unfamiliar with 800-53 • Would make it more complicated for the industry to follow the changes • Might not be as clear how we could leverage existing security implementations

			• Applicability to industrial control systems	
Acceptability Ranking Scale	***4** = acceptable, I agree*	***3** = acceptable, I agree with minor reservations*	***2** = not acceptable unless major reservations addressed*	***1** = not acceptable*
	4	**3**	**6**	**2**

Avg. =2.6

Other

- As the Lead for the "Controls" sub group and a person familiar with NIST, does Keith have a recommended approach?
- The controls like in 800-53 should be a guideline not in the stander. This will make it where the auditors will allow new technology. NIST 800-53 ties us to today's technology only.
- *I find any of these approaches acceptable. I can't identify any pros/cons that have not already been submitted. I believe that A and B should be done in combination ensure that in the development of controls we have taken in to account what the ramifications are with respect to what the industry has already been taught and developed and ensure the documented 706 issues are all addressed.*
- *As we extend beyond the initial strawman, in addition to 800-53, I believe we should use the controls based standards referenced in section 3 as additional reference material since these may provide better verbiage and/or insight in the development of CIP Controls which need to be crafted as measurable standards.*

Other Approaches- Thomas M. Overman, Boeing

A. Defense Information Assurance Certification and Accreditation Process (DIACAP) provides a robust C&A guideline. As the Grid is a national asset, subject to attack by sophisticated state-sponsored adversaries, grid security should reference guidelines designed for such an environment. DIACAP is one such example.

B. Assess the risks (insiders, and external attackers, script kiddies to terrorists to organized crime to state-sponsored intelligence services). Two phases: Near term risk mitigation (procedural, some technical) vs. long term architectural and systemic approach.

SECTION 3: DRAFT STRAWMAN SECURITY CONTROL GUIDANCE

This section lists documents for the team to consider when drafting security controls (in addition to previous versions of CIP, FERC Order 706 and NIST 800-53). Although individuals or sub-teams may consider any guidance when drafting controls, the proposal would be to use these documents as a major influence and reference them in communication from the team.

A. Consider the DHS Catalog of Control Systems Security Recommendations for Standards Developers[2] in the development of security controls.

+++++ Pros- Strengths +++++	------- Cons- Weaknesses --------
• Control system centric • Is a good source for testing of completeness • Considering all of these documents may lead to a broad approach that considers different perspectives. • We should consider all guidance available • Comprehensive set of requirements • Supplemental Guidance wording provides useful wordage that would be used in explaining/justifying controls…but • This is being used to develop the Smart Grid Cyber Security Standards. We will immediately be compared with this effort anyway.	• Not meant for compliance monitoring • Time consuming – Do we have time and resources to research all of these documents • Too specific and will give a black hat a road map. • Too comprehensive – goes well beyond the existing CIP standard, in areas such as environmental control, supply chain requirements and strategic planning. • Supplemental guidance wording is necessary for understanding, but does not fit with the current NERC standard framework. • *Not as familiar*

[2] http://www.us-cert.gov/control_systems/pdf/Catalog_of_Control_Systems_Security_Recommendations.pdf

• Control System specific • Focused on control systems • Very detailed			• Many controls are more appropriately directed at control system vendors, not end users of purchased turnkey systems. • Has a lot of good ideas, but things that should not be mandatory requirements (honey pots, etc)	
Acceptability Ranking Scale	***4** = acceptable, I agree*	***3** = acceptable, I agree with minor reservations*	***2** = not acceptable unless major reservations addressed*	***1** = not acceptable*
	5	**6**	**4**	**0**

Avg. =3.1

B. Consider the SANS 20 Critical Security Controls[3] in the development of security controls.

+++++ Pros- Strengths +++++			------- Cons- Weaknesses --------	
• Well known in cyber security circles • Considering all of these documents may lead to a broad approach that considers different perspectives. • We should consider all guidance available • Common sense and needed • As reasonable list as any (based on a cursory review) • Technical focused • Offensive in nature • This is aimed directly at addressing system security. It provides a starting point to prioritizing controls on the basis of risk. • A review wouldn't hurt to make sure we have them covered at the end. • Good starting point			• Too general • Not control system specific • Not intended for compliance • Time consuming – Do we have time and resources to research all of these documents? • Not specific enough to control systems • Somewhat motherhood (based on a cursory review) • New Standard that some may not have had experience implementing • *Not as familiar* • Not control system specific, general IT specific • No surprises in a 'Top 20' – covers the basics. • Should already be included in other larger control frameworks. • High level document • Not focused on industrial control systems	
Acceptability Ranking Scale	***4** = acceptable, I agree*	***3** = acceptable, I agree with minor reservations*	***2** = not acceptable unless major reservations addressed*	***1** = not acceptable*
	5	**5**	**4**	

Avg. =3.0

C. Consider the ISO/IEC 27001 & 27002[4] Standards in the development of security controls.

+++++ Pros- Strengths +++++			------- Cons- Weaknesses --------	
• Well known and comprehensive framework and controls • Recognized international standards organization • Internationally accepted • Better suited to be used as a reference for completeness • Considering all of these documents may lead to a broad approach that considers different perspectives. • We should consider all guidance available • Common sense • Mature Standard • Concise • Internationally recognized			• Not specific to control systems • Not structured for compliance monitoring, more structured for certification • Time consuming – Do we have time and resources to research all of these documents • Have not read! • No access, will not comment or rank • Non-open, proprietary, for purchase only standards. • Generic IT security standard, not control system specific • If we are going to base on generic standards, let's just do NIST and be done with it. Our goal is to write BES Reliability focused standards, not reinvent yet another generic IT Security standard.	
Acceptability Ranking Scale	***4** = acceptable, I agree*	***3** = acceptable, I agree with minor reservations*	***2** = not acceptable unless major reservations addressed*	***1** = not acceptable*

[3] http://www.sans.org/critical-security-controls/cag.pdf
[4] http://www.27000.org/ (for purchase)

	4	**5**	**4**	**0**

Avg. =3.0

D. Consider the ISA 99[5] Standard in the development of security controls.

+++++ Pros- Strengths +++++	------- Cons- Weaknesses --------
• Industrial systems centric • ISA well accepted in industrial environments • Considering all of these documents may lead to a broad approach that considers different perspectives. • We should consider all guidance available • Mature Standard • *Matches my corporate program* • *Familiar to many*	• Not well defined • In development • Not structured for enforcement • Time consuming – Do we have time and resources to research all of these documents • Too specific and will give a black hat a road map. • No access, will not comment or rank • Could be too technical • Non-open, proprietary, for purchase only standards

Acceptability Ranking Scale	***4** = acceptable, I agree*	***3** = acceptable, I agree with minor reservations*	***2** = not acceptable unless major reservations addressed*	***1** = not acceptable*
	2	**8**	**3**	**0**

Avg. =2.9

GUIDANCE DOCUMENTS COMMENTS

- In order to develop a complete set of controls, all of the aforementioned Standards should be considered with the caveat that NERC CIP/NIST 800-53 serve as the baseline and SANS, ISO, DHS, and ISA-99 provide supplemental or amplifying guidance.
- Does the team have enough time to consider many other security controls guidance?

SECTION 4: DRAFT STRAWMAN SECURITY CONTROL SCOPE AND APPLICABILITY

This section lists several methods for applying reasonable and appropriate security controls.

A. Consider applicability of requirements for differing environments for Generation, Transmission and Control Centers.

+++++ Pros- Strengths +++++	------- Cons- Weaknesses --------
• Significant increase in clarity of application and relevance of requirement • Support from stakeholders • Better compliance monitoring • We need targeted controls. • The lack of applicable requirements is one of the industry's major criticisms of existing CIP. • This is crucial to the success of our standards. • Takes into account operational realities • Is the only real justification for writing our own controls versus wholesale adoption of other control frameworks? • We need separate controls of each of the three environment • Might be simple for participants. • Value in a separation for "Control Centers" for entities that don't actually control any "big iron", NOT SCADA master type control centers. • Each environment is distinctly unique • Could reduce ambiguity for industry • *Addresses the differences specifically*	• Increases complexity of the requirement set as a whole • Increases the volume of requirements • Requires specific expertise in targeted environments of generation, transmission and control centers. • Targeting the approach will probably take longer. • It will make the quasi-governmental utilities mad. • Time consuming • This separation is a red herring. Of more value is the nature of the cyber environment and equipment (i.e. embedded single purpose microprocessor based devices vs. PC's versus severs, etc). • Significant level of effort • Requires in depth knowledge of each environment that may not be present on the SDT • Difficult to maintain • Need to examine further to determine if the controls we develop truly apply differently to different operating environments. • *More complex*

[5] http://www.isa.org/MSTemplate.cfm?MicrositeID=988&CommitteeID=6821 (for purchase)

• *Allows greater focus on more critical areas* • Addresses 'one size fits all' flaw • Allows entities to do what makes sense in varying risk environments • Could help provide real examples for the industry	• May need a rename; 'Transmission' is not descriptive of what we're really talking about – we are talking about substation environments, or plant environments, or data center environments.

Acceptability Ranking Scale	***4** = acceptable, I agree*	***3** = acceptable, I agree with minor reservations*	***2** = not acceptable unless major reservations addressed*	***1** = not acceptable*
	6	**5**	**2**	**0**

Avg. =3.2

A1. Establish the applicability of each environment (generation, transmission, and control centers) within each requirement.

+++++ Pros- Strengths +++++	------- Cons- Weaknesses --------
• Single catalog • All in one place • Allows an entity to focus on what is applicable to them. • Only if we use the existing 003 through 009 structure • This may save the SDT some time in writing the requirements. • May ultimately reduce documentation required by the entity. • Easier to maintain • Simplifies the management of the standard. • Easier for entities with more than one type of facility. • Easier to maintain by having a consolidated standard • This would be easier for the industry to read and comprehend. • *Simpler.* • A requirement is stated once in the standard	• Makes requirements complex • Difficult to draft • May require drastically different requirement formatting • May be confusing • Difficult to follow applicability for a specific entity of a certain type • *May not address specific differences* • Could make for huge, confusing requirements with numerous caveats. • All entities will have to search to find what applies to them • Could be out of date very quickly and lack flexibility with the ever changing cyber world • Difficult to follow •

Acceptability Ranking Scale	***4** = acceptable, I agree*	***3** = acceptable, I agree with minor reservations*	***2** = not acceptable unless major reservations addressed*	***1** = not acceptable*
	3	**8**	**3**	**1**

Avg. =3.0

A2. Group all requirements for each environment of generation, transmission, and control centers, separately.

+++++ Pros- Strengths +++++	------- Cons- Weaknesses --------
• Clear set of requirements for each group • Ease of application for functional entities • Each set is simpler (i.e. requirements in each set are simpler) • May provide greater clarity. • Allows one entity to focus on the types of assets they own • Typically, different departments will be handling implementation at substations vs. plants vs. control centers, so this may ultimately improve readability of the requirements. • We need separate controls of each of the three environment • Simpler to follow • Lets entities focus on just what they need to do rather than having their requirements strung out and hard to find over an	• Increases overall volume of the standards • Duplication of requirements in each set • Increase work for responsible entities which are integrated. • Creates redundancy. • May create additional work for SDT. • This should be by functional model and BES function. • Have to make three updates for common items • Redundancy in the standard itself. • In the future, a single change could require multiple edits. • Difficult to maintain • The same requirement could appear in multiple places. • Might cause some redundancy for entities having more than one environment

entire catalog of controls. • Matches most organizational structures so each can be given their piece to implement. • Separated by function	• Would probably cause redundancy in the standards which could confuse the industry and auditors • May miss opportunity for common solutions

Acceptability Ranking Scale	***4** = acceptable**,** I agree*	***3** = acceptable, I agree with minor reservations*	***2** = not acceptable unless major reservations addressed*	***1** = not acceptable*
	4	**8**	**2**	**0**

Avg. =3.1

B. Consider differing vulnerability and threat (risks) in the design of requirements. Use differing levels of application (e.g. basic, enhanced).

+++++ Pros- Strengths +++++	------- Cons- Weaknesses --------
• Reflect practical realities • Great philosophy • Proper risk assessments are the cornerstone of a sound security policy. • *Not sure (no rank)* • I think this is mandatory. A completely standalone non-networked system vs. a networked system should have differing requirements • This could be used to limit controls applied to cyber devices that have no external connectivity •	• Increases complexity • May change over time • Confusing to write. • The approach lacks clarity and may change rapidly. • Cyber vulnerability and threat is not risk to the BES • Not sure we can make this paradigm shift with our current schedule. • FERC may not accept any acceptance of risk, especially given the current national security posture. • If we consider different vulnerabilities and threats as a basis for applicability, then we assume a demonstrable risk management framework. • *Not sure (no rank)* • We have to figure out how to handle inherited security via compensating controls, but this is a must do anyway. • Requires significant detail and is complex

Acceptability Ranking Scale	***4** = acceptable**,** I agree*	***3** = acceptable, I agree with minor reservations*	***2** = not acceptable unless major reservations addressed*	***1** = not acceptable*
	5	**3**	**5**	**0**

Avg. =3.0

C. Consider differing applications of requirements for general purpose software operating environments and proprietary software operating environments.

+++++ Pros- Strengths +++++	------- Cons- Weaknesses --------
• Considers practical applicability • Considers risk/vulnerability • Would be able to isolate cyber security requirements for control systems vs. other systems. • Definitely the way utilities see things. • Would allow for sane application of controls to equipment (not more inane requirements for mal-ware on a network switch!) • Would eliminate the need for TFE's • *Protection based on actual risks* • Yes, requirements MUST take into account the system they are being required on. • Focuses on specific types of software •	• Introduces (necessary?) complexity • May require updates as "proprietary" become general purpose • Definition of proprietary somewhat problematic • I think this will be confusing and complex for the drafting team to figure out. • I feel these two categories are too vague to separate. For instance, many devices run on some type of Linux distro without the end users knowledge. • Ultimately, we must work toward improving the overall security of all applications, whether they are general purpose or custom built • Future changes to environments may require entities to significantly change their security. • May introduce blind spots to security holes. • May trigger equipment changes to avoid implementing requirements (while this may be seen as "gaming", if it does not decrease or possibly improves the security posture, what is wrong with it?) • "General purpose" and "Proprietary" are problematic terms to define. • These apply mainly to technical controls, and I'm not sure there would be any difference in applicability for many of the controls. • *Possibly more complex* • Requires enumeration of these OS'es in the standard • Not clear why this is needed

Acceptability Ranking Scale	***4** = acceptable, I agree*	***3** = acceptable, I agree with minor reservations*	***2** = not acceptable unless major reservations addressed*	***1** = not acceptable*
	4	**3**	**6**	**1**

Avg. =2.8

D. Consider a process for allowing entities to apply compensating security controls on the basis of a risk management program and approval process.

+++++ Pros- Strengths +++++	------- Cons- Weaknesses --------
• Practical and flexible • Details are important • More Flexibility for entities. • We have tried "reasonable business judgment" and TFEs because we acknowledge the need to apply appropriate controls on the basis of risk and the limitation of the SDT to draft perfect controls. In other words, we have to have something, and I don't think TFEs are it. • *Allows security risks to be managed differently* • If scope = all systems, this is essential. Meets the NIST framework, which is something we've been ordered to incorporate • Helps apply reasonability	• Subject to "gaming" • Difficult to monitor and enforce compliance • Has been tried before with adverse public perception • Not sufficiently specific. • Will result in some of the same problems we have today concerning leaving the interpretation up to the individual company. • At face value, this appears difficult to audit consistently. • The age old problem of who can ultimately provide approval. • Sounds suspiciously like TFE's, to me…and I'd rather get rid of them… • Who approves? • Risk management is hard or impossible to assess. • *More complex* • *Approval, by whom?* • A non-bright line, but I think it's necessary. • Danger that 'approval processes could turn into TFE on steroids nightmare.

			• Not sure industry would want to share the required sensitive details with an approving entity • Who would be the approver and what criteria would they use to say what is acceptable • Approval by whom?	
Acceptability Ranking Scale	***4** = acceptable**,** I agree*	***3** = acceptable, I agree with minor reservations*	***2** = not acceptable unless major reservations addressed*	***1** = not acceptable*
	2	**2**	**8**	**0**

Avg. =2.5

OTHER SCOPE AND APPLICABILITY PROPOSALS *(list below)*

SDT Member Comments

- We should refer to requirements (as opposed to controls).
- If I did not answer these questions right (the way you want this to go) will I still be allowed on the straw man team?
- We need to lay out security/reliability goals for each of the environments and then draft requirements/controls that meet those goals. For example, we need to have in mind what level of security needs to be in place at a high impact substation and what needs to be in place at a low impact substation. We need to lay out the nine possibilities (Gen/Trans/Control Center and an L/M/H of each) and determine what we are shooting for in each. Only then, with these agreed upon goals in mind, can we split off into different teams looking at different areas of controls. The old "Begin with the end in mind" thing.

Other Approaches-

Thomas M. Overman, Boeing

The grid will be either integrated or stove-piped. Subjecting Generation, Transmission & Distribution to separate requirements will limit the desired integration of the Smart Grid.

Consider another approach:

- Safety of life (protection of line crews, public{primarily from hydro ops}, mechanics, operators, etc)
- System stability (national, regional, local)
- Equipment protection (Major affecting national capabilities (large generating plant and equipment, NW-SW Intertie, 4C sub, etc), medium affecting regional or large municipal supplies, local affecting city/county)
- Business operations (IT, metering, etc)

Appendix # 7
SECURITY CONTROLS SUB-TEAM MEMBER PREFERENCE FORM
JANUARY 20, 2010

SDT Member Preferences: Rob Antonishen (RA), Jeri Domingo Brewer (JDB)Jim Brenton (JB), Jackie Collett(JC), Jay Cribb (JCr), Joe Doetzl (JD), Sharon Edwards (SE), Jeff Hoffman(JH)
Jerry Freese (JF) Phil Huff(PH) Doug Johnson (DJ) Rich Kinas(RK), David Revill(DR), Kevin Sherlin (KS) Jon Stanford (JS),Keith Stouffer(KSt)) John Varnell (JV) Bill Winters(BW)

Sub-Team	Preference Order #1 through #6	Control Families
A. Security Governance and Assessments Jon Stanford, Rich Kinas, Jerry Freese, *Dave Norton & John LIm*	**JS (1) RK(1) KSt(1) JF(1) PH(1) JDB(2) JH(2)**SE(3)JB(4)JC KS(4)(5) DR (5) JCr(5)RA(5) JV(5)BW(5) DJ(6)	Security Governance *(CIP 003- R1, R2, R3)* Security Assessments *(CIP 005, R4, CIP 007 R 8*
B. Personnel and Physical Security Doug Johnson, Rob Antonishen, Kevin Sherlin	**DR (1) DJ(1)RA(1) KS(1) JF(2)** JS(3) JH(3)JDB(4)JB(5)SE(5) JC (6) JCr(6)JV(6)RK (6)KSt(6) PH(6) BW(6)	Personnel and Training *(CIP 004 R 1, R2, R3)*, (4) Physical Security *(CIP 006 R1-R6)*
C. Operations Security Jay Cribb, Jim Brenton, John Varnell, Jackie Collett	**JC (1) JCr(1) JV(1) JB(1), JDB(1) JH(1) BW(1)KS(2)RK(2)KSt(2)SE(2)RA(2)** DR(3)PH(3)DJ(3)JF(4) JS(5)	Communication Protection *(CIP 005 R1, R3)*, Systems Management *(CIP 007 R2, R3, R4, R6)*
D. Recovery and Response Scott Rosenberger Jeri Brewer, , Joe Doetzl	**JS(2)** JC (3) BW(3) JDB(3)JCr(4) JV(4) DJ(5) KS(5)RK(5)KSt(5)PH(5)JH(5)DR (6) JB(6) JF(6)SE(6)RA(6)	Incident Response (*CIP 008 R1 R2)*, (7) Recovery Plans *(CIP 009, R1-R5)*
E. Access Control and Auditing Sharon Edwards, Phil Huff, Jeff Hoffman	**SE(1)JC (2) JB(2) DJ(2) JCr (2) PH(2) JV(2)**RK(3)DR (4) RA(4) JS(4)KSt(4)JF(5) KS(6) JDB(6)JH 6) BW(4)	Access Control, (*CIP 003, R5, CIP 005 R2, CIP-007 R5, CIP 004 R4* Audit and Accountability *CIP 005 R5, CIP 007 R9)*
F. Change Management, System Lifecycle and Information Management Dave Revill, Keith Stouffer, Bill Winters	**DR (2) BW(2)** KSt(3)JF(3) JB(3)JCr(3)JV(3) KS(3)RA(3)JC(4) DJ (4) RK(4)SE(4)PH(4)JDB(5)JS(6)JH (4)	Configuration Management and System Lifecycle *(CIP 003, R6, CIP 007 R1, R7)* (11) Information Management *(CIP 005 R4, CIP 007 R8)*

Appendix #8 Security Controls Strawman Document

SECURITY CONTROL DRAFTING PRINCIPLES

GUIDANCE IN DRAFTING SECURITY CONTROLS TO ENSURE A CONSISTENT OUTCOME AMONG SUB-TEAMS

Drafting Principles

16. **Applicability [NERC Rules of Procedure[6]] –** Each reliability standard shall clearly identify the functional classes of entities responsible for complying with the reliability standard, with any specific additions or exceptions noted. Such functional classes include: reliability coordinators, balancing authorities, transmission operators, transmission owners, generator operators, generator owners, interchange authorities, transmission service providers, market operators, planning authorities, transmission planners, resource planners, load-serving entities, purchasing-selling entities, and distribution providers. Each reliability standard shall also identify the geographic applicability of the standard, such as the entire North American bulk power system, an interconnection, or within a regional entity area. A standard may also identify any limitations on the applicability of the standard based on electric facility characteristics.
17. **Reliability Objective [NERC Rules of Procedure] –** Each reliability standard shall have a clear statement of purpose that shall describe how the standard contributes to the reliability of the bulk power system. The following general objectives for the bulk power system provide a foundation for determining the specific objective(s) of each reliability standard:
    a. **Security** – Bulk power systems shall be protected from malicious physical or cyber attacks.
18. **Performance Requirement or Outcome [NERC Rules of Procedure]** – Each reliability standard shall state one or more performance requirements, which if achieved by the applicable entities, will provide for a reliable bulk power system, consistent with good utility practices and the public interest. Each requirement is not a "lowest common denominator" compromise, but instead achieves an objective that is the best approach for bulk power system reliability, taking account of the costs and benefits of implementing the proposal
19. **Measurability [NERC Rules of Procedure] –** Each performance requirement shall be stated so as to be objectively measurable by a third party with knowledge or expertise in the area addressed by that requirement. Each performance requirement shall have one or more associated measures used to objectively evaluate compliance with the requirement. If performance can be practically measured quantitatively, metrics shall be provided to determine satisfactory performance.
20. **Technical Basis in Engineering and Operations [NERC Rules of Procedure] –** Each reliability standard shall be based upon sound engineering and operating judgment, analysis, or experience, as determined by expert practitioners in that particular field.
21. **Completeness [NERC Rules of Procedure] –** Reliability standards shall be complete and self-contained. The standards shall not depend on external information to determine the required level of performance.
22. **Consequences for Non-Compliance[NERC Rules of Procedure] –** In combination with guidelines for penalties and sanctions, as well as other ERO and regional entity compliance documents, the consequences of violating a standard are clearly presented to the entities responsible for complying with the standards.
23. **Clear Language [NERC Rules of Procedure] –** Each reliability standard shall be stated using clear and unambiguous language. Responsible entities, using reasonable judgment and in keeping with good utility practices, are able to arrive at a consistent interpretation of the required performance.

[6] *Rules of Procedure of the NERC*, June, 16th, 2009, pp. 6, 7

24. **Practicality [NERC Rules of Procedure] –** Each reliability standard shall establish requirements that can be practically implemented by the assigned responsible entities within the specified effective date and thereafter.
25. **Consistent Terminology [NERC Rules of Procedure] –** To the extent possible, reliability standards shall use a set of standard terms and definitions that are approved through the NERC reliability standards development process.
26. **Reduce Risk** [**3.5 acceptability among survey respondents**] **–** Security controls reduce risk appropriately for applicable BES impact categories
27. **Change Documentation** [**3.3 acceptability among survey respondents**] – Changes from prior versions of CIP Standards have clear rationale. These include the following types of changes:
    a. Above and beyond the current standards
    b. Removal of requirements
    c. Major formatting changes
28. **Reduce Administrative Overhead** [**Suggested principle**] **–** Administrative documentation kept to the minimum that is necessary to verify acceptable risk
29. **Priority [Suggested Principle] –** Implementation and compliance with the Standards are prioritized according to BES risk. The industry should focus on mitigating the greatest risk (i.e. not spend the majority of our resources on the low-impact Cyber Systems).
30. **Minimize TFEs** [**Suggested principle**] **–** Security controls should minimize the need for TFEs

Security Control Groups

Control groups are split initially by the CIP Standards, and additional control groups (8-13) are pulled out to prevent cross-Standard references. Each control group has the relevant CIP and 800-53 families mapped. This approach should reflect the team's consensus to:

> *"Begin with the current CIP-003 to 009 requirements review and document the applicable Order 706 directives and review any new ways to combine and select those NIST SP 800-53 controls that should be used in a new CIP set of controls."*

ID	Control Group	NERC Standard	NIST 800-53 Family
1	Security Governance	CIP-003 – R1, R2, R3;	Planning, Risk Assessment, Program Management
2	Personnel and Training	CIP-004 – R1, R2, R3	Awareness and Training, Personnel Security
3	Communication Protection	CIP-005 R1, R3	System and Communication Protection
4	Physical Security	CIP-006 R1 through R6	Physical and Environmental Protection
5	Systems Management	CIP-007 R2, R3, R4, R6	System and Information Integrity
6	Incident Response	CIP-008 R1 & R2	Incident Response
7	Recovery Plans	CIP-009 R1 through R5	Contingency Planning
8	Access Control (Technical)	CIP-003 R5; CIP-005 R2; CIP-007 R5; CIP 004 R4	Access Control, Identification and Authentication
9	Audit and Accountability	CIP-005 R5, CIP-007 R9	Audit and Accountability
10	Configuration Management and System Lifecycle	CIP-003 R6; CIP-007 R1, R7	Configuration Management, Maintenance, Media Protection, System and Services Acquisition
11	Information Management	CIP-003 R4	Access Control, Media Protection
12	Security Assessments	CIP-005 R4, CIP-007 R8	Security Assessment and Authorization

Drafting Sub-Teams
Additional members may be necessary for teams that have a large number of requirements or FERC directives allocated.

Team	Control Families
Security Governance	(1) Security Governance
Personnel and Physical Security	(2) Personnel and Training, (4) Physical Security
Operations Security	(3) Communication Protection, (5) Systems Management
Recovery and Response	(6) Incident Response, (7) Recovery Plans , (12) Security Assessments
Access Control and Auditing	(8) Access Control, (9) Audit and Accountability
Change Management, System Lifecycle and Information Management	(10) Configuration Management and System Lifecycle, (11) Information Management

Team Assignments

Each team shall assemble the following documentation as part of their drafting assignments. The additional documentation should assist in (1) maintaining consistency across the teams and (2) presenting the purpose and background of the security controls to the industry.

Each team should begin by determining the security controls within their assigned control families necessary to mitigate risk to the BES. Begin by taking the set of applicable Requirements from version 3 CIP Cyber Security Standards and reconcile with applicable NIST 800-53 security controls. Then incorporate additional sources where applicable to mitigate unacceptable risk to the BES functions.

The initial work product should be a set of security controls with applicability to high, medium and low impact Cyber Systems and how specific FERC directives have been addressed (as indicated in Appendix A: FERC Directives from Order 706).

Additionally, for each security control[7]:

7. **Statement of Risk –** State how the security control reduces risk appropriate to the impact categorization [**Drafting principle 11**]
8. **Measures –** State how an objective third party with knowledge or expertise in security can measure the control [**Drafting principle 4**]
9. **Change Documentation –** State the rationale for making changes from previous versions [**Drafting principle 12**]
10. Denote the applicability to (1) Generation Subsystems, (2) Transmission Subsystems, and (3) Control Centers. Provide clarifications or enhancements where necessary to meet the security control objective in that environment [**3.2 acceptability among survey respondents**].
11. Denote the priority for the security control relative to the risk it mitigates (i.e. P1, P2, P3, None). [**SP800-53 introduced this in version 3, and it could help in developing VRFs and implementation plans**]
12. *Team needs to discuss the following scoping exercise to determine how to accomplish these goals of applying appropriate security controls:*
    a. Denote applicability for differing vulnerability and threat profiles. Write controls based on risk profile (as well as impact categorization) [**2.9 acceptability among survey respondents**].
    b. Denote applicability for general purpose vs. proprietary operating systems [**2.8 acceptability among survey respondents**].

Security Controls for Impact Categories

This section provides guidance in the types of controls applicable to High, Medium and Low impact categories. The basic premise is that the cost to implement security controls should reflect the reduction of risk to the BES commensurate with the impact category. The industry as a whole should first focus on mitigating the greatest amount of risk.

Cost to Implement and Maintain / Risk Reduction (Benefit)	Significant	Moderate	Minimal
Signficant	Hi/Med	All	All
Moderate	Hi	Hi/Med	All
Minimal	N/A	Hi	Hi/Med

Figure 1: Applicability to Impact Categories based on Cost vs. Risk Reduction

CIP Security Profiles (Examples For Discussion Only)

Transmission Subsystems (aka substations. Environment = remote, unmanned locations)

[7] This section calls for specific documentation of only a few *Drafting Principles.* Other *Drafting Principles* provide evaluation criteria for security controls.

- **Low** *Primary Concern:* Attackers using it as a launching point to higher impact assets.
  - Controlled access to upstream networks
  - All passwords must be changed from manufacturer defaults on all devices that support a password.
  - No physical security requirements
- **Medium**
  - Same as low for subs??
- **High** *Primary Concern:* The substation is itself a target or a launching point.
  - Physical access control and logging.
  - Electronic access control and logging for all remote access. Strong authentication for remote access.
  - Little to no systems management in substation environment since it consists mostly of dedicated devices (IEDs). Make it mostly about strong access control both electronically and physically with notifications of unauthorized access.

Generation Subsystems (aka plants. Environment = Campus with widely distributed cyber components)

- **Low** *Primary Concern:* Upstream attacks
  - Controlled access to upstream networks (limit use as a launching point for attacks)
  - All passwords must be changed from manufacturer defaults on all devices that support a password.
- **Medium** *Primary Concern:* Attackers gaining control of multiple units within the plant.
  - Good segmentation with access control between individual generating units or groups of smaller units
- **High** *Primary Concern:* Attackers gaining control of multiple units within the plant or across several plants.
  - Strong, highly controlled segmentation between individual generating units.
  - Strong authentication required for all remote electronic access
  - Good systems management, change mgt, vulnerability mgt on control system servers, HMIs.

Control Centers (Environment = centralized data centers)

- **Low** *Primary Concern:* Attacks over their connectivity to higher impact control centers
  - Controlled access to other control networks.
  - Controlled physical access.
  - Vulnerability management on all systems that communicate outside ESP
- **Medium** *Primary Concern*: Same as low (only < 2000 MW centers)
  -
- **High** *Primary Concern:* The ultimate target – gaining control of numerous assets.
  - All the current requirements plus Order 706 changes plus what makes sense out of 800-53.
  - The strongest perimeters (physical and electronic)
  - Stringent systems management, change mgt, vulnerability mgt.
  - Strong personnel controls.

Sources

In order to develop a complete set of controls, all of the aforementioned Standards should be considered with the caveat that NERC CIP/NIST 800-53 serve as the baseline and SANS, ISO, DHS, and ISA-99 provide supplemental or amplifying guidance.

- DHS of Control Systems Security Recommendations for Standards Developers[8]
- Federal Information System Controls Audit Manual (FISCAM) Mapping to CIP Requirements[9]
- ISA 99[10]
- ISO/IEC 27001 & 27002[11]
- SANS 20 Critical Security Controls[12]

Appendix A: FERC Directives from Order 706

Paragraph	Text	Phase[13]	Team
25	we direct NERC to address revisions to the CIP Reliability Standards CIP-002-1 through CIP-009-1 considering applicable features of the NIST framework.	Version 4	ALL
253	While we adopt our CIP NOPR proposal, we recognize that the ERO has already initiated a process to develop such guidance … leave to the ERO's discretion whether to incorporate such guidance into the CIP Reliability Standard, develop it as a separate guidance document, or some combination of the two.	Guideline / Version 4	CIP-002
254	direct the ERO to consider these commenter concerns [how to assess whether a generator or a blackstart unit is "critical" to Bulk-Power System reliability, the proper quantification of risk and frequency, facilities that are relied on to operate or shut down nuclear generating stations, and the consequences of asset failure and asset misuse by an adversary]when developing the guidance.	Guideline / Version 4	CIP-002
257	we direct the ERO to consider this clarification [the meaning of the phrase "used for initial system restoration," in CIP-002-1, Requirement R1.2.4] in its Reliability Standards development process.	Guideline / Version 4	CIP-002
272	the Commission directs the ERO, in developing the guidance discussed above regarding the identification of critical assets, to consider the designation of various types of data as a critical asset or critical cyber asset.	Guideline / Version 4	CIP-002
272	The Commission directs the ERO to develop guidance on the steps that	Guideline /	CIP-002

[8] http://www.us-cert.gov/control_systems/pdf/Catalog_of_Control_Systems_Security_Recommendations.pdf
[9] http://www.gao.gov/new.items/d09232g.pdf (FISCAM document only. CIP mapping available from NERC staff)
[10] http://www.isa.org/MSTemplate.cfm?MicrositeID=988&CommitteeID=6821 (for purchase)
[11] http://www.27000.org (for purchase)
[12] http://www.sans.org/critical-security-controls/cag.pdf
[13] Schedule phases in this column mean one or more of the following:

- "Version 2" – complete in filed version 2
- "Version 4" – planned for next major version (12-18 months plus)
- "Guideline" – stand alone guidance started after corresponding requirement is determined
- "TFE Filing" – 2009 filing on TFE proposal and Appendix 4D to RoP
- "not scheduled" – beyond Version 4
- "CMEP" – part of an existing or ongoing compliance audit, self-report or other process
- "VRF Filing(s)" – one of several already-filed (or very soon to be filed in the case of Version 2) VRF and/or VSL filings

Phase may also be self-explanatory if not one of these entries

Paragraph	Text	Phase[13]	Team
	would be required to apply the CIP Reliability Standards to such data and to consider whether this also covers the computer systems that produce the data.	Version 4	
282	the Commission directs the ERO, through the Reliability Standards development process, to specifically require the consideration of misuse of control centers and control systems in the determination of critical assets	Guideline / Version 4	CIP-002
285	we direct the ERO to consider the comment from ISA99 Team [ISA99 Team objects to the exclusion of communications links from CIP-002-1 and non-routable protocols from critical cyber assets, arguing that both are key elements of associated control systems, essential to proper operation of the critical cyber assets, and have been shown to be vulnerable – by testing and experience].	Version 4	ALL
322	The Commission adopts its CIP NOPR proposal to direct that the ERO develop through its Reliability Standards development process a mechanism for external review and approval of critical asset lists.	Version 4 (Note: proposed version 4 methodology obviates the need for external review0	CIP-002
329	the Commission directs the ERO, using its Reliability Standards development process, to develop a process of external review and approval of critical asset lists based on a regional perspective.	Version 4 (Note: proposed version 4 methodology obviates the need for external review0	CIP-002
376	the Commission adopts its CIP NOPR proposal and directs the ERO to clarify that the exceptions mentioned in Requirements R2.3 and R3 of CIP-003-1 do not except responsible entities from the Requirements of the CIP Reliability Standards.	Version 4	CIP-002
386	The Commission adopts its CIP NOPR proposal and directs the ERO to develop modifications to Reliability Standards CIP-003-1, CIP-004-1, and/or CIP-007-1, to ensure and make clear that, when access to protected information is revoked, it is done so promptly.	Version 4	Access Control and Auditing
397	The Commission directs the ERO to develop modifications to Requirement R6 of CIP-003-1 to provide an express acknowledgment of the need for the change control and configuration management process to consider accidental consequences and malicious actions along with intentional changes.	Version 4 / Guideline	Change Management, System Lifecycle and Information Management
433	we direct the ERO to consider, in developing modifications to CIP-004-1, whether identification of core training elements would be beneficial and, if so, develop an appropriate modification to the Reliability Standard.	Version 4	Personnel and Physical Security
434	The Commission adopts the CIP NOPR's proposal to direct the ERO to modify Requirement R2 of CIP-004-1 to clarify that cyber security training programs are intended to encompass training on the networking hardware and software and other issues of electronic interconnectivity supporting the operation and control of critical cyber assets.	Version 4	Personnel and Physical Security
435	Consistent with the CIP NOPR, the Commission directs the ERO to determine what, if any, modifications to CIP-004-1 should be made to	Version 4	Personnel and Physical

Paragraph	Text	Phase[13]	Team
	assure that security trainers are adequately trained themselves.		Security
443	We also direct the ERO to identify the parameters of such exceptional circumstances through the Reliability Standards development process	Version 4	Security Governance
460	The Commission adopts the CIP NOPR proposal to direct the ERO to develop modifications to CIP-004-1 to require immediate revocation of access privileges when an employee, contractor or vendor no longer performs a function that requires physical or electronic access to a critical cyber asset for any reason (including disciplinary action, transfer, retirement, or termination).	Version 4	Personnel and Physical Security
464	We also adopt our proposal to direct the ERO to modify Requirement R4 to make clear that unescorted physical access should be denied to individuals that are not identified on the authorization list, with clarification.	Version 4	Personnel and Physical Security
473	The Commission adopts its proposals in the CIP NOPR with a clarification. As a general matter, all joint owners of a critical cyber asset are responsible to protect that asset under the CIP Reliability Standards. The owners of joint use facilities which have been designated as critical cyber assets are responsible to see that contractual obligations include provisions that allow the responsible entity to comply with the CIP Reliability Standards. This is similar to a responsible entity's obligations regarding vendors with access to critical cyber assets.	Version 4	Security Governance
476	we direct the ERO to modify CIP-004-1, and other CIP Reliability Standards as appropriate, through the Reliability Standards development process to address critical cyber assets that are jointly owned or jointly used, consistent	Version 4	Security Governance
511	The Commission adopts the CIP NOPR's proposal to direct the ERO to identify examples of specific verification technologies that would satisfy Requirement R2.4, while also allowing compliance pursuant to other technically equivalent measures or technologies.	Version 4	Operations Security
525	The Commission adopts the CIP NOPR proposal to require the ERO to modify CIP-005-1 to require logs to be reviewed more frequently than 90 days	Version 4	Access Control and Auditing
526	the Commission directs the ERO to modify CIP-005-1 through the Reliability Standards development process to require manual review of those logs without alerts in shorter than 90 day increments.	Version 4	Access Control and Auditing
526	The Commission directs the ERO to modify CIP-005-1 to require some manual review of logs, consistent with our discussion of log sampling below, to improve automated detection settings, even if alerts are employed on the logs.	Version 4	Access Control and Auditing
528	the Commission clarifies its direction with regard to reviewing logs. In directing manual log review, the Commission does not require that every log be reviewed in its entirety. Instead, the ERO could provide, through the Reliability Standards development process, clarification that a responsible entity should perform the manual review of a sampling of log entries or sorted or filtered logs.	Version 4	Access Control and Auditing
541	we adopt the ERO's proposal to provide for active vulnerability assessments rather than full live vulnerability assessments.	Version 4	Recovery and Response
542	the Commission adopts the ERO's recommendation of requiring active vulnerability assessments of test systems.	Version 4	Recovery and Response
544	the Commission directs the ERO to revise the Reliability Standard so that annual vulnerability assessments are sufficient, unless a significant	Version 4	Recovery and Response

Paragraph	Text	Phase[13]	Team
	change is made to the electronic security perimeter or defense in depth measure, rather than with every modification.		
544	we are directing the ERO to determine, through the Reliability Standards development process, what would constitute a modification that would require an active vulnerability assessment	Version 4	Recovery and Response
547	we direct the ERO to modify Requirement R4 to require these representative active vulnerability assessments at least once every three years, with subsequent annual paper assessments in the intervening years	Version 4	Recovery and Response
581	The Commission adopts the CIP NOPR proposal and directs the ERO to develop a modification to CIP-006-1 to require a responsible entity to test the physical security measures on critical cyber assets more frequently than every three years,	Version 4	Recovery and Response
609	We therefore direct the ERO to develop requirements addressing what constitutes a "representative system" and to modify CIP-007-1 accordingly. The Commission directs the ERO to consider providing further guidance on testing systems in a reference document.	Version 4 / Guideline	Change Management, System Lifecycle and Information Management
610	we direct the ERO to revise the Reliability Standard to require each responsible entity to document differences between testing and production environments in a manner consistent with the discussion above.	Version 4	Change Management, System Lifecycle and Information Management
611	the Commission cautions that certain changes to a production or test environment might make the differences between the two greater and directs the ERO to take this into account when developing guidance on when to require updated documentation to ensure that there are no significant gaps between what is tested and what is in production.	Version 4	Change Management, System Lifecycle and Information Management
619	The Commission adopts the CIP NOPR proposal with regard to CIP-007-1, Requirement R4. [The Commission proposed to direct the ERO to eliminate the acceptance of risk language from Requirement R4.2, and also attach the same documentation and reporting requirements to the use of technical feasibility in Requirement R4, pertaining to malicious software prevention, as elsewhere. The Commission discussed the issues of defense in depth, technical feasibility, and risk acceptance elsewhere in the CIP NOPR and applied those conclusions here. The Commission further proposed to direct the ERO to modify Requirement R4 to include safeguards against personnel introducing, either maliciously or unintentionally, viruses or malicious software to a cyber asset within the electronic security perimeter through remote access, electronic media, or other means]	Version 4 / not scheduled	Operations Security
622	The Commission also directs the ERO to modify Requirement R4 to include safeguards against personnel introducing, either maliciously or unintentionally, viruses or malicious software to a cyber asset within the electronic security perimeter through remote access, electronic media, or other means, consistent with our discussion above	Version 4 / not scheduled	Operations Security
628	The Commission continues to believe that, in general, logs should be reviewed at least weekly and therefore adopts the CIP NOPR proposal to require the ERO to modify CIP-007-1 to require logs to be reviewed	Version 4	Access Control and Auditing

Paragraph	Text	Phase[13]	Team
	more frequently than 90 days, but leaves it to the Reliability Standards development process to determine the appropriate frequency, given our clarification below, similar to our action with respect to CIP-005-1		
629	The Reliability Standards development process should decide the degree to which the revised CIP-007-1 describes acceptable log sampling. The ERO could also provide additional guidance on how to create the sampling of log entries, which could be in a reference document.	Version 4 / guideline	Access Control and Auditing
633	The Commission adopts the CIP NOPR proposal to direct the ERO to clarify what it means to prevent unauthorized retrieval of data from a cyber asset prior to discarding it or redeploying it.	Version 4	Change Management, System Lifecycle and Information Management
635	the Commission directs the ERO to revise Requirement R7 of CIP-007-1 to clarify, consistent with this discussion, what it means to prevent unauthorized retrieval of data.	Version 4	Change Management, System Lifecycle and Information Management
661	the Commission directs the ERO to develop a modification to CIP-008-1 to: (1) include language that takes into account a breach that may occur through cyber or physical means; (2) harmonize, but not necessarily limit, the meaning of the term reportable incident with other reporting mechanisms, such as DOE Form OE 417; (3) recognize that the term should not be triggered by ineffectual and untargeted attacks that proliferate on the internet; and (4) ensure that the guidance language that is developed results in a Reliability Standard that can be audited and enforced	Version 4 / Guideline	Recovery and Response
673	The Commission adopts the CIP NOPR proposal to direct the ERO to modify CIP-008-1 to require each responsible entity to contact appropriate government authorities and industry participants in the event of a cyber security incident as soon as possible, but, in any event, within one hour of the event, even if it is a preliminary report.	Version 4 / Guideline	Recovery and Response
676	the Commission directs the ERO to modify CIP-008-1 to require a responsible entity to, at a minimum, notify the ESISAC and appropriate government authorities of a cyber security incident as soon as possible, but, in any event, within one hour of the event, even if it is a preliminary report.	Version 4 /. Guideline	Recovery and Response
686	The Commission adopts the CIP NOPR proposal to direct the ERO to modify CIP-008-1, Requirement R2 to require responsible entities to maintain documentation of paper drills, full operational drills, and responses to actual incidents, all of which must include lessons learned.	Version 4	Recovery and Response
686	The Commission further directs the ERO to include language in CIP-008-1 to require revisions to the incident response plan to address these lessons learned.	Version 4	Recovery and Response
694	For the reasons discussed in the CIP NOPR, the Commission adopts the proposal to direct the ERO to modify CIP-009-1 to include a specific requirement to implement a recovery plan.	Version 4	Recovery and Response
694	We further adopt the proposal to enforce this Reliability Standard such that, if an entity has the required recovery plan but does not implement it when the anticipated event or conditions occur, the entity will not be in	Version 4	Recovery and Response

Paragraph	Text	Phase[13]	Team
	compliance with this Reliability Standard.		
739	The Commission adopts the CIP NOPR proposal to direct the ERO to modify CIP- 009-1 to incorporate guidance that the backup and restoration processes and procedures required by Requirement R4 should include, at least with regard to significant changes made to the operational control system, verification that they are operational before the backups are stored or relied upon for recovery purposes	Version 4	Recovery and Response
748	The Commission adopts the CIP NOPR proposal to direct the ERO to modify CIP-009-1 to provide direction that backup practices include regular procedures to ensure verification that backups are successful and backup failures are addressed, so that backups are available for future use.	Version 4	Recovery and Response

Appendix #9 Communication Plan

Communications Plan for Cyber Security Order 706 Project – Version 4

Background

On January 18, 2008, the Federal Energy Regulatory Commission (FERC) issued Order No. 706 that approved Version 1 of the Critical Infrastructure Protection standards (CIP-002-1 through CIP-009-2). In the Order, FERC also directed numerous modifications to the standards. NERC initiated Project 2008-06 – Cyber Security Order 706, whose scope includes addressing the FERC directives in Order No. 706. The drafting team assembled for this project segmented the scope of work into multiple phases: Versions 2 and 3 of the CIP standards addressed timely FERC directives regarding reasonable business judgment and other non-controversial issues. The bulk of the Order No, 706 directives are to be addressed in Version 4 of the standards. NERC's objective is to produce an approved revision to CIP-002 by June, 2010 and revisions to CIP-003 through CIP-009 by the end of 2010.

NERC and especially the drafting team recognizes that effective communications regarding the ongoing work of the team is crucial to the success of the project and is vital to achieving the consensus necessary for passage in the balloting process.

Mission

Inform and educate reliability stakeholders about Version 4 of the Project 2008-06 — Cyber Security Order 706 standards project, and promote input and participation from stakeholders and regulators.

Scope/Objectives

1. Obtain stakeholder (industry and government) buy-in by communicating importance of Version 4 of the CIP-002 through CIP-009 reliability standards:
    a. communicate paradigm shift in approach to Version 4 relative to prior versions
    b. communicate benefits to reliability
    c. justify commitment of resources
    d. justify aggressive schedule for completion in 2010
2. Ensure key audiences (FERC, trade groups, NERC committees) are kept abreast of the drafting team's plans, successes, and challenges
3. Prepare industry stakeholders, in particular the Registered Ballot Body, to respond promptly and fully to requests for comment and ballots by providing adequate information about drafting team discussions and decisions as they occur
4. Create a feedback clearinghouse to determine information gaps and develop FAQ, where necessary

Audience

- All NERC registered entities held to compliance with NERC CIP-002 through CIP-009 reliability standards
- NERC standards, compliance, and other relevant staff (ex. Standard Coordinators, Compliance Registry, Enforcement, etc)
- NERC Member Representatives Committee
- NERC Standing Committees and relevant taskforces, ad hoc groups, subcommittees, and contractors (ex. Operating Committee, Planning Committee, Critical Infrastructure Protection Committee)
- Regional Entity staff and committees (ex. equivalent of NERC Standards Committee)
- Regional Entity management group
- FERC Commissioners, Office of Electric Reliability staff, and Office of Enforcement staff

- Industry executives (senior managers and CEOs)
- Line employees, subject matter experts, and members of standard drafting teams
- Trade associations (EEI, APPA, NRECA, EPSA, ELCON, NARUC)
- Public Utility Commissions

Topics

Concepts	• Core aspects of CIP-002-4: categorizing cyber systems based on BES reliability functions; • Core aspects of CIP security controls (requirements) based on cyber system categorization (CIP-003-4 through CIP-009-4)
Benefits and importance	• demonstrate the criticality of project success in 2010 to NERC's overall success • improve the overall quality and robustness of the NERC critical infrastructure protection standards • more objective determination (bright line thresholds) of asset categorization for applying security controls • positive impact on overall reliability of the grid • benefits to stakeholders by demonstrating ability to produce good standards timely • obtain CEO-level support for project that is communicated throughout organizations
Resources	• what resources are needed to support the drafting team in producing Version 4 technically and administratively • when and for how long
Timeline	• CIP-002-4 ballot completed by end of May, 2010 • CIP-003-4 through CIP-009-4 ballot completed by end of 2010
Impact on process	• what will be different in the drafting, reviewing, and balloting process for these Version 4 CIP standards as opposed to other typical standards projects • import of external support to facilitate drafting team efficiency, e.g. facilitation, technical writing, etc. • impact of resource commitment to Project 2008-06 may impact support for other active projects
Information sources	• where stakeholders can get further information as project proceeds in 2010 • provide access to message packages as they are available (especially for trade groups)

Delivery Methods

e-mail	• use distribution lists to ensure full coverage (NERC, Regional Entities, etc.) • use Regional Entity distribution lists to reach targeted personnel
Webinars	• associated with each posting of the standards for comment; o conduct for each significant proposal/modification for which comment is requested • record and "distribute/make available" for those who cannot attend

	• include feedback option (on demand after structured presentation/Webinar)
Committee meetings (NERC, Regional)	• attend meetings and communicate message • request special call if necessary for briefing
NERC Web site	• centralized place; linked from Regional Entity sites • headline news, big button on home page (similar to "Renewables"), pop-up page, project page, standards under development, and other frequently hit pages
Structured conference call and/or meeting	for standards drafting team representatives and NERC coordinators, including contractors;
Face-to-face outreach	• e.g. trade groups, FERC commissioners and staff, Regional Entities, committees • high-level involvement from NERC • goal: discuss Version 4 standards project with each trade organization, and at each Regional Entity general meeting at least once in spring and once in Fall, 2010.
"Canned message"	• slides and presentations (project information – overview, etc.) • files accessible via Web site and possible in-person delivery of recorded message
Press releases	As significant milestones are achieved – e.g. ballot approval, NERC Board approval, regulatory approval.
Newsletters	Monthly NERC News updates; Regional Entity newsletters
Workshops	• Include as agenda item on regional workshops • Special Cyber Workshop (?) • NERC Standards workshop (Fall 2010)
Regional Entity management group meetings/calls	Group holds weekly (Friday) conference calls and meets face-to-face prior to certain high-level meetings – standing committees, BOT Ask Regional Entity Mangers to discuss the initiative at various conferences they attend to relay the message and gain additional support from stakeholders

Delivery Plan/Timeline

Planned Tactics:

Date	Tactic	Audience	Content Developer(s)	Presenter/Delivery
January 22, 2010	Announce NERC-sponsored Webinar	Industry	Carl Dombek, Gerry Adamski	Carl Dombek, Gerry Adamski
January 25, 2010	Submit communications plan to drafting team for endorsement	Drafting team	Gerry Adamski	Gerry Adamski
End of January 2010	Review and revise web page for high-level updates (with links from home page and standards pages)	Industry/FERC	Gerry Adamski, Carl Dombek,	Gerry Adamski
Periodically	Provide custom NERC cyber newsletter on development efforts	Industry	Joe Bucciero	Joe Bucciero
February 2010	Develop a frequently asked questions document for Web page	All	Drafting team	Drafting team
February 3, 2010, 1 PM EST	Conduct industry webinar to discuss CIP-002-4 draft	Industry	Standard Drafting Team	Philip Huff, et al.
February 15, 2010	Provide status update	MRC and NERC Board	Gerry Adamski/Mike Assante in concert with drafting team	Gerry Adamski/Mike Assante
February 19 2010	Develop talking points and core messages that would be used in various levels of detail for all communications for CIP-002-4 posting and for CIP-003-4 through CIP-009-4 development.	All	Standard Drafting Team members TBD, NERC staff (Carl Dombek), NERC regional communications group	TBD
February - December 2010	Provide individual briefings on anticipated process and schedule	Electric trade associations, regional entity member meetings, FERC Reliability	Gerry Adamski, Mike Assante, Drafting Team leaders	Gerry Adamski, Mike Assante, Drafting Team leaders

Date	Tactic	Audience	Content Developer(s)	Presenter/Delivery
	Obtain feedback	Office		
March 16-18, 2010	Provide status update	Standing Committees	Gerry Adamski/Mike Assante in concert with drafting team	TBD
Early April 2010	Conduct (and record) Webinar held on CIP-003-4 through CIP-009-4. Solicit feedback during Webinar	Industry	Drafting team, NERC staff	Drafting team members TBD
April, 2010	Issue Cauley letter to executive leadership of organizations sponsoring drafting team members expressing appreciation for commitment	Drafting team executive organizational leadership	Carl Dombek, Gerry Adamski	Gerry Cauley
April 2010	Announce NERC-sponsored CIP-003-4 through CIP-009-4 in-person technical conference	Industry	Carl Dombek, Gerry Adamski	Carl Dombek, Gerry Adamski
May 11, 2010	Provide drafting team status report to NERC MRC at May meeting (include assessment of ability to meet targets)	NERC MRC and Board	Gerry Adamski/Mike Assante in concert with drafting team	Gerry Adamski/Mike Assante
May. 2010	Issue news release on positive ballot results for CIP-002-4	All	Gerry Adamski, Carl Dombek	Carl Dombek
May 2010	Issue Cauley letter to stakeholders expressing appreciation for support	Stakeholders	Gerry Adamski; Carl Dombek	Gerry Cauley
June/July 2010	Conduct NERC-sponsored CIP-003-4 through CIP-009-4 in-person technical conference Solicit feedback during Webinar	Industry	Drafting team	Drafting team
June/July 2010	Review efforts conducted through June and draft plan for remainder of year	Communications team	Carl Dombek, Gerry Adamski, Drafting Team leadership	Carl Dombek

Date	Tactic	Audience	Content Developer(s)	Presenter/Delivery
June 15-17, 2010	Provide status update	Standing Committees	Gerry Adamski/Mike Assante in concert with drafting team	TBD
August 4, 2010	Provide status update	MRC and NERC Board	Gerry Adamski/Mike Assante in concert with drafting team	Gerry Adamski/Mike Assante
August, 2010	Announce webinar in support of CIP-003-4 through CIP-009-4	Industry	Carl Dombek, Gerry Adamski	Carl Dombek, Gerry Adamski
August 2010	Conduct webinar in support of CIP-003-4 through CIP-009-4	Industry	Standard Drafting Team	Philip Huff, et al.
September 14-17, 2010	Provide status update	Standing Committees	Gerry Adamski/Mike Assante in concert with drafting team	TBD
November 3, 2010	Provide status update	MRC and NERC Board	Gerry Adamski/Mike Assante in concert with drafting team	Gerry Adamski/Mike Assante
December 7-9, 2010	Provide status update	Standing Committees	Gerry Adamski/Mike Assante in concert with drafting team	TBD
December. 2010	Issue news release on positive ballot results for CIP-003-4 through CIP-009-4	All	Gerry Adamski, Carl Dombek	Carl Dombek
December 2010	Issue Cauley letter to stakeholders expressing appreciation for support	Stakeholders	Gerry Adamski; Carl Dombek	Gerry Cauley

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Agenda
Cyber Security Order 706 SDT Meeting with FERC

January 28, 2010 | 10:30 am – 4:00 pm EST
Dial in: 1-866-740-1260 | Access Code: 6517897

1. **Administrative Items**
    a. Introductions — All
    b. NERC Antitrust Compliance Guidelines — Howard Gugel
    c. Agenda and Objectives — Phil Huff/Howard Gugel

2. **Brief Status of CIP-002 Standard Development —** Phil Huff/Howard Gugel
    a. Current Posting for Informal Industry Comment
    b. Industry Webinar and Outreach
    c. Consideration of Comments by SDT
    d. Schedule for Formal Posting, Ballot, and BOT Approval

3. **Brief Status of Security Controls Standard Development —** Phil Huff/Howard Gugel
    a. Security Controls Drafting Principles
    b. SDT Subteam Process
    c. Schedule

4. **FERC Staff Questions for Standard Drafting Team**

5. **Standard Drafting Team Questions to FERC Staff**

6. **Next Steps —** Phil Huff/Howard Gugel

7. **Action Items —** Howard Gugel

8. **Adjourn**

116-390 Village Blvd.
Princeton, NJ 08540
609.452.8060 | www.nerc.com

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Notes
Cyber Security Order 706 SDT — Project 2008-06

Thursday, January 28, 2010 from 10:30 am – 4:00 pm Eastern
Conference Number: 1-866-740-1260
Conference Code: 6517897

1. **Administrative Items**
   a. Introductions — All
   b. NERC Antitrust Compliance Guidelines — Howard Gugel
   c. Agenda and Objectives — Phil Huff/Howard Gugel

2. **Brief Status of CIP-002 Standard Development — Phil Huff/Howard Gugel**
   a. Current Posting for Informal Industry Comment
   b. Industry Webinar and Outreach
   c. Consideration of Comments by SDT
   d. Schedule for Formal Posting, Ballot, and BOT Approval

3. **Brief Status of Security Controls Standard Development — Phil Huff/Howard Gugel**
   a. Security Controls Drafting Principles
   b. SDT Subteam Process
   c. Schedule

4. **FERC Staff Questions for Standard Drafting Team**

5. **Standard Drafting Team Questions to FERC Staff**

6. **Next Steps — Phil Huff/Howard Gugel**

7. **Action Items — Howard Gugel**

8. **Adjourn**

116-390 Village Blvd.
Princeton, NJ 08540
609.452.8060 | www.nerc.com

Action Items

- FERC to provide feedback to the team as necessary while observing team meetings.
- Regis Binder to look into commission staff providing informal feedback in regard to technical content prior to the formal comment period closing on CIP-002-4.
- FERC and NERC staff to explore policy options in providing formal feedback from the commission.
- FERC and NERC staff to explore options in developing a better approach for allowing entities to apply more appropriate controls while still meeting the compliance objective.

Introduction

Howard Gugel read the NERC Anti-trust guidelines.

Dave Taylor provided a brief introduction of the meeting objectives. The primary meeting objective was to begin a dialogue between the FERC and the SDT on efforts to address directives from Order 706.

Regis Binder provided opening remarks, stating that FERC has followed the SDT cyber security standards development process within constraints of their limited resources. He also indicated that FERC staff cannot speak on behalf of the commission and they cannot discuss matters related to pending orders by the commission.

Status of CIP-002 Standard Development

Philip Huff opened by stating that the purpose of the meeting was to foster ongoing communications between the team and FERC staff. He expressed that the project has a tight schedule, and it will be imperative that there is open dialogue throughout the process if the schedule is to be met.

CIP-002-4 was developed to identify and categorize cyber systems related to Bulk Electric Systems (BES) in North America. The standard is posted for an informal industry comment period that ends February 12. Various team members have attended trade organization meetings in order to open a dialogue and encourage participation during the comment period. The team expects to post the standard for a formal comment period toward the end of February. The project schedule calls for the standard to be filed with FERC by June 1.

Philip further stated that the focus of CIP-002-3 was to protect critical cyber systems. In the new version CIP-002-4, the focus is on protecting the reliability of the BES, not necessarily all cyber systems. This idea was presented in a concept paper published to the industry in July, 2009, which was well received. A critical aspect of this process is the development of security controls, which are under development and are expected to be posted in draft form prior to the ballot on CIP-002-4. Additionally, the team had a few targets in mind. The first was to address direction given to NERC in FERC Order 706. The team also wanted to write the standard to minimize the necessity of TFEs.

At this point, the concept of using a cost vs. benefit for risk analysis was discussed. Previously, a "cafeteria" approach (pick what you like and dislike) was used to develop priorities. The team intends to develop justifications for priorities.

The team members have been split into 6 small groups in order to develop the security controls. The teams will finalize their drafts at the March Standard Drafting Team meeting in Phoenix, in order to post drafts in April.

FERC Questions to SDT

1) They expressed concern about upstream attacks from low impact targets and how the SDT planned to address these in the Standards. They want to ensure that everything would have at least some minimal baseline of security.

- D. Batz - How do we not treat the low assets differently than the very high impact assets?
- Dave Norton - Need to preclude the damage a device could do upstream. Protection needs to prevent navigability to higher impact assets.
- Mike Peters – One of the directives in Order 706 dealt with a mutual distrust architecture in the system. Need to create a true mutual distrust where access to a single facility or system does not translate to full access.
- Norton - Need more rigor about how we apply controls to the "weakest link". Prevent upstream attacks to low impact asset.

2) How is the team using NIST 800-53 with the current compliance program? How do you measure compliance within the NIST Framework?

Refer to question #1 of SDT to FERC. The team had also posed this question to the commission staff.

3) Order 706 directed regional oversight for the identification of Critical Assets. How do you obtain Regional Oversight in the proposed CIP-002-4?

- Jim Brenton - We accomplish this through bright-line, objective criteria.
- R. Binder and M. Peters - On their reading, they would agree this meets the directive of oversight.

4) Regarding the approval of engineering studies by the Reliability Coordinator, do RC's have problems with taking on that responsibility? [Not a concern as much as a question]

Brenton - A lot of concerns on compliance risk and safe-harbor for RCs

SDT Questions to FERC

1) 800-53 is an organizational risk management framework, which allows for tailoring, compensating controls and organizationally defined criteria. However, FERC Order 706 calls for extensive oversight for any exceptions. What are their thoughts on reconciling these seemingly conflicting objectives?

- R. Binder – Cost/benefit principle is difficult to implement in compliance.
- Scott Wartz – Is this a repackaging of Reasonable Business Judgement?
- Philip Huff – No. Compensating controls still achieve the desired objective. It's not a blanket statement.
- M. Peters – Need to identify the control objective and demonstrate how you meet it.

Separate discussion

- M. Peters – Paragraph 152 of Order 706: TFEs is not just technically feasible but also operationally reasonable.
- D. Batz - Uncomfortable with the term "cost". Need to determine the appropriateness and prioritization. Not appropriate to apply same level of protection across every single asset.
- M. Peters - Need to have a minimal level of protection for all of your assets.
- Norton - Brought up "culture of compliance" and difference between "culture of security". It takes auditors that are highly effective.
- Allen Mosher - Fundamentally, this encompasses the approach of results-based standard.

2) The process to make modifications to the Standards through a FERC Order is very resource intensive. Conversely, changes made prior to industry balloting are relatively cheap. Is it possible to have a process where the team can receive feedback from FERC prior to ballot?

FERC staff will investigate options for formal input. In addition, FERC staff will attempt to attend future meetings as schedules allow. They have concerns about providing comments about filings that are pending before the commission.

3) What expectations are there regarding coordination with the Smart Grid CSCTG (Cyber Security Coordination Task Group) product and how we use 800-53/DHS Catalogue?

- Mike Peters – Look at those interface use-cases they are building. You don't have to match exactly what SG does, but the team should consider participating in the process and provide mutual feedback.

4) Have we captured all of the directives from order 706 in the filing from December?

- R. Binder – I don't believe we can comment on this matter since it concerns a pending order.

5) What are their thoughts about filing CIP-002 separate from the remaining security controls?

- R. Binder – There are concerns with filing separately
- P. Huff – This shouldn't be a problem because CIP-002-4 does not reference the Security Controls
- D. Taylor – Yes, but they are a suite of Standards. CIP-002-3 would need to be retired.
- D. Batz – The industry would find it difficult doing technical work for a standard [CIP-002-4] that has no effect.
- J. Brenton – At least the industry can begin work on an approved standard in preparation for the security controls.
- M. Peters – This approach is similar to 800-53, right? Are you looking at eliminating CIP-003 through -009?
- J. Brenton – We don't know how it is going to break out. We'll definitely include what's in the current CIP Standards.
- Allen Mosher – Will there be a mapping of changes?
- J. Brenton – Yes
- H. Gugel – We haven't made decisions on format as a team yet.

[*Later discussion: during SDT question period*]

- R. Binder - Conceptually filing separately provides problems. He just wasn't sure what to do with that.
- Dave Taylor – The security controls would follow soon after
- Jan Bargain – You would be posting the security controls informally, right?
- D. Taylor - Yes
- J. Bargain - As long as the plan to marry the two standards, it shouldn't be a problem.
- R. Binder – Not sure that we can approve CIP-002-4 ahead of the security controls.

6) To what degree can we remove, lessen, or make substitution for prescriptive elements in the current CIP Standard where the risk reduction does not justify the consumption of industry resources in administrative overhead?

- R. Binder – There would need to be a justification for doing so.
- M. Peters - pg.233 of Order 706 reads that any provisions that would better protect the BES, the Standards Dev. Process has the freedom to so. If the administrative elements actually lessen the reliability of the BES, then we can use that provision.
- Dave Taylor - Requires the SDT to have the type of mapping to demonstrate changes and provide justification anyway.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Agenda
Cyber Security Order 706 — Project 2008-06

February 16, 2010, Tuesday- 1 PM to 5 PM CST
February 17, 2010 Wednesday- 8 AM to 5 PM CST
February 18, 2010 Thursday- 8 AM to 5 PM CST
February 19, 2010 Friday- 8 AM to 2 PM CST
ERCOT Austin MET Cente
7620 Metro Center Dr.
Austin, Texas 78744

NOTE:
1. Agenda Times May be Adjusted as Needed during the Meeting
2. Drafting Group Meetings May Not Have Access to Telephones and Ready Talk

Proposed Meeting Objectives/Outcomes

- Review the CSO 706 SDT 2010 Work plan
- Receive updates on other related cyber security initiatives
- Receive a NERC update on implementing the CIP Communication Plan
- Review, discuss industry comments and identify issues raised to be addressed in refinements;
- Review, refine and adopt a revised CIP 002-4 for posting
- Receive progress reports and review assignments for Security Control Sub-Teams
- Agree on next steps and assignments

Draft Agenda

Tuesday February 16, 2009
1:00 p.m. Welcome and Opening Remarks- *John Lim, Chair & Phil Huff, Vice Chair*
Roll Call; NERC Antitrust Compliance Guidelines
Facilitator review and SDT acceptance of January 19-22, 2010 Tucker SDT meeting summary
1:10 Review of Meeting Objectives, Agenda and Meeting Guidelines- *Bob Jones*
1:15 Review of CSO 706 SDT Workplan- February-December, 2010- *Stu Langton*
1:20 Updates on other related cyber security initiatives- *NERC Staff and SDT Members*
1:30 Update on CIP Communication Plan, including Webinar Report
1:45 Review of needed CIP-002-4 Documents for posting: Introduction, Comment Form,

Requirements, Attachments, Implementation Plan.
2:00 Overview of the Industry Comments on the CIP-002-4 *John Lim and Phil Huff*
2:45 Break
3:00 Identification of Key CIP 002-4 Issues Raised by Industry Responses to Comment form
Questions (1-13)
4:30 Review and Initial Discussion of Other Proposed Approaches to CIP-002-4 *(Dave Norton*
etc.)
5:25 Review of Proposal for Wednesday's Agenda
5:30 *Recess*

Wednesday February 17, 2010
8:00 Welcome and Agenda Review- *John Lim & Phil Huff*
8:10 Discussion and Consensus Testing of Concepts and Responses to Industry Comments and
Critiques
10:15 Break
10:30 Discussion and Consensus Testing of Concepts and Responses to Industry Comments and
Critiques
12:00 *Working Lunch*
12:45 Review and Agree on How to Refine CIP 002-4 *(Full Group or Drafting Sub-Groups)*
1:15 Clarify Issues and Begin Draft Possible CIP 002-4 Refinements *(Full Group or Drafting*
Sub-Groups)
4:00 If Sub Team Formed- Initial Reports and Flagging Issues Needing Full Team Guidance
4:55 Review Assignments and Thursday Agenda
5:30 Recess

Thursday February 18, 2010
8:00 Welcome and Agenda Review- *John Lim & Phil Huff*
8:15 Review any Drafting Group Requests/Needs Full Team Feedback
10:00 Break
10:15 Reconvene Drafting Groups to Complete CIP-002-4 Refinements
12:00 *Working Lunch*
1:30 Drafting Group Reports and Full Team Consideration and Consensus Testing of CIP-
002-4 Refinements and Changes.
3:00 Break
4:45 Review Any Final Drafting CIP 002-4 Assignments and Friday's Agenda
5:00 Recess

Friday February 19, 2010
8:00 Welcome and Agenda Review- *John Lim & Phil Huff*
8:05 Review and Adopt Final CIP 002-4 for 45-Day Formal Comment Posting
8:50 *Stretch Break*
9:00 Security Control Sub Teams (6) Progress Reports and key format and substantive issues
for Full Team Guidance to Sub Teams.
12:00 *Working Lunch*- Review and Agree on Next Steps for Developing Security Controls (CIP
003-009) and Work plan for March 2010 Meeting on Security Controls.
Meeting Evaluation
1:00 Adjourn
CSO 706 SDT Meeting Agenda Packet, February 16-19, 2010, Austin TX 3

PROJECT 2008-06 CYBER SECURITY ORDER 706 SDT MEMBERS

1. Rob Antonishen Ontario Power Generation
2. Jim Brenton ERCOT
3. Jackie Collett Manitoba Hydro
4. Jay S. Cribb Information Security Analyst, Southern Company Services
5. Joe Doetzl Manager, Information Security, Kansas City Pwr. & Light Co.
6. Sharon Edwards Duke Energy
7. Gerald S. Freese Director, Enterprise Info. Security America Electric Pwr.
8. **Phillip Huff, Vice Chair** Arkansas Electric Coop Corporation
9. Doug Johnson Exelon Corporation – Commonwealth Edison
10. Frank Kim Ontario Hydro
11. Rich Kinas Orlando Utilities Commission
12. **John Lim, Chair** CISSP, Department Manager, Consolidated Edison Co. NY
13. David Norton Entergy
14. David S. Revill Georgia Transmission Corporation
15. Scott Rosenberger Luminant Energy
16. Kevin Sherlin Sacramento Municipal Utility District
17. Jonathan Stanford Bonneville Power Administration
18. Keith Stouffer National Institute of Standards & Technology
19. John D. Varnell Technology Director, Tenaska Power Services Co.
20. William Winters Arizona Public Service, Inc.

Roger Lampilla NERC
Scott Mix NERC
Dave Taylor NERC
Howard Gugel NERC
Joe Bucciero NERC/Bucciero Consulting, LLC
Robert Jones FSU/FCRC Consensus Center
Hal Beardal FSU/FCRC Consensus Center
Stuart Langton FSU/FCRC Consensus Center

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

CSO 706 SDT MEETING SCHEDULE

JANUARY –DECEMBER 2010

CSO 706 SDT Meeting Agenda Packet, February 16-19, 2010, Austin TX 5

CSO 706 SDT WORKPLAN TO DATE

OCTOBER, 2008 –DECEMBER 2009

DEVELOPMENT OF CIP VERSION 2 AND NEW VERSION FRAMEWORK
OCTOBER 2008–JULY 2009

1. **October 6–7, 2008 — Gaithersburg, MD** Reviewed CIP-002-CIP-009, Agreed on Version 2 approach.
2. **October 20–21 —Sacramento, CA** CIP-002-CIP-009 Version 2 development
3. **November 12–14, 2008 — Little Rock, AR** CIP-002-CIP-009 Version 2 adoption for comment and balloting; CIP-002-CIP-009 New Version process reviewed.
4. **December 4–5, 2008 — Washington D.C.** CIP-002-CIP-009 Version 3 reviewed and debated, SDT member white "working" papers assigned, Technical Feasibility Exceptions white paper reviewed and refined.
5. **January 7–9 — Phoenix, AZ,** Reviewed Technical Feasibility Exceptions white paper**,** reviewed industry comments on CIP-002-CIP-009 Version 2 products — established small groups to draft responses, reviewed New Version white "working" papers.
6. January 15 — WebEx meeting(s) Small group drafted responses to industry Version 2 comments.
7. January 21 — WebEx meeting(s) Small group drafted responses to industry Version 2 comments.
8. **February 2–4, 2009 — Phoenix, AZ** Update on NERC Technical Feasibility Exceptions process**,** VSL process and SDT role**,** review of Version 3 White papers, strawman and principles**,** reviewed and adopted SDT responses to industry comments on Version 2 and Version 2 Product Revisions.
9. **February 18–19, 2009 — Fairfax, VA** Update on Version 2 process**,** NERC TFE process and VSL Team process; reviewed, discussed and refined Version 3 CIP-002 White papers, strawman, and principles.
10. **March 10–11, 2009 — Orlando, FL** Update on NERC TFE and VSL and VRF Team process and review and refine Version 3 CIP-002 Strawman Proposals
    - *March 2–April 1, 2009 — 30-day Pre Ballot*
    - *Mid-March — NERC posts TFE draft Rules of Procedure for industry comment*
    - *March 30, 2009 — WebEx meeting(s) White Paper Drafting Team*
    - ***April 1–10 — NERC Balloting on Version 2 Products***
    - *April 6, 2009 — WebEx meeting — White Paper Drafting Team*
    - *April 8, 2009 — WebEx meeting(s) — White Paper Preview- Full SDT Conference Call*
    - *April 11, 2009 — Version 2 Ballot Results (Quorum: 91.90% Approval: 84.06%) and Industry Comments*
11. **April 14–16, 2009 — Charlotte NC** Update on NERC TFE process, VSL Team process and NERC Critical Assets Survey; agreed and adopted responses for Version 2 industry comments for recirculation ballot; reviewed and refined Version 3 whitepaper and consensus points and progress report to NERC Member Representative Committee (MRC) May meeting.

- *April 28 and May 6, 2009 — White Paper Drafting Team Meetings and WebEx*
- *April 17–27, 2009 — Recirculation Results: Quorum: 94.37% Approval: 88.32%*
- *May 5, 2009 — NERC MRC Meeting, Arlington, VA- SDT progress report.*

12. **May 13–14, 2009 — Boulder City NV** Reviewed MRC presentation and further SDT refinement and discussion of the Version 3 White Paper.
    - June 8 and June 15, 2009 — Working Paper Drafting Team Meetings and WebEx
13. **June 17–18, 2009 — Portland OR** Further SDT refinement of the draft CIP Version 3 Working Paper(s), reviewed SDT development process for June-December 2009; discussed potential SDT subcommittee structure and deliverables.
    - *June — WebEx meeting(s)*
    - *Working Paper drafting group sessions including inputs from selected industry personnel to help establish BES categorization criteria*

CIP-002 DEVELOPMENT OF REQUIREMENTS, MEASURES, ETC. JULY-DECEMBER 2009

14. **July 13–14, 2009 in Vancouver, B.C., Canada**

SDT reviewed, refined, and adopted SDT Working Paper. SDT adopted its response to NERC for Interpretation of CIP-006-1. SDT reviewed and adopted a proposal for CIP-002 Subgroups and Deliverables and convened subgroup organizational meetings to develop work plans. SDT =adopted 2010 Meeting Schedule.

- *July–August Interim Conference call meeting(s)*
- *CIP-002 Subgroup meetings*
- *CIP-002 Coordination Team meeting*

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Notes
Cyber Security Order 706 SDT — Project 2008-06

February 16, 2010 | 1:00 PM to 5:00 PM CST
February 17, 2010 | 8:00 AM to 5:00 PM CST
February 18, 2010 | 8:00 AM to 5:00 PM CST
February 19, 2010 | 8:00 AM to 1:00 PM CST

Robert Jones, Stuart Langton, and Hal Beardall
Facilitation and Meeting Design
FCRC Consensus Center, Florida State University

Joe Bucciero, Bucciero Consulting, LLC

http://www.nerc.com/filez/standards/Project_2008-06_Cyber_Security.html

116-390 Village Blvd.
Princeton, NJ 08540
609.452.8060 | www.nerc.com

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

CSO706 SDT February 16-19, 2010 Meeting Summary Contents

CSO706 SDT FEBRUARY 16-19, 2010 MEETING
EXECUTIVE SUMMARY

On Tuesday afternoon, the Chair, John Lim welcomed the members and Joe Bucciero conducted a roll call of members and participants in the room and on the conference call. Mr. Bucciero reviewed the need to comply with NERC's Antitrust Guidelines. The host Jim Brenton, a SDT member, welcomed everyone to the ERCOT facilities and covered logistics. The Chair reviewed the meeting objectives and Bob Jones, facilitator, reviewed the proposed meeting agenda. On Thursday morning the SDT approved without objection the meeting summary for the January 19-22, 2010 SDT session in Tucker, Georgia.

Bob Jones reviewed the SDT workplan and schedule and provided an overview of an alternative schedule that Chair John Lim developed for the SDT's consideration. Mr. Lim noted that Gerry Adamski, NERC's standards director, contacted him and the Vice Chair late last week to discuss the schedule in light of industry concerns with going to ballot with CIP-002-4 separately from the balloting of the controls requirements standard. Following the meeting, the Chair put together a draft alternative schedule to address this concern which was cited by over 75% of industry comments and was raised in the February 9 SDT conference call to review trade association and regional meetings that discussed CIP-002-4. The new schedule is designed to give the SDT more time to address comments and prepare a better, more complete draft for formal posting later in the year. On Thursday, the revised schedule with a memo and Gant chart to be drafted for the Standards Committee's review was unanimously adopted by the SDT.

Mike Gent, former President of NERC and Vice Chair of the ERCOT Board, thanked SDT members for their work and noted that with at least three bills in Congress giving FERC more authority, we know we have to act even though there may be different visions of what doing the right thing means.

On Friday, Gerry Adamski, Director of Standards provided an overview of the Communication Plan that was circulated to the SDT at the conclusion of the Tucker meeting and after discussion with the SDT agreed to begin planning for an industry workshop in late Spring after the new CIP 002 and the controls requirements standards are out for review.

NERC Staff and members provided brief updates on related cyber security efforts relating to the Critical Asset and Cyber Asset Identification Process, a presentation on the Team's work at the ARC World Forum, a NERC bulk system policy statement, and NIST's release of a second draft of their report and a Cyber Shock Wave cyber attack exercise
The SDT reviewed industry responses to the Comment Form Questions provided with the preliminary draft CIP-002-4 standard for industry comment and discussed refinements of CIP 002-4. The Chair and Vice Chair proposed using the "points of agreement/disagreement/confusion table" that was started on Tuesday and asked members to

add any additional concerns as the Team reviewed the industry responses to Comment Form questions. The Industry Comment Form featured 13 questions and the Team received over 500 pages in comments. For most of the questions, there was a relatively low level of industry agreement with the proposals (between 20-40%). In preparation for the meeting, John Lim, Phil Huff, Howard Gugel and Scott Mix agreed to review the industry comments received in response to the Comment Form questions and provide the SDT with a review of the themes and a summary of the industry's comments. The full SDT reviewed the summary of industry comments, and later split into the following sub-teams to review and propose revisions to the CIP 002-4 standard based on the comments received: Definitions; Attachment #1; VSLs; Standards Requirements; and External Oversight.

CSO 706 SDT Points of Agreement, Disagreement and Confusion in Terms of CIP 002-4

Points of Agreement *regarding Industry Comments on CIP 002-4*	**Points of Disagreement *regarding Industry Comments on CIP 002-4***	**Industry Points of Confusion *regarding CIP 002-4***
1. Flexibility is needed but may or may not be included in today's language	1. What is the CIP standard trying to protect against?	1. Do you start with R1 and work through R3 or is there more flexibility possible in CIP 002-4?
2. Functions of BES need to be considered, but may not be clear in today's standard language	2. Should it be connectivity vs. impact assessment	
3.Some form of inventory will be needed regardless of approach	3. How extensive should the inventory be for each approach	
4. Any approach needs to result in a categorized list of cyber systems	4. The cyber system should inherit the categorization of the BES asset (indirect impact mapping) vs. basing the categorization on an assessment of the external and internal threats (direct impact mapping)	
5. The SDT is addressing a range of cyber systems at play in the real-time control and operation of the BES	5. There should be flexibility and third party oversight as to what equipment has a reliability impact on the BES	
6. Bright lines will help to simplify the implementation and compliance with the standards	6. Categorization should be based on threat/ reach/ connectivity	
7. Where ever possible, the SDT should seek to combine steps and simplify the approach	7. If we are using a compliance framework, we should stick with a CIP 003-009 structure	
8. We function in a compliance vs. a performance assurance framework.		
9. The standard should be designed so those implementing it know why they are protecting assets and systems.		

10.We are designing a compliance not a performance assurance framework		

The SDT Reviewed Alternative Approaches to CIP 002-4 including a categorization of BES cyber systems based on use of routable protocols. Dave Norton had circulated in advance of the meeting a proposal which suggested the categorization of BES cyber systems should be primarily based on use of routable protocols (threat/reach/connectivity). The following proposal was presented for the Team's consideration:

Categorizations of BES cyber systems based on the potential impact of their compromise through the use of routable protocols as attack vectors.

- **Control center routable protocol = high**
- **Generation plant/transmission substation = medium**
- **All else = low**

Acceptability Ranking Scale	***4** = acceptable, I agree*	***3** = acceptable, I agree with minor reservations*	***2** = not acceptable unless major reservations addressed*	***1** = not acceptable*	***AVG.***
	6	**4**	**9**	**2**	**2.7 of 4**

Jay Cribb offered the following concept for ranking:

Cyber System Impact on BES →	high	medium	low
Connectivity ↓			
Routable	high		
Non-Routable	high		
Stand Alone	medium		

Acceptability Ranking Scale	***4** = acceptable, I agree*	***3** = acceptable, I agree with minor reservations*	***2** = not acceptable unless major reservations addressed*	***1** = not acceptable*	***AVG.***
	4	**13**	**3**	**0**	**3.1 of 4**

Stu Langton reviewed with the Team the difficult nature and complexity of the task at hand and reminded them that we will continue to have disagreements. He noted that the SDT has met all previous deadlines and will continue to work together to meet the upcoming deadlines. Consensus doesn't mean we have to all agree and that we can disagree sometimes – differences are okay – if 75% want to move on, then we will – we need the minority on different issues to hang in there and keep working with us.

Scott Rosenberger presented a revised proposal on Wednesday and spoke about risks presented by connectivity and the challenges in defining terms accurately.

"Include connectivity as a factor in the BES Cyber System categorization"
Revised Proposal: Matrix for Levels of Controls to Be Applied

BES (attachment #1 of CIP 002-4)	High	Med.	Low
Connectivity-Routable/Dial-up	High	High	Med.
Non-Routable	Med.	Low	Low
Not Connected	Low	Low	Low

Acceptability Ranking Scale	***4** = acceptable, I agree*	***3** = acceptable, I agree with minor reservations*	***2** = not acceptable unless major reservations addressed*	***1** = not acceptable*	***AVG.***
	12	**4**	**2**	**0**	**3.6 of 4**

Phil Huff offered the following successive proposals for testing acceptability related to combining Attachment #1 & #2 for the SDT to rank. The SDT reviewed and ranked three versions of the proposal, as follows:

1st Version Proposed by Phil Huff
Attachment 2 and Attachment 1 should be combined into a single set of criteria. The subject of each criterion is the BES Cyber System and the verb would be the function being performed (the Criteria is the Span of Control).

Acceptability Ranking Scale	***4** = acceptable, I agree*	***3** = acceptable, I agree with minor reservations*	***2** = not acceptable unless major reservations addressed*	***1** = not acceptable*	***AVG.***
	2	**9**	**9**	**0**	**2.65 of 4**

2nd Version Proposed by Phil Huff
Attachment 2 and Attachment 1 should be combined into a single set of criteria. The subject of each criterion is the BES Cyber System and the verb would be the function being performed. ~~(the Criteria is the Span of Control).~~

Acceptability Ranking Scale	***4** = acceptable, I agree*	***3** = acceptable, I agree with minor reservations*	***2** = not acceptable unless major reservations addressed*	***1** = not acceptable*	***AVG.***
	1	**11**	**6**	**1**	**2.6 of 4**

Revised Concept of Combining Attachment #1 and #2

On Friday morning, Dave Revill presented a concept of combining Attachment 1 & 2 that was discussed overnight by a group including John Lim, Phil Huff, Dave Revill, Rich Kinas, Patrick Leon, Joe Doetzl, and Dave Norton. He noted that under this proposal:

- Attachment 2 becomes more of a guidance document
- REs shall categorize the BES cyber systems by applying criteria in CIP 002 Attachment 1
- Changed ~~BES Subsystems~~ to BES Cyber Systems
- Changed Generation ~~Subsystem~~ in Attachment 1 to Generation facility.
- Move Attachment 2 to a guidance document to identifying what immediate affect on real-time operations means

This proposal combines Attachment 1 and Attachment 2 by tying the criteria in Attachment 1 to BES Cyber Systems that immediately (i.e., 15 minutes or less) affect real-

time operation. Attachment 2 is moved to a guidance document for identifying Cyber Systems that immediately affect real-time operations. (including the connectivity matrix)

Acceptability Ranking Scale	***4** = acceptable, I agree*	***3** = acceptable, I agree with minor reservations*	***2** = not acceptable unless major reservations addressed*	***1** = not acceptable*	***AVG.***
	8	**10**	**1**	**0**	**3.4 of 4**

The SDT reviewed and ranked the following related to the proposal above:

R1. As a step in identifying appropriate security controls for its assets, each Responsible Entity shall categorize its BES ~~Subsystems~~ Cyber Systems ~~under its ownership~~ by applying the criteria in *CIP-002-Attachment 1 – Criteria for BES Impact Categorization of BES* ~~Subsystems.~~ *Cyber Systems*. (*Violation Risk Factor: High*)

Attachment 1: Criteria for BES Impact Categorization of BES Cyber Systems
Cyber Systems that would immediately affect real-time operations for:

- Generation ~~subsystem facilities~~ with aggregate rated name-plate generation of 2,000 MVA or more.
- Etc.

Move Attachment 2 to a guidance document to identifying what *Immediate affect on real-time operations* means.

Acceptability Ranking Scale	***4** = acceptable, I agree*	***3** = acceptable, I agree with minor reservations*	***2** = not acceptable unless major reservations addressed*	***1** = not acceptable*	***AVG.***
	15	**6**	**1**	**0**	**3.6 of 4**

On Friday morning, the SDT discussed next steps regarding refinements to CIP-002-4 and the development of a response document for the industry's consideration. The Chair proposed and the members agreed that a subteam of 4-6 members would be formed to work on refining CIP-002-4 between now and the March meeting in Phoenix, where they would present a new draft standard back to the full SDT as well as a response document. The team may also continue after the March meeting to finalize these tasks.

On Friday, the Security Controls Requirements Sub-Teams (including Personnel and Physical Security, Security Governance, Recovery and Response, Access, Control and Auditing, Change Management, System Lifecycle and Information Management and Security Operations) reported on progress made since the Tucker meeting, reviewed a set of threshold questions and drafting guidance statements, and met in Sub-teams to work further on their efforts and agreement on next steps. The questions included:

1) How we are going to handle writing requirements that apply to 'BES Cyber Systems' rather than 'Critical Cyber Assets'?
2) At what level are we to write the requirements?
3) We've got to have some kind of ruling on the topic of compensating controls in a NERC

CMEP world.

4) We need a standard way to not only handle the difference in impact and environment (CC/Gen/Tran), but the difference in cyber system/device class.

Based on the SDT discussion, the following guidance statements were proposed to be added to those developed at the Tucker meeting:

- Requirements should apply to either (1) the BES Cyber System as a whole, or (2) components of the BES Cyber System. When a requirement only applies to specific types of components, describe those types of components to determine where component classes exist. Requirements specific to boundary protection or ESP can be written to the interface of the BES Cyber System.
- Sub-Teams should start with the CIP words and tweak if needed to include some DHS language. However, the "level" of the requirements text should be raised, if needed. Be specific, not prescriptive.
- Compensating Controls are not allowed. Need to write a "what" requirement, not a "how" requirement.
- As guidance, the focus should be on setting the level of controls at a level to avoid applying it to a device class, or explain why a control is being applied to a device class (e.g., general purpose platform vs. purpose built platform also, Part A of the TFE for a set of classes)

The Chair reviewed the progress made at the meeting and the need for the sub-teams to continue to meet between Austin and the Phoenix meeting to prepare draft language for the security controls for review by the full SDT. He also noted the agreement on a revised schedule by the SDT and the formation of a subteam to take the CIP-002-4 draft and make refinements and develop a response document to the industry's comments.

The Vice Chair agreed to work with the facilitators to revise the Sub-team drafting guidance statements based on this discussion and circulate them in advance of the March meeting.

The meeting adjourned at 12:15 p.m.

_____

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

CSO 706 SDT JANUARY 19-22, 2010
AUSTIN, TEXAS

MEETING SUMMARY

I. AGENDA REVIEW, WORKPLAN, UPDATES AND COMMUNICATION PLAN

A. Agenda Review

On Tuesday afternoon, the Chair, John Lim welcomed the members and Joe Bucciero conducted a roll call of members and participants in the room and on the conference call *(See appendix #2*). Mr. Bucciero reviewed the need to comply with NERC's Antitrust Guidelines *(See Appendix #3).* He urged the team and other participants in the process to carefully review the guidelines as they would cover all participants and observers. He urged all to avoid behaviors or appearance that would be anti-competitive nature and also reminded the group of the sensitive nature of the information under discussion.

The host Jim Brenton, a SDT member, welcomed everyone to the ERCOT facilities and covered logistics. The Chair reviewed the meeting objectives noting that focus of this meeting will be reviewing the industry comments received and discussing schedule forward – start drafting responses to comments following review and discussion of the schedule in response to comments and concerns from industry about addressing 002-4 separately from the rest of the standards. Phil Huff noted the intention was to consider the summary and full set of comments in small groups related to the questions posed in the comment form in order to develop general responses. He reminded the SDT that these are "informal comments" and we want to be responsive and keep the dialogue with industry going. Bob Jones, facilitator, reviewed the proposed meeting agenda *(See appendix #1*). On Thursday morning the SDT approved without objection the meeting summary for the January 19-22, 2010 SDT session in Tucker, Georgia.

B. SDT Workplan and Schedule

Bob Jones reviewed the SDT workplan and schedule and provided an overview of an alternative schedule that Chair John Lim developed for the SDT's consideration. (*See Appendix #5).* Mr. Lim noted that Gerry Adamski, NERC's standards director, contacted him and the Vice Chair late last week to discuss the schedule in light of industry concerns with going to ballot with CIP-002-4 in late Spring and then separately later in 2010 balloting CIP 003-009. Following the meeting, the Chair put together a draft alternative schedule to address this concern which was cited by over 75% of industry comments and was raised in the February 9 SDT conference call to review trade association and regional meetings that discussed CIP-002-4 *(See Appendix #)*

Mr. Lim noted that this issue could put at risk the CIP 002-4 ballot without the remaining pieces being out for simultaneous industry review. The new schedule is designed to give the SDT more time to address comments and prepare a better, more complete draft for formal posting later in the Spring. It calls for informally posting an revised CIP-002-4 draft in March and by April begin to bring the security controls together with the CIP-002 governance standards.

SDT Discussion comments on the Schedule:

- Would a formal request for a second informal comment period need to be approved by the Standards Committee? Probably yes.
- The SDT needs to show progress but also be responsive to concerns from industry to see everything before agreeing to almost anything even in the informal comment period.
- Confused as to what is being proposed regarding the second informal comment period of CIP 002 and 003-009 controls schedule?
- Option to put 002 out for additional informal comment period or wait until other pieces are ready for combined informal comment period
- Posting for standards drafting team review by end of March (or April meeting?)
- CIP 003-009 ready for team review by March and finalized draft of CIP 002 – full package informal posting by April 19th
- The SDT is counting on time in March to prepare the security controls
- This is a slipped schedule – has FERC bought off on this? At the FERC/NERC meeting FERC staff acknowledged it might be problematic to put 002 out early and thought a combined posting made sense.
- CIP 002 is intended to determine bright lines of what to protect, not the how to protect it. Not sure we should say to people can wait until they see the how. This could lead to more gaming the system, what we are trying to get away from.
- People need the 003-009 security controls to understand the intent of CIP-002. Are we rushing to quickly through CIP 002 to get to CIP 003-009? Our schedule makes the assumption members have enough time to do this.
- Concerned about how the controls will match up with CIP-002 – the industry push back means they do not understand how the high/medium/low will work and fear that too much will be put in the high category. The schedule may be quick but not sure how else to do it.
- Early March post revised CIP 002 draft for comment to the SDT – remove “informal” to avoid confusion – FERC is going to wait until the whole package is ready to review. In order to meet end of the year deadline there is not much we can pull out of this proposed schedule – open to ideas for changes that would improve the product.
- Change “post” to circulate to avoid confusion
- The SDT members should be careful and avoid using “gaming the system.” The reality is that people are not sure what high/medium/low means and how controls will help define and be applied to each.
- We will not be ready to present the first draft of security controls at the March SDT meeting. Can present progress to review with full committee – this meeting we could focus and getting CIP-002 closer to completion.

- Taking CIP-002 off the table by June may help us to polish CIP002 but may take time away from preparing security controls. CIP- 002 is the most important piece to get right.
- It will be difficult to meet this proposed schedule– to have prayer of doing this we need to clarify common understanding of threshold questions across the sub-teams.
- Question for NERC standards committee? Communication with FERC regarding changes in the schedule?
- Be sure to look at the July period on – posting for three comment periods will require a lot of time for responding to those questions
- People are confused by the multiple sources requesting comments – series of rapid turnarounds may further confuse the industry
- Need to approve a new schedule? Review highlights and check on questions:
- In Austin – react to comments and develop consensus on 002 – start redrafting 002
- Sub-team meetings in next two weeks to refine 002 – by beginning of March have draft for full team review.
- Phoenix – finalize CIP 002 draft by end of first meeting day for posting/review but not comments – focus on sub team drafting of 003-009 controls.
- April 5th– have all control groups to have drafts for circulation to the rest of the SDT team as a package
- March in Phoenix: First draft of what? The controls? Should say draft CIP 002 for full team comment in Phoenix followed by team review of sub-team progress and drafts of sub team drafts of controls requirements.
- Present controls draft requirements for full team review and comment week of 4/12 followed by Sub-team refinements as needed in response.
- Posting of full package in May for informal comment
- May time period for a technical conference (face-to-face) or webinar with industry for review and comments?
- Should we think of a thirty day comment period allowing us to post May 1 with comments by May 31 – gives us time to work in sub teams through April – deal with comments/responses at the June meeting – everything following June stays the same
- Consider the mid-May meeting dates in Dallas for preparing for a technical conference to follow a week or two later.
- June SDT respond to comments.
- Series of ballot/comment periods in subsequent SDT meetings – formal comment periods require responses to each comment.
- Schedule allows for three comment periods if needed – can make changes to the draft based on the comments – allowed to keep the same ballot pool and deviate from required process to shorten periods required for re-balloting
- Need to verify assumptions in schedule with the Standards committee – Chair will take this forward.
- May need more time at the end to be sure prepared to file
- If make significant changes to the standard may impact those who need to be in the ballot pool

- Attach a draft schedule with a memo for the Standards Committee – put into a gant chart to show alignment?
- Review on Friday for adoption
- Schedule needed to meet requests is aggressive and will require people at this table to devote time and resources to make it happen – once approved we will be stuck with it

On Thursday the Revised schedule with a memo and Gant chart to be drafted for the Standards Committee's review was unanimously adopted by the SDT.

Mike Gent, former President of NERC and Vice Chair of the ERCOT Board, thanked SDT members for their work and noted the Team should blame him for some of this work. He also noted the facilitation team helped NERC in working with the Blue Ribbon Group in 1997-98 that lead the creation of the ERO. We wanted to be sure that the industry were effective without being too burdensome because doing nothing is unacceptable. While there may be different visions of doing the right thing and we are still not sure what we have to do, but know we have to do it. There are presently at least three bills in Congress giving FERC more authority.

C. NERC Update on Implementing the CIP Communication Plan

On Friday, Gerry Adamski, Director of Standards provided an overview of the Communication Plan that was circulated to the SDT at the conclusion of the Tucker meeting.

- Begin work on implementation in terms of industry outreach.
- NERC may produce a newsletter of which this would be a part as well as a maintained frequently asked questions list. For example the new concept of connecting CIP 002 with CIP 003-009 for industry review would be a good example.
- NERC also convened a meeting with FERC in January to review SDT progress.
- Need to hear more about the communication plan at a meeting soon
- The SDT Webinar on CIP 002-4 in late January was a helpful effort that had 475 registered and that members Jay Cribb and Sharon Edwards moderated and John and Phil joined in as well. There were many thoughtful questions – many of the concerns in the industry comments came out during the Webinar discussions
- Spent a lot of time explaining why the changes were needed
- The most heard comment involved the need to see CIP 003-009 before approving CIP 002
- They expressed they were used to the current system and hoped the SDT would build on it . They did not say it was necessarily the best system.

SDT Questions and Comments

- The team's adopted revised schedule will impact our communication plan.

- We need to communicate with a summary document our work on and with the informal comments – "post" the revised CIP-002 on website without soliciting industry comment and wait to marry this with the rest of the package of security controls.
- Consider an industry conference call to lay out the new strategy and schedule.
- Also consider an in-person face-to-face technical conference/workshop later in the Spring (Late May). This would take a lot of work and communication on NERC's part.
- Use the mid-May SDT Meeting to work on preparation for the workshop.
- Consider marrying the workshop up with the June team meeting in Sacramento?
- Need to get an updated copy of the communication plan to members so they can review and offer comments or suggestions.
- What would be the preferred location for the workshop? Connected to a SDT meeting? Near a central major airport?

D. Related Cyber Security Efforts:

NERC Staff and members provided the follow brief updates on related cyber security efforts:

- Scott Mix noted that the Critical Asset and Cyber Asset Identification Process comment period closes at the end of February. He noted there has been some confusion regarding these overlapping but distinct efforts and the closing of this process should help in that regard.

- Keith Stouffer reported on a presentation on the Team's work at the ARC World Forum much of the audience familiar with what is going on – aware of proposed expansion of scope of the standards – some worried it would seep down into distribution – anxious to see the final product.

- NERC is also coming out with a bulk system policy statement. It would be helpful to the Team to have someone from NERC provide clarification – may expand our understanding of the bulk electric system.

- Joe Bucierro noted that NIST has released a second copy of their report. He suggested that individual Team members may want to review and comment as appropriate. There also may be some point of coordination that the Team may want to consider going forward. Several Team members have been participating in the development of the report.

- Cyber Shock Wave was a bi-partisan policy group running an cyber attack exercise. Jay Cribb and other Team members were involved in helping write the scenarios.

II. SDT REVIEW OF INDUSTRY COMMENTS ON CIP-002-4

A. Reviewing Industry Responses to Comment Form Questions and Discussion of Refinements

The Chair and Vice Chair proposed to use the points of agreement/disagreement/confusion table (*see B.2 Below*) started on Tuesday and asked members to add any additional concerns as the Team reviewed the industry responses to Comment Form questions.

The Industry Comment Form featured 13 questions and the Team received over 500 pages in comments. In preparation for the meeting, John Lim, Phil Huff, Howard Gugel and Scott Mix agreed to review the industry comments responding to the questions and provide a review of the themes and a summary of the industry's response to CIP 002-4.

1. Comment Form Question #1 – Definitions

Scott Mix provided the overall summary for Question #1 from the industry responses for definitions of new or revised terms for possible inclusion in the NERC Glossary. These included: Cyber System, BES Cyber System, Bulk Electric System Subsystem (BES Subsystem), Generation Subsystem, Transmission Subsystem, Control Center, High BES Impact, Medium BES Impact, and Low BES Impact.

1. Do you agree with the definitions and adoption of the following new or revised terms for inclusion in the NERC Glossary: Cyber System, BES Cyber System, Bulk Electric System Subsystem (BES Subsystem), Generation Subsystem, Transmission Subsystem, Control Center, High BES Impact, Medium BES Impact, and Low BES Impact? If not, please supply and explain your proposed modification.

Overview of Industry Responses to Question #1 Definitions

General Responses.

- CIP 002-4 is still too complex / no clarity / ambiguous / vague
- Retain existing definitions – with clarification, don't reinvent the wheel.
- "BES" vs. "BPS" discussion – consistent across regions – 100kV bright line
- Proper use existing NERC Glossary definitions such as "Element", "Facility", "Adverse Reliability Impact", etc
- Need to see CIP-003 – CIP-009 to assess definitions.

Specific Responses

1.a. Cyber System Definition

1.a. Cyber System — A discrete set of one or more programmable electronic devices organized for the collection, storage, processing, maintenance, use, sharing, communication, disposition, or display of data.

Option	Count	Percent
Agree with proposed definition	30	29.1

Disagree with proposed definition	63	61.2
Total:	**93**	**100.0**

Overview of Industry Responses to Cyber System Definition

- "Subsystem" adds unneeded step and confusion
- More clearly define "Subsystem" / "one or more"
- How do we determine what a "subsystem" is
- Routable and dial-able protocols – accessibility?
- Overly broad definition?
- What does "programmable" mean and where does it come in?
- Cyber "system" term may be unnecessary
- Add phrase "all components necessary to make BES function"
- Is this too vague?

SDT Discussion of Cyber System Definition

- Focus on Routable protocols, dial-up assets / connectivity / accessibility
- Mandate "testing" and "recovery"
- Why include "maintenance", "sharing", "communications", "disposing"
- This is an overly broad definition
- "Programmable" not defined – where programmed (factory or end-user?)
- This may be an unnecessary term – Consider using "Cyber Assets"
- Focus on real-time applications
- Does address "Non-cyber" cyber systems?
- Would encompass every cell phone, etc as a cyber system?

1.b. BES Cyber System Definition

1.b. BES Cyber System — A Cyber System which if rendered unavailable, degraded, or compromised has the potential to adversely impact functions critical to the reliable operation of the Bulk Electric System.

Question 1.b. (99 Responses)

Option	Count	Percent
Agree with proposed definition	27	26.2
Disagree with proposed definition	72	69.9
Total:	**99**	**100.0**

Overview of Industry Responses to BES Cyber System Definition

- Add “also includes all components necessary to ensure the protection of the reliability functions being performed”
- Should refer to Attachment 2
- “Has the potential” is to vague
- Define “critical”, “adverse”, “degrade”, “compromise”, “critical functions”, etc
- Use “Adverse Reliability Impact” which is a defined term
- Use concept of risk
- No benefit over use of Critical Cyber Asset – use Critical Cyber Asset
- Remote accessibility
- Define the term, not the impact
- Capture “misuse”
- Change term to “Critical Cyber System”
- Change “has potential” to “has significant potential” – or change to “will”
- Accessibility issue (wired and wireless)
- Availability of asset impacts “potential to adversely impact” – is this what the SDT wants?
- Add “essential to operations” and “routable protocol”
- Relationship to NRC (nuclear) definitions
- Exclude market systems
- Change to “Cyber Systems controlling BES Facilities”

SDT Discussion Points of BES Cyber System Definition

- Need definitions of compromised, misuse, etc.
- No concept of risk or vulnerability?
- Retain CCA definition
- Change to critical cyber system
- Wired and wireless accessibility
- What about the concept of risk?
- Add essential to operations.
- Note the terms being used here versus those in use in nuclear industry
- Exclude market systems if that is what you want.

1.c BES Subsystem Definition

1.c. Bulk Electric System Subsystem (BES Subsystem) — A group of one or more BES Facilities (i.e., Generation Subsystem, Transmission Subsystem, and Control Center) used to generate energy, transport energy or ensure the ability to generate or transport energy.

Question 1.c. (95 Responses)

Option	Count	Percent
Agree with proposed definition	30	29.1
Disagree with proposed definition	65	63.1

Total:	**95**	**100.0**

Overview of Industry Responses to BES Subsystem Definition

- Define "BES Functions"
- Change to "Generic term for Generation Subsystem, Transmission Subsystem, and Control Center"
- Include "Protection Systems", "SPS', "RAS", "Automatic Load Shedding"
- Change "transport energy" to "transport electricity" -- or drop phrase
- Unnecessary – can use individual terms without loosing any meaning
- Define "shared element"
- We need to better define "BES facility." Break down into transmission, generation and control systems?
- "Transmit" electricity not transport energy
- Shared cyber and subsystems in generation subsystem
- We shouldn't' introduce the ability to decertify to meet compliance.
- Clarify "control system" versus "control room" concept – lack of definition causes confusion.
- Don't include the impact
- Misuse and decoupling causes bad behavior
- It is a open question as to where does generation ends and transmission begins.
- Change "output" to capacity
- Is "capable of" is overreaching?
- Change to "alarm processing"

SDT Comments on Question #1 First Round Responses, 1c. BES Subsystem Definition

- Potential agreement – h/m/l definition should be removed vs. tied to criteria –
- This misunderstanding cascades through the rest of the document.
- **BES Impact.** Support for a BES impact definition? – We need something in the glossary or in the text – but we should leave it at a very high level.
- Consider a BES impact clarification language in the preamble to this.
- Many comments refer to adverse reliability impact? Should we tie to that?
- Keep in mind that we will reference h/m/l in the controls too.
- Does defining BES impact add anything to common use or dictionary definition?
- Do we need BES impact? Already have adverse reliability impact and it covers the need (as read)
- There appears to be a lot of confusion in industry responses between BES cyber systems and cyber systems.
- Move into one definition – remove cyber system definition and collapse into single term of BES cyber system.

- Many of the respondents appear concerned with the subsystem definition and want it removed.
- **How Broad should the "Subsystems" Definition Be?** We have to be careful in responding to the comments– some may be understanding "subsystem" as a unit in a plant. Consider defining it better rather than removing it.
- Confusing topic – The SDT itself could not agree on how many subsystems there are in a plant.
- We do need a better definition – no one knows where this begins or ends – may need to get rid of it?
- Alternatively, we need to be more specific as to what we mean in the criteria.
- Need to better define rather than get rid of it – don't know how to clearly look at our assets as now written. It may be tempting to decouple systems which is not our intent.
- Perhaps use generation and transmission in distinguishing subsystems.
- If the SDT redefines this, we can not leave as a choice. We have to make it clear what a subsystem is.
- Need clarity, not throwing it out.
- If we create new definitions then we need to be clear what we mean – adding new layers doesn't serve anyone.
- Has to be clear for purposes of compliance – be clear or stay away from it.
- Security guidelines define common mode of impact – shared elements have cyber controls – has to be something we can make a difference on cyber security, otherwise we should not group together.
- If we cannot describe it sufficiently, then we need to drop it.
- Many of the comments indicate the subsystems definition was overly broad – can we all agree it should be more limited?
- BES cyber system is an effort to limit it to those impacting the BES system.
- Cannot look at transmission, generation and control systems without the other – can't start with just cyber system.
- Do we want to add back in the distinctions between routable protocol and dial up?
- Want protections over all cyber systems that may impact reliability and connectivity – but careful how we word this. Routable protocols may be easier to access and need higher level of control – but in the end it is about the controls we apply.
- What are we protecting? You can take out a substation and the BES will still function.
- Have not talked about the concept of protecting "data in motion" and how you that can be done.
- **Role of Controls in Handling Vulnerability.** Many industry comments on how to handle vulnerability, connectivity, accessibility to the system – do we handle it in the controls – is it a h/m/l or does it need to be addressed in the requirements?
- You don't put in either.
- Comments suggest we need to handle it – question is where do we best handle it?

- Industry concerned about removal of "routable" – are these critical infrastructure protection standards or cyber security standards? Cyber exists because of routable protocols – clarify which we are focusing on
- **Connectivity.** Putting protection on cyber system in a substation that does not have connectivity is not necessary.
- If BES is high then any cyber system associated with it may be swept in as high as well. We need a separate "if- then" determination of whether the related cyber system is high or not.
- **Categories vs. Risk Categorization.** Categories are impact only – they are not a risk categorization – we haven't come up with a risk categorization that can be audited -
- **N-1.** Propose adding into "disagreement" for discussion the N-1 concept
- "Individual field assets have intrinsically lower impact, on the basis of N-1 (planning?) engineering, than do control systems."
- Does N-1 matter?
- Intrinsically control centers are more important due to the manner we operate – to real time operations
- N-1 refers to credible contingency. There are many items not consider "credible" under N-1 that may still need to be considered in cyber security, e.g. transmission corridor failure is not considered "credible" –
- N-1 is important to planning but may not be to security of the cyber system.
- N-1 doesn't address intentional misuse. Instead is it about handling the largest single contingency?
- Is the 002 concept more succinct than N-1?
- Remove 'on the basis of N-1 engineering" – also change to "control centers" –Now move this up to points of agreement?
- BES is planned to a much higher standard than N-1 – if a transmission corridor is a common one, then contingencies are planned for – we are concerned with multiple external threats – if planning is not considered then you cannot identify the systems that need protection ahead of time.
- Cyber security for N-1 requires understanding the scope and reach of the hacker. This is not an apples-to-apples comparison.
- The way we engineer and operate the current system works. Thatmore accurately captures what I was trying to say than looking at it as N-1.
- Cannot build and design transmission systems for every contingency.
- Removed routable language at the direction of NERC to avoid perception of "gaming." Confusion in industry as to why this was removed is understandable.
- Careful about creating unintended consequences: e.g. airlines are now cancelling flights rather than risk fines for letting passengers sit in the plane on tarmacs too long.
- Need to look at mitigating risk from interconnectivity and from physical access.
- Make sure focus is on power system alarms.

SDT 2nd Round Discussion of Definitions- BES Subsystem Definition

- Need to clarify on the SDT as to what we are trying to protect against. E.g. protect against cyber attack that will impact the BES.
- However that leaves broad areas still open. We need to establish bright lines of potential threats and assure "graceful degradation" under a cyber attack.
- But how can it be measured in a compliance context rather than in a performance-based process?
- We can't prevent an attack, but we can design this so as to slow the attack.
- Cyber security – potential for hackers to attack and infiltrate bulk power system control and operations systems, such that assets could be damaged or misused in sufficient scale as to cause unacceptable outcomes for the BES.
- We need to design not just to address the attack potential, but also so we can avoid impacts due to negligence from within – not just attack vectors from outside.
- "Graceful degradation" as concept, how would it be measured?
- NERC definition– protect against rather than prevent.
- Minimize the impact of a cyber incident – including attack or misuse. We are trying to minimize the negative impacts regardless of internal or external, intentional or not. "Hackers" are not limited to external threats
- It is a term of art widely seen in industry as external and intentional – we need to protect from internal and unintentional too.
- Note the NERC definition includes the language in the paragraph before "cyber security" – includes minimize the risk.
- Still unnecessarily constrains the definition to outsiders with intentions. This does not even include current standards?
- Homeland Security definition? "Use sound risk management principles to implement physical and cyber protective measures that enhance preparedness, security and resiliency." (DHS)
- Maintain/preserve/assure reliability of the BES through implementation of generally accepted information system security practices (GASSP or GAISSP)

1.d. – Generation Subsystem Definition

1.d. Generation Subsystem — Generation plants, or generation units including the Facilities required to connect them to a transmission system, singularly or in combination, including generation units whose combined output could become unavailable due to loss or compromise of a shared element or shared Cyber System.

Question 1.d. (89 Responses)

Option	Count	Percent
Agree with proposed definition	21	20.4
Disagree with proposed definition	68	66.0
Total:	**89**	**100.0**

Overview of Industry Responses

- Remove “shared element”, “shared cyber system”
- See glossary term- “Common Mode”
- Add “misuse”
- Opportunities to decouple systems as artificial behavior
- Define “Generating Plant”, “Generating Unit”, “Transmission System”, “Shared Element”, “Shared Cyber Asset”
- Clarify “Control room” vs. “Control Center”

1.e. – Transmission Subsystem Definition

1.e. Transmission Subsystem — Transmission substations, transmission busses, or transmission lines including the Facilities required to connect them to Elements, singularly or in combination, including transmission lines or busses whose combined output could become unavailable due to loss or compromise of a shared element or shared Cyber System.

Question 1.e. (89 Responses)

Option	Count	Percent
Agree with proposed definition	20	19.4
Disagree with proposed definition	69	67.0
Total:	**89**	**100.0**

Overview of Industry Responses

- Remove “shared element”
- Does “element” refer to glossary term?
- Don’t include impact
- Loss of multiple Elements may not impact reliability
- Add “misuse”
- Opportunities to decouple systems as artificial behavior
- Tie to registration requirements
- No bright line in the generation switch yard
- Add “one or more”
- “singular or in combination” – brings significant uncertainty
- Change “output:” to “capacity”

1.f. – Control Center Definition

1.f. Control Center — A Control Center is capable of performing one or more of the functions listed below for multiple (i.e., two or more) BES assets, such as generation plants or transmission substations. Functions that support real-time operations of a Control Center typically include one or more of the following:

- Supervisory control of BES assets, including generation plants, transmission facilities, substations, Automatic Generation Control systems or automatic load-shedding systems

- Acquisition, aggregation, processing, inter-utility exchange, or display of BES reliability or operability data for the support of real-time operations
- BES and system status monitoring and processing for reliability and asset management purposes (e.g., providing information used by Responsible Entities to make operational decisions regarding reliability and operability of the BPS)
- Alarm monitoring and processing
- Coordination of BES restoration activities.

Question 1.f. (92 Responses)

Option	Count	Percent
Agree with proposed definition	22	21.4
Disagree with proposed definition	70	68.0
Total:	**92**	**100.0**

Overview of Industry Responses

- Control room in a plant vs control center (or in a substation)
- "BES Asset" too vague
- Asset management includes commercial and market systems
- Change "of the" to "such as"
- "Capable of" is overreaching
- Change "alarm monitoring and processing" to "alarm processing"
- Define "BES Assets – or change to "BES Functions"
- Would include laptops and PDAs w/ SCADA client software – should only be fixed server locations and not remote clients
- Use actual configuration, not theoretical capability
- Define alarm to be "power system alarm", not fire alarm, etc
- Would bring into scope NERC RCIS, TLR, MISO outage scheduler, OATI, etc
- Data acquisition, aggregation, processing, etc too broad

1.g. – HIGH BES Impact Definition

1.g. High BES Impact — BES Subsystems have High BES Impact if, when destroyed, degraded or otherwise rendered unavailable:

- they could directly cause, contribute to, or create an unacceptable risk of-
  - BES instability; and/or
  - BES separation; and/or
  - a cascading sequence of failures.

  or
- in a planning time frame, they could, under emergency, abnormal, or restorative conditions, directly cause, contribute to, or create an unacceptable risk of-
  - instability; and/or
  - separation; and/or
  - a cascading sequence of failures;

or

- could hinder restoration to a normal condition.

Question 1.g. (94 Responses)

Option	Count	Percent
Agree with proposed definition	8	7.8
Disagree with proposed definition	86	83.5
Total:	**94**	**100.0**

Overview of Industry Responses

- 1st bullet – change to "that could directly and immediately cause"
- Add "unacceptable risk to IROL"
- Don't support 3 levels – add "no impact" – too complex or confusing
- Planning is not operations
- Does not match attachment 1
- Need to quantify "risk" – or remove "risk"
- Use "Adverse Reliability Impact"
- "prevent restoration" vs. "hinder restoration"
- Cranking path discussion
- Change "name plate rating" to MOD-024 requirements
- Don't need H / M / L definitions – use Attachment 1 instead
- "Unacceptable risk", "contribute to", "hinder", "planning timeframe" "degrade" is undefined
- Generation – use concept of capacity and time; differentiate base load units from peak units
- Not tied to mitigate vulnerabilities
- Restoration from blackout is not the same as causing / preventing blackout
- High impact Control Centers different than high impact transmission substations (transmission probably not high)
- Replace with "BES Impact" definition
- Use NERC event categories

1.h. Medium BES Impact Definition

1.h. Medium BES Impact — BES Subsystems have Medium BES Impact if, when destroyed, degraded or otherwise rendered unavailable, they could:

- directly affect the electrical state or the capability of the BES;
- directly affect the ability to effectively monitor and control the BES; or
- in a planning time frame, under emergency, abnormal, or restorative conditions,
  - directly affect the electrical state or the capability of the BES; or
  - directly affect the ability to effectively monitor and control the BES.

Question 1.h. (95 Responses)

Option	Count	Percent
Agree with proposed definition	11	10.7
Disagree with proposed definition	84	81.6
Total:	**95**	**100.0**

Overview of Industry Comments

- Refer to "High" definition comments
- Move 3 definitions to attachment 1 as a preface / corollary
- "affect the electrical state" too broad

1.i. Low BES Impact Definition

1.i. Low BES Impact — BES Subsystems have Low BES Impact if, when destroyed, degraded or otherwise rendered unavailable, they could not**:**

- directly cause, contribute to, or create an unacceptable risk of BES instability; or BES separation; or a cascading sequence of failures.
- hinder restoration to a normal condition.
- directly affect the electrical state or the capability of the BES;
- directly affect the ability to effectively monitor and control the BES;

Question 1.i. (98 Responses)

Option	Count	Percent
Agree with proposed definition	15	14.6
Disagree with proposed definition	83	80.6
Total:	**98**	**100.0**

Overview of Industry Comments

- Reference back to High / Medium comments
- Change to "no impact"
- Add "no impact"

2. Comment Form Question # 2- Purpose of CIP-002-4

2. The Purpose of draft CIP-002-4 states, "To identify and categorize the BES Cyber Systems that support the functions critical to the reliable operation of the Bulk Electric System (BES) as a basis for applying security controls commensurate with the potential impact those BES Cyber Systems have on the reliability of the BES." Do you agree that CIP-002-4 accomplishes this objective? If not, please explain why and provide specific suggestions for improvement.

Question 2 (96 Responses)

Option	Count	Percent

Agree	27	26.2
Disagree	69	67.0
Total:	**96**	**100.0**

Overview of Industry Responses

- Only address real time operations
- Does not consider level or risk, e.g., remote access
- Need to consider CIP-002 – CIP-009 together; need to see CIP-003 – CIP-009
- Network connectivity
- Need a "no impact" category
- Effective date of standard toed to other standards (CIP-003 – CIP-009)
- Still a one-size-fits-all for cyber systems (inheritance issue)

SDT Discussion of Purpose

- Idea between 2 (asset based) and 3 (security based) are approaches to consider as either/or choice

3. Comment Form Question # 3-- Method of Categorizing BES Cyber Systems

3. The proposed method of categorizing BES Cyber Systems is to categorize BES Subsystems based on the criteria in Attachment 1, then determining the BES Cyber Systems that have the potential to adversly impact the functions in Attachment 2 performed by those BES Subsystems. An alternative method could consist of inventorying all BES Cyber Systems that can affect the reliability functions in Attachment 2 and determining their impact on BES Subsystems using the criteria in Attachment 1. Do you prefer the method proposed in the standard? If not, please provide specific suggestions for a preferred alternative method.

Question 3 (82 Responses)

Option	Count	Percent
Prefer method proposed in the standard	46	44.7
Prefer alternative method of inventorying all BES Cyber Systems that can affect the reliability functions in Attachment 2 and determining their impact on BES Subsystems using the criteria in Attachment 1.	36	35.0
Total:	**82**	**100.0**

Overview of Industry Responses on Method of Categorizing BES Cyber Systems

- Need simplified criteria
- Flexibility to use either approach
- Must look at it both ways anyway for comprehensive approach
- Does not understand the question: standard does not say which way

- Use CIP-002-3 base, expand to BES assets instead of critical assets, apply R1.2 (list of asset types)
- "Cyber first approach" (using connectivity for categorizing): 8 entities support this approach.
- Need to know impact of CIP-003-009.
- "We believe that regardless of the method chosen, it will be so complex to implement that its costs will far outweigh its benefits."
- Hybrid approach: BES Engineering to filter out low impact subsystems and their BES cyber systems. For remainder, switch to cyber system approach and classify per "span of control" of BES assets.
- 2 dimensions of risk: BES subsystems and cyber systems (matrix approach)

SDT Discussion of Method of Categorizing BES Cyber Systems

- Not all the comments/responses are related to the question asked.
- Not intended to be a strict interpretation and not clear what is or is not captured in each – just a rough showing of confusion in the industry
- The question did not include "cyber first" as an option for consideration so we shouldn't give much weight to these industry preferences– again may just show there is no consensus for any one approach
- Merit to both approaches but each tackles a different aspect of what is needed – asset approach is appealing to get filter up front but may not capture all of the potential vulnerabilities – cyber first captures many of the vulnerabilities but without tying back to the assets.
- Hybrid approach – getting an inventory of every asset is immense and perhaps not necessary. The cyber impact was never intended to override the asset impact. If you have a high cyber impact but on a low impact asset, then it should still be a low category.
- Many utilities using CIP 002 to determine if they are meeting CIP 003-009 – Industry is worried about meeting CIP 002-4 process in terms of money and time only to find out they do not need to do much in CIP 003-009. We should provide entities an opportunity to understand up front as to whether they need to go through the whole process or not.
- Need to focus on the real attack vectors. For example, how many sites do we need to deal with because of routable protocols?
- **Combine Attachment #1 and #2.** Phil's proposed hybrid takes Attachment #1 and #2 and combines them to create a more bright line approach. The approach assumes it is criteria-based rather than the asset or cyber first approach – it also simplifies the current approach.
- The functions talk about what we are doing with the computers –may need to put this into the "disagreement" category because I am not sure I am comfortable yet with cutting out Attachment #2.
- Not sure there are not some unintended consequences with some of the terms used.

- This hybrid was intended as an example or starting point for further discussion and refinement.
- Still concerned about looking at cyber systems first before looking at assets. You would apply the same criteria. We need more detail added before adopting this as an alternative approach.
- This would simplify to a single requirement – makes audits simpler – impact based criteria – requirement is to list cyber systems that impact your high level assets (?)
- Inherited impact is addressed too
- Affects the risk rather than the impact
- Industry comments to the concept paper in the Fall were concerned with the complexity – so we removed the h/m/l of impact.
- Taking a leap that h/m/l of asset identification will identify the key cyber systems that need to protect the BES system.
- We cannot make the assumption but need to be careful in the scoping to mitigate the problem.
- Making the cyber system the subject of the sentence addresses the bulk of the comments from the industry – everything becomes high because of the physical asset – changing the subject here fixed that.

4. Comment Form Question # 4 Requirement-1 Responsible Entity Categorizes BES Subsystems

4. Requirement R1 of draft CIP-002-4 states "As a step in identifying appropriate security controls for its assets, each Responsible Entity shall categorize the BES Subsystems under its ownership by applying the criteria in *CIP-002-Attachment 1 – Criteria for BES Impact Categorization of BES Subsystems*.
1.1 The Responsible Entity shall update its categorized list of BES Subsystems, if applicable, as a result of the commissioning of any new BES Subsystem, decommissioning of any existing BES Subsystem or any other change in the electric system that coulsd affect the impact of BES Subsystems on the Bulk Electric System, within 30 calendar days of the completion of the change.
1.2 The Responsible Entity shall document any engineering evaluation or other assessment method(s) approved by its Reliability Coordinator or Reliability Assurer to support the categorization of BES Subsystems where required by Attachment 1."
Do you agree with this requirement? If not, please explain why and provide specific suggestions for improvement.

Option	Count	Percent
Agree	18	17.5
Disagree	75	72.8
Total:	**93**	**100.0**

5. Overview of Industry Responses to Requirement-1 Responsible Entity Categorizes BES Subsystems

- Need to know impact of CIP-003-009
- RCs should be removed from approval of engineering analyses
- Suggest Planning Coordinator for approval of engineering analyses
- Change within 30 days alternatives included: change to 30 days of being aware; change to 90 days; prefer annual reviews for changes; and any other change too broad: need better definition of this criteria
- Engineering analysis: need criteria for approval and consistency
- RCs and RAs should be required to publish approved engineering analyses
- General comments on vagueness of "subsystems"
- Blanket statement on engineering analysis (at front end of attachment 1)
- Subsystems it operates instead of owns. (joint ownership).
- Need explicit requirement for total list of subsystems.

SDT Discussion of Requirement #1- 1st Round

- Many people say they "disagree" even if they agree in order to get their comment read and considered
- **Owner/operator issue** – operating assets you don't own or own assets but don't operate them.
- Devices in the Texas interconnection system are owned by utilities by operated by regional entity
- The issue is who owns the cyber asset – they are responsible for the controls.
- Asset on site may be owned by the utility but operated by someone off site
- Need guidance from the NERC Compliance Group
- Add owner/operator issue to the agreement list for further discussion
- Even those who "agreed" often added suggestions for refinement or voiced concern
- Reviewed all the comments whether they "agreed" or "disagreed"
- **"Engineering assessment"?** How will we address those comments? Need a bright line approach.
- Draw bright lines but allow an option of an engineering assessment approach?
- FERC is not against exceptions, but must have appropriate controls and oversight of exceptions to ensure they are not misused.
- An engineering analysis could be used to either opt out as an exception or to opt in for units that are deemed to be critical.
- Need a way to allow an entity to declare something for a higher level protection without requiring a full analysis.
- What we are protecting against may need to be clarified for any review of the underlying analysis. Are we protecting against a single point or multiple point of attack?
- NERC was concerned with opt out, not with opt in

SDT Discussion, Requirement #1 - 2nd Round

- Needs more discussion – I think cyber approach takes more – I don't believe this discussion is worthwhile
- Is this a disagreement we need to reach a conclusion on now? Remove from list?

5. Comment Form Question # 5 -Requirement-2 Notification Proposal and Approach

5. Requirement R2 of draft CIP-002-4 states, "To support the proper categorization of BES Subsystems as identified in Requirement R1, and to ensure that Transmission Subsystem owners have accurate information concerning any directly interconnected Generation Subsystem for use in identifying appropriate security controls for their assets, each Responsible Entity that owns any Generation Subsystem categorized as High or Medium BES Impact shall, within 30 calendar days of developing or updating its BES impact categorization of that Generation Subsystem, provide the following information to those Transmission Subsystem owners directly interconnected to that Generation Subsystem:

2.1 Description of the Generation Subsystem that includes Facility designation(s), or name(s), location,
and other identifiers needed to identify the Facility(ies)

2.2 The Responsible Entity name

2.3 The BES impact categorization level"

Do you agree with this notification proposal and approach? If not, please explain why and provide specific suggestions for improvement.

Question 5 (86 Responses)

Option	Count	Percent
Agree	39	37.9
Disagree	47	45.6
Total:	**86**	**100.0**

Overview of Industry Responses- Requirement-2 Notification Proposal and Approach

- Define directly interconnected
- Change Transmission subsystem owners to transmission owners and operators
- Include method of notification and date of notification
- The same burden for information sharing should be placed on the Transmission Operators/Owners
- How does the GO/GOP know who his transmission owner/operator is? (He must connect to it?).
- Must be signed by Senior Manager
- Purpose of requirement not generally understood, must clarify and be more direct.
- Information protection issues

- Prefer annual requirement
- Address jointly owned facilities with different assessments (in attachment 1?)
- Several comments where allusions are made to the Transmission Subsystem owners categorize the Generation Subsystems.
- Modify CIP-002-3 approach
- RCs should categorize Generation subsystems – wide area view

SDT Discussion Requirement-2 Notification Proposal and Approach - 1st Round

- Annual requirement – if impact is changing frequently and have to continually reassess then put in the requirements – For audits do we have to determine or fix the point in time? Otherwise trying to do it in real time?
- Who doesn't know who their interconnect agreements are with? Have to have an interconnect agreement – how can you not know who the transmission owner/operator is?
- If you have joint ownership and they assess it at different levels, which applies? The higher assessment? Need to clarify

SDT Discussion of Requirement-2 Notification Proposal and Approach 2nd Round

- General agreement, but need to work on this as a team activity to see if it is possible. The language here is offered as an example.
- Adding "controlling/monitoring/alerting/protecting" is the key addition to the existing language
- "Unless it has been determined … {by} engineering evaluation…" are the opt out or weasel words that FERC is trying to get rid of – first part of the sentence is the bright line with the second part suggesting that you don't really have to meet the bright line. This paragraph is at cross purposes with itself.
- And RC/RAs don't want to do this.
- However there is no science behind the number offered here as the bright line.
- Alternative criteria for categorizing these?
- There should be no opt-out from a high but there could be an opt-up from medium or low approach – determined by an engineering assessment to be a high?
- May need to have a way to opt-down but not opt out .
- Assuming we are trying to drive issue to something the SDT can rank or shape for small groups to work with?
- I heard this as a suggested compromise approach to simplify R1 and R3.
- We cannot assure the bright line is correct and need to offer a way to address if it is not right for all entities in all situations.

- Change from "BES subsystems" to change the subject of the sentence to be "BES cyber subsystems."
- No bright line can cover all situations – must have an exceptions process available.

6. Comment Form Question # 6- Requirement-3 --Assigning Highest Impact Level of Associated BES Subsystems.

6. Requirement R3 of draft CIP-002-4 states, "As a step in assigning appropriate security controls for its assets, each Responsible Entity shall categorize and document BES Cyber Systems as follows:

3.1. Each Responsible Entity shall list each BES Cyber System associated with a BES Subsystem categorized in Requirement R1 that has the potential to adversely impact any of the functions identified in CIP-002 - Attachment 2 - Functions Critical to the Reliable Operation of the Bulk Electric System.

3.2. For each BES Cyber System the Responsible Entity shall assign the same BES impact to the BES Cyber System as is assigned to the associated BES Subsystem. Where a BES Cyber System is associated with more than one BES Subsystem and the BES Subsystems have different BES impacts, the responsible entity shall assign the BES impact of the BES Cyber System to be the highest BES impact categorization level assigned to the associated BES Subsystems."

Do you agree with this requirement of assigning the highest impact level of the associated BES Subsystems? If not, please explain why and provide specific suggestions for improvement.

Question 6 (90 Responses)

Option	Count	Percent
Agree	36	35.0
Disagree	54	52.4
Total:	**90**	**100.0**

Overview of Industry Responses Requirement-3 --Assigning Highest Impact Level of Associated BES Subsystems.

- Attachment 2 is overly broad in scope or worse, open-ended.
- Specifically, situational awareness can incorporate just about any cyber system. The SDT should review each Reliability Function to determine what is in/out of scope.
- The focus should be on real-time systems or those that can cause an Adverse Reliability Impact as a result of compromise (as opposed to those cyber systems that provide a maintenance, planning, or other non-essential function).
- The focus of Attachment 2 should NOT be on what can compromise these functions but the adverse impact if these functions are compromised (i.e. Attachment 1). Rename the attachment to "Activities Performed to Maintain the Reliable Operation of the BES."
- The size/rating of a "BES Subsystem" (whatever that is – say, for sake of discussion, a substation) has no logically valid correlation with the degree of potential severity of adverse impact on BES reliability resulting from compromise of its associated cyber assets. The impact of the Cyber System should be taken into account first. A system

may pose LOW impact to its associated BES Subsystem but HIGH impact to a control system on the basis of being connected using a routable protocol.

- Categorization should take into account both the functions and BES Subsystem impact to determine the true impact category (i.e. bring back the categorization lookup-table that combines BES Subsystem and BES Cyber System impact categories). BES Cyber Systems associated and having the potential to impact BES Subsystems could create a "race to the top" and make everything High impact. Not all associated Cyber Systems will have High impact. For example, the pH monitor or ambient air sensor for a Generation Control System should not inherit the same category as the Generation Subsystem. Other factors to consider include:
  - the role of the BES cyber system within the broader context of the operation of the BES subsystem (Is this the only mode of failure of the BES subsystem?);
  - the technical capabilities of the cyber system (Does it provide information sensing capability or interactive control?)
  - the nature of the network that the interconnected BES cyber system is using (IP or serial); and
  - the connectivity if any outside a BES sub-system (Is remote access allowed?); are examples of the factors to consider.
- Redundancy (often mandatory requirements in other reliability standards) should be considered as it may reduce the impact of an individual BES Cyber System component. Redundant systems with different architecture or modes may require a lesser degree of security controls due to an inherent robustness, determined through a vulnerability assessment. Master ends of BES Cyber Systems may be categorized higher than the individual remote ends of the BES Cyber Systems, but no higher than the associated BES Subsystem.
- The categorization should take risk into account instead of just impact. Many comments equated this to taking remote accessibility into account when assigning a category. Others cited non-routable protocols as part of the risk equation. Still others called for a broader risk assessment.
- It is sufficient that the BES systems are assessed to have an impact. The degree of an impact is superfluous.
- Categorization should be addressed as part of the Security Controls.
- Need some guidance on identifying Cyber System components.
- Only High and Medium impact Cyber Systems should be identified since Low impact Cyber Systems do not have impact to the reliability of the BES; or since BES Cyber Systems would default to Low, there is no reason to specifically categorize them as such.
- We believe an appropriate path forward is to focus Attachment 1 solely on High BES Impact items and create an Attachment 2 H/M/L categorization based on the cyber technology in use.
- It should be clear that an entity cannot be found in violation of R3 given an omission of BES Subsystems in R1.

- Recommend that additional asset categories be addressed as well (i.e.: PSP, ESP, non-critical cyber assets, access control, monitoring, etc.)
- Attachment 2 should be placed in a guidance document.
- Why move away from Critical/non-critical? If the Cyber Systems pose little risk to the BES, then why spend significant resources protecting them?
- Need a timeframe for adding Cyber Systems to the list after identifying or recategorizing BES Subsystems. The CEMP could require an immediate change to the BES Cyber System as listed.
- It is not clear how firewalls, routers, HVAC and other supporting systems would be classified.
- Remove the explanatory text at the beginning of Requirement 3. It does not add anything.
- There should be a 4th, *no impact*, category.
- In order to support compliance activities, add the following and update the Measures section appropriately: R3: add text to require that the documentation created when categorizing and subsequent documentation called for in R3.1 & R3.2 to be signed and dated (by proper personnel identified per CIP-003 / R2).

SDT Discussion of Requirement-3 --Assigning Highest Impact Level of Associated BES Subsystems- 1st Round

- Possibly grouping the controls for organizational (process and procedure issues) or better definition of the low level of controls
- Or are they included in the low impact level – trying to address concerns regarding the burden of inventory
- A category of 'no impact" and do I have to then have to have a spreadsheet that documents everything else? Concerned how auditors will treat such a category
- Low by definition could include the "no impact" assets – like having criteria that better defines the "low" category
- Auditors should focus on the high and medium categories – the low left to the entity to secure as they see fit

SDT Discussion- 2nd Round

- Is it the data/information sharing or the network? What is the scope of the comment?
- Revisit later – in the scheme of issues, it is not vital at this point
- It is a possible attack vector – if not included, then it becomes the attack vector

7. Comment Form Question # 7 Proposed Violation Risk Factors and Violation Severity Levels

7. Do you agree with the proposed Violation Risk Factors and Violation Severity Levels? If not, please provide suggested improvements on the proposed VRFs and VSLs.

Question 7 VRF (66 Responses)

Option	Count	Percent
Agree with VRFs	32	31.1
Disagree with VRFs	34	33.0
Total:	**66**	**100.0**

Question 7 VSL (68 Responses)

Option	Count	Percent
Agree with VSLs	20	19.4
Disagree with VSLs	48	46.6
Total:	**68**	**100.0**

Overview of Industry Responses on VSLs and VRFs

Broad VSL Responses

- Concerning VSLs, we recommend replacing zero-based quality prescriptions in the requirements, measures and violation severity levels with based performance targets that correspond to the vulnerability of concerted, well-planned attacks against multiple points. For example, requirements and measures should focus on performance objectives as follows: program implemented, program and security controls in place reviewed periodically (for example, every 12 months not to exceed 15 or every 90 days not to exceed 120) and correcting items found in the reviews timely (for example, within 30 days not to exceed 45). When an entity consistently performs, the security control objectives will be achieved. Violation severity levels should correspond, for example: severe-program not implemented, high-controls not implemented, moderate-reviews not completed, lower-corrections from reviews not completed. These should replace zero-defect quality prescriptions as perfection is not essential to achieving the objective of vastly reducing the risk of concerted, well-planned attacks against multiple points.
- We feel it is excessive for all three requirements to have a High Violation Risk Factor. This reflects a position that virtually all violations result in High classification determination which is not the case. Categorization of BES cyber systems and subsystems are an administrative process and do not present a high risk to the BES. Therefore it should have a low VRF; however, improper application of security controls might increase the risk to the BES.
- There needs to be VRFs for Transmission Operators and Reliability Coordinators not providing information to Generator Operators as required in Attachment 1 Sections 1.1, 1.2, 1.3, 1.4, 1.6 and 1.13.
- The requirements must be made much clearer in order to make the assessment of the appropriate level of VRFs.

- We suggest that the Violation Risk Factors and Violation Severity Levels in version 3 of CIP-002 be used as a pattern for version 4.
- Moving from a Moderate to a High to a Severe due to a set period of time passing (10 days) is not consistent with the current implementation of VSLs and VRFs. The penalty matrix already assesses fines based on VSL / VRF and time. It seems like a double penalty to receive an increased VSL due to time and to receive a higher penalty due to the length of time a violation existed.
- VSLs should be tied to the Measures, which are supposed to indicate whether or not the Requirements were sufficiently met. Various degrees of failing to "measure up" would equal the various severity levels. For example, what would be the VSL for a failure to have the evidence required for M1.2? That doesn't seem to be addressed here.
- Paradoxically, un-categorized BES subsystems or cyber systems must be categorized prior to VSL determination. Once they are categorized, the violation has been fully mitigated.
- Disagrees with the VSL level determinations due to the ambiguity associated with the high, medium and low categories.
- How will the number of "true" categorization or number of subsystems be determined as the basis of measuring what missed or mis-categorized? This severity level determination is far too reliant on an external judgment. The measurement needs to be absolute an unambiguous.
- Low impact BES subsystems have no effect on the BES and should not be in the violation security levels.
- Given the degree of subjective judgment that is involved with the categorization, it seems inappropriate to assess such a severe violation level for what could amount to a disagreement between the Entity and the Auditor on the Impact of a particular BES subsystem. Perhaps the VSL's should be based upon the completion or failure to complete a categorization exercise itself.
- The VSLs refer repeatedly to not categorizing a BES Subsystem of some impact level. Yet, without the categorization having taken place, how can the impact level have been determined? Also, the VSL refers to mis-categorized Subsystems. Who determines that the Subsystem was mis-categorized? Will the Regional Entities be performing their own independent categorization?
- Utilizing numeric values to change the VSL seems inappropriate when there may be wide variances in the quantity of BES Subsystems.

Specific VSL Responses

- R1 – Should be governed not only by the impact of the affected BES Subsystems, but also their number. VSLs for failure to update the BES Subsystem list should start at the Lower level, not the Moderate level. The numbers seem to be arbitrary and would have vastly different impacts on entities of different sizes.
- R1 – Moderate VSL should specify 31 to 60 days, and high VSL should specify 61 to 90 days, and Severe VSL should specify greater than 90 days to remain consistent with R2.
- R1 – Failure to update documentation should not carry the same weight as not categorizing any BES Subsystems.

- R1 - We suggest “One to three Medium Impact BES Subsystems have not been categorized or have been mis-categorized as Low Impact.” Then updating Moderate VSL to “Three or more Medium Impact BES Subsystems have not been categorized or have been mis-categorized as Low Impact.”
- R2 – make the timeframes consistent with the expectations in R1. 30-40, 41-50, 51-60. We require the Responsible Entity to update the list in these timeframes but do not require the Generator Subsystem owner to report the change in like timeframes
- R3 – the VSLs have gaps. For example in the Lower level, there is no violation if 1-4 BES Cyber Systems have not been categorized. There needs to be full coverage for all violations of the requirement to be consistent with NERC and FERC obligations. The other levels have similar issues. A remedy could be to assign impact levels based on the number of BES Cyber Systems not categorized (1 for Lower, 2 for Moderate, 3 for High, More than 3 for Severe)
- R3 (Moderate) – should reference BES Cyber Systems, not BES Subsystems.
- R3 – if a non-affiliated BES subsystem owner fails to correctly categorize its BES subsystem leading the Transmission Subsystem owner to assign too low a categorization to its cyber systems, then it may lead the Transmission Subsystem owner to incorrectly categorize its associated cyber system. Assigning a severe VSL to the Transmission Subsystem owner under these circumstances is inequitable.
- R3 – Moderate VSL: Add “Cyber” after “BES.” Per the current R3 VSLs miscategorizing 1 or 2 Medium Impact BES Cyber Subsystems will NOT result in a violation. The suggested change to R3, Lower VSL above will solve this issue. Severe VSL: The last sentence states “The Responsible Entity does not have a list of ALL its BES Cyber Systems.” Technically this means if the entity misses listing even one of its Low Impact BES Cyber Systems they would have committed a severe violation. Suggest changing “all” to “any.”
- The Violation Severity Levels appear inconsistent by equating a missed deadline for updating the categorized BES Subsystem list, with not categorizing any BES Subsystems under the Severe Violation Severity Level. All the deadlines for the VSLs should be 30 days, with differences based on impact level categorization. R1 Lower VSL should include “The Responsible Entity has failed to update its categorized list of Low BES Impact BES Subsystems in accordance with Requirement R1, Part 1.1 for more than 30 days of the completion of the change.” The time component of the Moderate VSL should be changed to “The Responsible Entity has failed to update its categorized list of Medium BES Impact BES Subsystems in accordance with Requirement R1, Part 1.1 for more than 30 days of the completion of the change.” The time component of the High VSL should be changed to “The Responsible Entity has failed to update its categorized list of High BES Impact BES Subsystems in accordance with Requirement R1, Part 1.1 for more than 30 days of the completion of the change.” The time component of the R1 Severe VSL should be removed.
- The quantity thresholds used in the Violation Severity Level table should be a a weighted score of an entity’s subsystems, where multiple Low BES Impact Subsystems

or BES Cyber Systems are considered equivalent to single High Impact BES Subsystem or BES Cyber System, respectively.

SDT Discussion VSLs and VRFs

- Comment suggesting a different path for VSLs?
- EEI representative clarified concern – the bar should be a little higher and performance based.
- Add a more succinct version of the comment to the list.
- Consciously chose not to penalize entity for one-time violation of requirements in drafting the VSLs.
- True for medium but not high which is seen as severe.
- May push entities to high to address audits?
- Revisit the low level of VSLs with regard to zero based quality instead of zero based defect (see, EEI comment)
- Absolute perfection is the low bar –that is how the compliance system works – 99 out of 100 still fails

8. Question # 8 Attachment 1 Proposed Criteria-High, Medium, Low BES Impact Categories

8. Attachment 1 to draft CIP-002-4 contains criteria for High, Medium, and Low BES Impact categories developed in collaboration with representatives of the NERC Operating and Planning Committees. Do you have any suggestions that would improve the proposed criteria? Suggestions for improving proposed criteria:

Overview of Industry Responses- Proposed Criteria-High, Medium, Low BES Impact Categories

- What is the basis for the bright line criteria (e.g. 2000 MVA/1000 MVA)?
- Must run: that have wide area impact
- Definition of Medium Impact is too vague
- More precise terms
- Criteria for the classification of Facilities for High, Medium or Low BES Impact should be based on the risk (probability and consequence) of one or more events that may cause an Adverse Reliability Impact, such as an event that may cause an IROL to be exceeded or cause a supply / demand mismatch greater than a certain metric such as the Contingency Reserves of a reserve sharing group (or another metric determined by study in the region).
- Bright line thresholds (such as 2000 MVA or 2000 MW) are useful default values that should be used in the absence of a particular BES design value used in a region for planning studies and real-time operations.

- The entire Attachment 1 can be boiled down to two metrics: supply / demand mismatch and IROLs.
- The categorization of black start units and transmission cranking paths between the black start units and the units to be started should be those identified under EOP-005-2 and based on approved region-wide restoration plans developed under EOP-006-2. As discussed earlier, "High Impact" from a restoration perspective should focus on preventing restoration efforts and "Medium Impact" should focus on hindering restoration in accordance with the regional plan. Hence, High Impact should be for a Cyber System that, maliciously used, could prevent black start efforts from multiple black start units and their cranking paths in the regional plan. Medium Impact should be for Cyber System that, maliciously used, could hinder black start efforts from a single black start unit or cranking path in the regional plan. Black start capable units that are not in the regional plan should be Low Impact.
- Reliability standards should be based on net demonstrated capability testing results as determined by the requirements specified in MOD-024-1. (Generation?)
- Request clarification on the wording "leaving" in 1.5. Alternatively, suggest 1.5 be made to read: Each Transmission Subsystem that contains switching stations operated at 300 kV or higher in the Eastern and Western Interconnections, 550 kV or higher for the Quebec Interconnection, or operated at 200 KV or higher in other Interconnections, with 3 or more transmission lines connected to the station…
- Restoration paths and UFLS: distribution facilities in scope?
- Request clarification on 2.5, which SPS 300 kV threshold, sensing, action or both?
- Remove Engineering Analyses.
- Blanket Engineering analysis opt-out in Attachment 1
- Exceeding an IROL does not cause instability if recovered within the timeframe allowed by the current standards requirements, and therefore should not be a H or M criterion

SDT Discussion = Round 1 Proposed Criteria-High, Medium, Low BES Impact Categories

- Role of transmission planning – industry wants it in and NERC is saying do not put it in
- Should we have engineering assessment opt outs?
- As applied to attachment one, struggled with the target number – agree we need to put it in even in the face of the directions from NERC
- Need to have it in there – up to the team, not NERC
- Seems clear to me that NERC does not expect to allow opt outs
- Moving to bright line gives a different framework than Commission considered when giving us guidance
- If there are exceptions to the requirements then need to be sure there is an accountability process
- May need an external party to review whether or not the rationale for the exception is appropriate

- Engineering assessment needs oversight – question would be who is willing to accept the responsibility?
- Still waiting for RAs to be designated – needs to be some entity to perform independent evaluations – may need to hold harmless from liability
- RAs are a renaming of RROs – version 4 document was approved a year ago December but the document was never brought to the Trustees for approval – version 5 is now on track to go before the Trustees – thus RA still not an official or legal standing and so no one has signed up yet
- 706 gives same protection that is granted to NERC –
- this is for telling you what assets need to be under the standards – can't just mark everything as high without documentation
- Should be discussing the validity of engineering assessments rather than who should do it – should we allow and if so, then discuss who and how
- We disagreed with having the engineering assessment as adding a layer of complexity – we are comfortable with the process we already have
- Opt out option seems to be contrary to the grouping of assets into the h/m/l buckets without adding value – create bright lines, but they don't really matter
- If we do not allow then saying bright line is absolutely correct for every entity across the country – irresponsible not to include
- The requirement is for "impact analysis" – throwing a number out there is not a true impact analysis – without exception then consider changing to "wild guess analysis"
- There is no right answer as to where to put the stake for analysis – what are we protecting against?
- Need to lock in what criteria will be used by a third party – not looking to except specific assets
- Have to have someway, with rules around it, to address changes – you can choose the bright line or if you choose an alternative then show us why and how
- Engineering analysis is use in two ways in the requirement
- Do we need a study to help set the criteria for the bright line?
- Can't possibly study all the possible situations across the country – put the burden on the entity seeking the exception to prove it is entitled
- NERC has bright lines in other standards without definitive analysis
- Who is the right organization to further study the issue?
- Leaving unspecified in the standard leaves it open to allowing anyone to do that – need to designate

SDT Discussion Round #2- Proposed Criteria-High, Medium, Low BES Impact Categories

- Added to the list for further discussion

9. Comment Form Question # 9 Attachment 1 High, Medium, Low BES Impact Categories for Load-Serving Entities, Transmission Providers and Interchange Coordinators.

9. Do you have suggested criteria for high, medium, or low impact categories for Load-Serving Entities, Transmission Service Providers, and Interchange Coordinators?

- Suggested Criteria for Load Serving Entities:
- Suggested Criteria for Transmission Service Providers:
- Suggested Criteria for Interchange Coordinators:

Overview of Industry Comments- Attachment 1 High, Medium, Low BES Impact Categories for Load-Serving Entities, Transmission Providers and Interchange Coordinators.

- The vast majority of responders had no suggested criteria for these entities.
- In fact, most felt that these entities should not be included as responsible entities in this standard.
- Those that felt that they should be included added that it depended on whether they had BES Cyber Systems.
- Some expressed that the systems were covered under other REs (Distribution Providers, TOPs, BAs)

SDT Discussion – Round #1 Attachment 1 High, Medium, Low BES Impact Categories for Load-Serving Entities, Transmission Providers and Interchange Coordinators.

- Does the definition even apply to the commenter?
- Possibly – may need to modify the language to clarify who it applies to.
- Demonstrates the folly of this approach – all of us are interconnected through the NERC net.
- Proper controls deal with that issue.
- DOD cannot fully protect its system, how can we?
- If we can't think of an instance where an entity should be included then it probably shouldn't be
- Review the registration criteria for including LSEs, TSPs and ICs under the CIP standards (if any)? If no criteria, then remove.

10. Comment Form Question # 10 Attachment 1 Proposed Criteria-High, Medium, Low BES Impact Categories for NERC and Regional Entities

10. Do you have suggested criteria for high, medium, or low impact categories for NERC and Regional Entities?

- Suggested criteria for NERC and Regional Entities:

Overview of Industry Responses Attachment 1 Proposed Criteria-High, Medium, Low BES Impact Categories for NERC and Regional Entities

- The only responders that felt these entities should be included said that NERC Net was probably the only concern.
- Several felt that even NERC Net would not affect the BES.

SDT Discussion Round #1 Attachment 1 Proposed Criteria-High, Medium, Low BES Impact Categories for NERC and Regional Entities

- NERC Net could be an Achilles heel if not properly protected
- We can't protect against the whole world – then every cell phone is an attack vector.
- The requirements around NERC and the regional entities are more stringent than the standards – and a better venue for addressing the information security issue – different audit regime by an outside third party entity
- NERC and regional entities were included in the CIP 002-4 draft – should they be? If you can create criteria, then yes. If cannot create criteria, then no.
- NERC alerts could affect the BES.

11. Comment Form Question # 11 Functional Entities- Distribution Provider and Reliability Assurer.

11. The SDT is considering including Distribution Provider and Reliability Assurer in the list of applicable Functional Entities. Do you have any comments regarding whether or not the CIP-002-4 Standard should apply to these Functional Entities?
    - Comments on adding Distribution Provider:
    - Comments on adding Reliability Assurer:

Overview of Industry Responses- Functional Entities- Distribution Provider and Reliability Assurer.

- Most responders felt that the Reliability Assurer could be excluded (pointing to the fact that the RA is not included in the NERC Glossary, and confusion over how compliance for NERC and Regional Entities could be measured).
- Results for the DP were mixed. Some felt that the DP could be excluded, since they did not involve facilities >= 100kV.
- Some felt that the DP should be substituted for the LSE.
- Some were unsure how load shedding and Smart Grid would affect this standard.
- Some were very opposed, feeling this opened distribution up to FERC regulation.

SDT Discussion Points Functional Entities- Distribution Provider and Reliability Assurer

- RA could be excluded – what BES can they be connected to?
- Careful about distribution provider based on registration criteria – includes the wires company, most of whom are not registered – be cognizant of what the registration criteria calls for and who is actually registered

- Term bulk power system – reviewed language – does not include local distribution of electricity
- Under frequency load shedding – applicability – may need a long list of applicability to be sure capture entities we want to see in and not those we do not
- Do RAs have cyber systems that should fall under this standard?
- Frequency load shedding is a design standard, not a performance standard

12. Comment Form Question # 12 Attachment 2 Functions Critical to Reliable Operation of BES

12. Attachment 2 to draft CIP-002-4 contains functions critical to the reliable operation of the Bulk Electric System that serve as a basis for categorization criteria and the definition of BES Cyber Systems. Do you have any suggestions that would improve the proposed functions?

- Suggestions for improving proposed functions:

Overview of Industry Comments Functional Entities- Distribution Provider and Reliability Assurer.

Broad Comments- Attachment #2

- The focus for these proposed functions should be cyber systems that support real-time operations.
- How are Attachment 2 functions different than the functional model? The standard already covers the assignment of applicability to functional entities and restating the tasks performed by the functional entities seems redundant.
- Does not indicate the varying levels of impact for the defined functions. This is a one-size-fits-all model for Cyber Systems associated with BES Subsystems.
- Attachment 2 is not careful as to whether it applies only to BES Elements. If it is taken to apply to any Element then it becomes a definition of the BES Subsystem.
- Make the list complete. The “include, but are not limited to” open ended function list leaves too much room for disagreement. Clearly identify if for each function if you need all of the elements below it or just one, to be considered having that function. For example if all you have is power system stabilizers, do you have the Dynamic Response function?
- Attachment 2 only adds confusion and should be eliminated.
- Attachment 2 supports the identification of cyber systems that support critical BES functions but seems to suggest by the title of the attachment that all functions being critical are also high impact and therefore does not assist with the categorization of assets that could potentially be medium or low impact.
- There are several places where the proposed standard could have unintended consequences with negative effects on reliability. For example, the requirement that all blackstart units registered as part of the regional reliability plan be classified as high-risk could lead to Entities reducing the number of declared black start units; an exemption based on an approved engineering study should be allowed.

- It is not clear how the list in attachment 2 was created. Consider leveraging other NERC documents such as the Functional Model or the Definition of Adequate Level of Reliability.
- This standard needs to be segmented into each applicable function and not try to use a "one size fits all" approach. If this path is taken, subject matter experts can help to better define what cyber systems should be in scope and out of scope on a very specific basis. This will eliminate much of the lack of clarity and misinterpretations of the present draft standard. It will also bring the focus back to protecting the highest risk elements with the highest level of protection and not try to do this for everything.
- Attachment 2 makes no allowance for system diversity and redundancy.
- The functions should be specifically covered in Attachment 1 under the impact categories they fit.
- Proposed attachment 2 looks comprehensive and well thought out.
- Replace "Functions Critical to the Reliable Operation" with "Functions that Affect the Reliability of the Operation". This attachment describes functions that may affect BES operation reliability, but the level of impact can range from no impact for some circumstances to critical for some possible circumstances.
- Please provide the basis for including each of the functions.
- There is concern with creating a definition and then supplementing the definition with an Attachment providing additional criteria and clarification of a term, as addressed with the High BES Impact comments. If a person were to just look in the NERC glossary then they would have no idea there were additional criteria defining a BES Cyber System. If an appendix or attachment is necessary, the definition should clearly reference the additional information.
- Clarify functions that are critical to reliable operation of interconnected BES, not isolated BES Subsystems.
- If you identify a control center in attachment 2 then this is not needed. Look at comment for clarity.
- Attachment 2 has potential for wider application and does not belong in a CIP standard.
- Failure or compromise of some cyber systems may not impact the operation of the subsystem for a significant length of time, allowing for repair. These systems should be excluded from the standard. For example, a PC based coal receiving unloading system. The fuel inventory on-site will supply the plant for a number of days, weeks or months depending upon the amount in inventory." No reliability improvement would be gained from applying cyber controls to this system.
- Request a FAQ/Guideline. Recommend moving the examples in Attachment 2 into the FAQ/Guideline

Specific Responses for Attachment #2

- Tools that are used in the planning horizon are not critical to BES reliability and should be removed from the proposed functions. (e.g. Unit Commitment under Balancing Load and Generation.)
- Consider combining 2, Balancing Load and Generation and 3, Controlling Frequency into one category.

- As a suggestion for consistency and to take advantage of the thoroughness of the info in the Concept Paper, why not use the nine functions identified in Figure 1 and Table 1 which include: 1) Contingency Reserve/Peakers; 2) Load Balancing, Frequency Response/Support; 3) Voltage Support/Reactive Power Supply; 4) Constraint Management; 5) Control and Operation; 6) Situation Awareness; 7) Restoration; 8) System Stability; 9) Load Management?
- We recommend reviewing for inclusion the following critical functions:
  1. Emission systems (with indirect impacts)
  2. Remote Cyber Support
- Recommend changing from "The Situational Awareness function includes activities, actions and conditions necessary to assess the current condition of the BES and anticipate effects of planned and unplanned changes in conditions." to "The Situational Awareness function includes activities, actions and conditions necessary to monitor and make real-time operational decisions regarding the reliability and operability of the BES."
- Attachment 2 lists monitoring of spinning reserves which requires telemetry from every generating unit. This implies that every generating unit, regardless of size, falls under this standard. This would also seem to include each RTU and all the communication equipment back to the EMS. We have the same concern regarding calculation of ACE. This implies that all communication equipment back from the RTU for every input into the ACE equation.
- Definitions need to be clarified (e.g.):
  - "Governor Response" - is this movement of a governor to respond to frequency deviation?
  - "Providing Actual Reserves" - Are these systems that request additional generation in response to an event?
- 1. Dynamic Response – Disagrees with the inclusion of Spinning Reserve and Governor Response as neither of these is dependent upon a cyber system.
- 1. Dynamic Response – Spinning Reserve is listed which by itself is not an automatically triggered and not a Dynamic Response quantity. Units, or capacity so designated, is controlled by AGC. Governor Response should specifically mention AGC. Unless its control is addressable, Governor Frequency response should not be included as a part of the Cyber standard. Excitation Systems with Automatic Voltage Regulators are not listed and should be.
- 1. Dynamic Response – Under and Over Frequency Relay, Under and Over Voltage Relays are covered under Protection Systems. To call them out separately implies otherwise.
- 1. Dynamic Response - Generator governor controls may be purely mechanical or local electronic controls without connections to remotely accessible systems.
- 1. Dynamic Response – Is the bullet under number 1 that deals with under and over frequency relay protection intended for all entities that participate in under or over frequency load shedding or just the bigger entities as stated in Attachment 1 section 1.14? We feel that applicability needs to be clarified throughout the standard to ensure that it's interpreted correctly. If under or over frequency load shedding are considered critical to the

reliability of the BES, it should be clearly defined in the criteria for the impact categories of Attachment 1 what levels of load shedding fit each category like 1.14 of Attachment 1.

- 2. Balancing Load and Generation - This section should be clarified to address the balancing of electrical system load vs. electrical system "supply". It could be interpreted to apply to the pure generation unit control aspect.
- 2. Balancing Load and Generation – Disagrees that any of the listed activities is solely dependent upon a cyber system. These functions can be performed without employing a cyber system. The listed activities should only be included if they are solely dependent on computer systems, intranet or internet to allow access to multiple parties.
- 2. Balancing Load and Generation – Is "Manually Initiated Load shedding" the area of interest or the ability to identify. If "identify" this is under the scope of Situational Awareness in Item 8.
- 2. Balancing Load and Generation – These functions may be outside the Control Center. It is not clear if the intent would be to expand scope beyond the control center.
- 3. Restoration of BES – Disagrees with including this function, as most restoration plans assume the transmission operator's system has suffered a total blackout. It is extremely doubtful in this case that any cyber systems will be used, because each step of the process will have to be manually tracked. Inclusion should be determined on a case-by-case basis based upon the specific restoration plan.
- 4. Controlling Voltage – This Controlling Voltage section does not list "Transmit adjustments to individual units" (in response to a voltage schedule).
- 5. Managing Constraints – The drafting team should clarify item 5 "Managing Constraints" of Attachment 2. Could this include cyber assets used in the calculation of ATC? Tagging systems used to submit schedules?
- 5. Managing Constraints – Is the intent to pull systems such as Oasis and OATT into scope under managing constraints?
- 6. Control & Operation – Please clarify "control".
- 6. Control & Operation – Recommend adding parameterization, calibration.
- 6. Control & Operation – AGC should not be listed in the Controlling Frequency section as it is a Dynamic Response.
- 6. Control & Operation – The Control & Operation section needs to include Generator controls for AVR, and AGC.
- 6. Control & Operation – suggests the example should include "electronic" control rather than "all" control.
- 7. Restoration of BES – Cranking Path should be clearly defined for application in this Standard.
- 8. Situational Awareness – The Situational Awareness section is covered by the other sections and is not needed.
- 8. Situational Awareness - A definition or the intent of "Change management" should be included. Is this the management of change as cover in other sister standards?
- 8. Situational Awareness is too broad and needs to be better defined. In particular, the "change management" aspect of Situational Awareness is unclear.

- 8. Situational Awareness, bullet 5 – Frequency monitoring should be better defined so that the loss of a single monitoring point in a many point scheme is not a problem.
- 8 - Situational Awareness, suggest these words should be consistent with the real-time operations words for situational awareness in the Control Center definition. Recommend changing to: "The Situational Awareness function includes activities, actions and conditions necessary to monitor and make real-time operational decisions regarding the reliability and operability of the BES."
- 8. Situational Awareness: It is unclear whether Change Management applies to IT Systems or change management as it relates to other work being performed on BES subsystems, for example repairs during a unit outage, or replacement of substation equipment.
- 8 – Situational Awareness. What is the team attempting to identify with Change management, and Current Day and Next Day planning? They both could be interpreted to mean outage scheduling applications.
- 9. Recommend changing 9- Inter-Entity Coordination and Communication from "The Inter-Entity coordination and communication function includes activities, actions and conditions necessary for the coordination and communication between Responsible Entities to ensure the reliability and operability of the BES." to "only inter-utility data communications". Existing language would include voice communications.

Question 12: comments already discussed under other questions

- No additional comments offered by the SDT members

13. Comment Form Question # 13 Other Comments

13. Do you have any other comments to improve the draft standard?

Overview of Industry Responses

- Most Other Comments were already provided in response to earlier questions:

B. SDT Points of Agreement and Disagreement for Refining CIP-002-4

CSO 706 SDT Points of Agreement, Disagreement and Confusion in Terms of CIP 002-4

SDT Points of Agreement *regarding Industry Comments on CIP 002-4*	**SDT Points of Disagreement** *regarding Industry Comments on CIP 002-4*	**Industry Points of Confusion** *regarding CIP 002-4*
1. Flexibility is needed but may or may not be included in today's language	1. What is the CIP standard trying to protect against?	1. Do you start with R1 and work through R3 or is there more flexibility possible in CIP 002-4?
2. Functions of BES need to be considered, but may not be clear in today's standard language	2. Should it be connectivity vs. impact assessment	
3.Agree some form of inventory will be needed regardless of approach	3. We disagree on how extensive the inventory will be for each approach	
4. Any approach needs to result in a categorized list of cyber systems.		
5. We are addressing the range of cyber systems at play in the real time control and operation of the BES reliability	4. The Cyber system should inherit the category of the BES asset (indirect impact mapping) vs. basing it on an assessment of the external and internal threats (direct impact mapping)	
6. Bright lines will help to simplify the implementation and compliance with the standards	There should be flexibility and third party oversight.	
7. Where ever possible, the SDT should seek to combine steps and simplify the approach	5. Categorization should be based on threat/ reach/ connectivity	
8. We function in a compliance vs. a performance assurance framework.	If we are using a compliance framework we should stick with a CIP 003-009 structure.	
9. The standard should be designed so those implementing it know why they are protecting assets and systems.		
10.We are designing a compliance not a performance assurance framework"		

SDT Member Comments on Points of Agreement/Disagreement

- Is #8 a point of agreement or a desired outcome? We don't have a choice to ignore compliance.
- This is a point of agreement – to clarify, change to "we are designing a compliance not a performance assurance framework"
- Agree some form of inventory will be needed – disagree how extensive the inventory for each approach

- Are we not going to have third party oversight? Don't we have to have it to allow industry the flexibility they are requesting? Need that up there under points of agreement or disagreement
- #2 under disagreements should be deleted – redundant with #5
- Is it not best to stick with a 3-9 structure if we are using a compliance framework
- a disagreement - clarity in practice as to what a BES system is –
- #4 – change to inventory of BES cyber systems
- #1 and 4 – redundant? Get rid of #1 or #4? Strike #4
- #5 limits on scope or range of cyber systems? Yes
- #18 – revisit the severe VSLs? Change to "revisit the VSLs"
- #12 – need better definition – don't agree to remove it – okay can remove it if we cannot get a better definition – it is a task rather than agree/disagree
- #2 – overall flexibility or flexibility in approach? Flexibility in starting with R1 or R3

C. Review of Alternative Approaches to CIP 002-4

1. Categorization of BES Cyber Systems Based on Use of Routable Protocols

Dave Norton had circulated in advance of the meeting a proposal which suggested the categorization of BES cyber systems should be primarily based on use of routable protocols (threat/reach/connectivity?). The following proposal was presented for the Team's consideration:

Proposal: Categorizations of BES Cyber systems based on the potential impact of their compromise through the use of routable protocols as attack vectors.

- **Control center routable protocol = high**
- **Generation plant/transmission substation = medium**
- **All else = low**

SDT Member Comments before ranking the Proposal

- Categorization based solely on that, primarily on that, etc.?
- Categorization based on risk presented by external attack surface
- This is a test of whether categorization is based on routable protocols
- There is a baseline of things we have to do – some with more than others (medium/high)- routable protocols and intuitive obviousness
- Can live with doing an impact assessment with a second level based on connectivity – two level of assessments based on routable and non-routable
- Bright line is routable protocols – the attack surface – the impacts are variable
- Are we back to function?
- Concerned that equal focus on connectivity adds complications from a generation aspect – look at BES impact first and then connectivity

- Proposal is to scope it with primary focus on routable protocols
- How do we capture measurable criteria?
- Low is everything BES cyber – what makes it go to medium or high?
- Direct or indirect impact?
- Is this a complete substitute? Not a "primarily"? Yes
- Different definitions of "control centers"
- The three bullets are examples to illustrate the proposal

Acceptability Ranking Scale	***4** = acceptable, I agree*	***3** = acceptable, I agree with minor reservations*	***2** = not acceptable unless major reservations addressed*	***1** = not acceptable*	***AVG.***
	6	**4**	**9**	**2**	**1.5 of 4**

Comments after Ranking

- Clarification – were the bulleted items included? Yes. I don't agree with the examples
- But the examples tell me what it means.
- Can we test the current language for level of support? Or #2?
- The cyber system should inherit the category of the BES asset (indirect impact mapping)
- But this is a piece of R1 & 3 – this replaces only part of R1 and R3
- We tested the new proposal that came in after we tested the original proposal.
- We need to resolve this issue so we can move forward.
- #1 Ranking – flies in the face of what we have done up to this point of not looking at attack vectors until we addressed them in the controls
- #1 Ranking – basing the risk on the network – not a complete cyber security approach
- #2 Ranking because of the routable protocol emphasis – preferred broader view of original
- Need to make significant changes to current draft to address the comments from the industry
- Would move my #2 to a #3 if we removed the examples.
- Not an either/or decision – routable protocol may not be easy to define for many and serial is not protected from attack –
- Raises the technology up to the BES impact –
- It tells us where to put it in the controls and do not have to inventory all of your big iron – zero in on IP for more controls – two levels of rigor
- #2 Ranking – routable protocol and attack surface may be a red herring – agree with concept but need an alternative – talking about a security of connectivity – intent is connectivity but routable protocols will not get us there
- We need a categorization method to start with – then work on the controls – a categorization method we can put controls onto
- Need a modifier – the inheritance as a base with connectivity (or lack of) as a modifier to bring it off of high.
- Don't see how you can let go of the BES asset.

2. Jay Cribb Proposal- Combining Cyber System Impact on BES with Connectivity

Jay Cribb presented his proposal in which he tried to combine both the cyber system impact on BES and connectivity as shown below.

Cyber System Impact on BES →	high	medium	low
Connectivity ↓			
Routable	high		
Non-Routable	high		
Stand Alone	medium		

The SDT ranked this proposal as follows:

Acceptability Ranking Scale	***4** = acceptable, I agree*	***3** = acceptable, I agree with minor reservations*	***2** = not acceptable unless major reservations addressed*	***1** = not acceptable*	***AVG.***
	4	**13**	**3**	**0**	**3.05 of 4**

- Looking for clarifications in a sloppy system
- The SDT needs to be on board with basic concepts – we are shoehorning everything into h/m/l – may need to reconsider
- Looking at concepts at different levels and trying to merge them together.
- Are these the only criteria?
- We should remove the e.g.
- I voted on this as a model not as criteria.
- Need to review more of the Industry responses – not sure we can ever be clear as to what is medium.
- Not looking at h/m/l requirements – these are impact levels.
- FERC asked us to look at it – and it doesn't work.
- I think it does work – still works if we do not have a moderate level and we only have a high/low assessment

- Chair John Lim asked Jay Cribb, Scott Rosenberger and Dave Norton to discuss this proposal in the evening over beer and invited other members to join and bring back a revised proposal based on Tuesday's discussion.

3. Revised Hybrid Approach

Stu Langton reviewed with the Team where we are, the request to a group to work on and bring back a proposal to the full group this morning, the difficult nature and complexity of the task at hand – we will continue to have disagreements but have met our previous deadlines and will continue to work to meet the upcoming deadlines – remind members that consensus doesn't mean we have to all agree and that we cannot disagree sometime – differences are okay – if

75% want to move on, then we will – we need the minority to hang in there and keep working with us.

Scott Rosenberg presented the revised proposal and spoke about risks presented by connectivity and the challenges in defining terms accurately. The BES impact will still be h/m/l, but the proposal introduces the connectivity risk of routable versus non-routable. The matrix similar to one used before. May look like a high, high-medium, medium, medium-low and low. They were trying to avoid incredibly detailed inventories. You would like to be able to split a system into high or medium, slice and dice as needed to limit having to treat everything high – down to bus or breaker level. If we do our perimeters right, we can limit the columns for audits. We need a formula or guidelines the auditors can work with. This proposal reconciles the good work done so far on BES side and on the cyber side. Looking to see if the SDT thinks this process is agreeable and then would look at analysis.

SDT Comments

- Absent an inventory how can you say you identified everything that needs a control and if the control is adequate?
- Maybe we need to identify capacity as the starting point.
- Need to avoid mis-categorizing or not capturing
- Not taking away categorization process we already developed but we do need to refine – comments to indicate the process is not clear – on top of that, if you identify the right assets, then you prioritize and refine categorization based on connectivity. If we do it right we will protect the right assets and not over protect the wrong assets. Join the approaches together but recognize this need more refinement to clarify issues.
- BES requirement was seen as site specific – follow up with cyber system inventory and then based on connectivity determine its impact.
- This attempts to allow you to justify not having to put too much protection on assets that are not interconnected.
- Once you figure out what is protected, you then look to develop protection controls.
- Sounds like current 002 for establishing the inventory with a new layer of prioritization.
- Need to nail this down so the small groups work from the same framework.
- Connectivity? Three categories: connected to routable network (clearly in), relay with Ethernet and substation network but no wire connecting it to the switch capable of being routable (in or out?) Need to discuss further what connectivity means. Third – not connected at any point.
- Now have direct mapping of BES assets to cyber systems
- System idea – matrix for categorizing your cyber systems
- Something connected serially to a routable box? That would be connected
- If I plug my pc in through another serial connection is it connected? Maybe not.
- Is it assets or system based? Categorize the BES asset systems – think in terms of running systems through a litmus test. Can you control it or not.
- Concern is about hitting multiple sites in order to impact the grid.

- Some divergence in the sub group on this issue – control systems versus ability to control a system – needs further refinement and discussion.
- Whether rout-ability or controls needs discussion once we agree to go with proposed connectivity approach – lets not get hung up on the criteria at this point.
- Where do we spend our money to protect the system.
- How did you determine what is scoped into a system? Assessing impact level of BES asset based on its connectivity – how do you determine its level of connectivity if it has multiple connectivity methods?
- Do we need to skinny down attachment 2?
- Problem with "system" – what do you call a system? Where do you draw the boundary? Need to define better, then connectivity between sites establishes the level.
- Type of connectivity matters – category of controls you apply depends on the type of connectivity.
- Need to better define system in CIP 002 so we know we can break it up as needed.
- The details we will have work through together as a team.
- Definition in form 417 – any need to consider as part of teamwork?
- Need to see both proposals to get the full picture (second proposal from Phil to combine R1 & 2)
- Still need to address controls, what is relevant to real time control – and need to address complex issue of "connectivity"

"Include connectivity as a factor in the BES Cyber System categorization"
Revised Proposal: Matrix for Levels of Controls to Be Applied

BES (attachment #1 of CIP 002-4)	High	Med.	Low
Connectivity-Routable/Dial-up	High	High	Med.
Non-Routable	Med.	Low	Low
Not Connected	Low	Low	Low

Acceptability Ranking Scale	***4** = acceptable, I agree*	***3** = acceptable, I agree with minor reservations*	***2** = not acceptable unless major reservations addressed*	***1** = not acceptable*	***AVG.***
	12	**4**	**2**	**0**	**3.6 of 4**

Comments After Ranking

- 2 = I do not see the difference with what we put out to the industry –
- It is modified by connectivity
- 2= don't like doing the BES asset assessment first
- still need to figure out what functions are in the attachment – scope it out some more
- must address Bulk power as the first step for industry support and this let's us do that
- small group will meet this evening to review and fill in the concept with text to help clarify concept – John Lim, Phil Huff, Rich Kinas, Jay Cribb – others can join them

4. Proposals for Combining Attachment #1 and #2

Phil Huff offered the following successive proposals for testing acceptability related to combining Attachment #1 & #2 for the SDT to rank. The SDT reviewed and ranked three versions of the proposal. Before ranking members discussed the proposal:

SDT Comments on the Proposal for Combining Attachment # 1 & #2

- Direct impact on BES cyber system – what does that system do?
- Where do we draw the lines in the BES cyber system?
- Other criteria that may need to be considered – may need to modify.
- What if system only meets or controls part of the aggregate number?
- Need a comparable format for both proposals.
- Attachment 2 goes away and section A is changed to say cyber systems
- Connectivity is mentioned over 80 times in the comments – controls over 40 times – important concepts we need to address.
- By dropping the last half of section B, we would clarify and provide a bright line for compliance/
- For Medium/Low Criteria: Cyber systems controlling/monitoring/alerting/protecting a Generation Subsystem with aggregate rated name-plate generation of x000MVA or more. (drop rest of section?)
- Do we need to line up with higher numbers used by NERC?
- We assume there is a size and impact relationship – but that is not clear – VRFs are the mechanism for connecting.
- Multiple small risks can add up to a large risk – need to get back to and discuss the relationship.
- Concerned about dropping Attachment 2 – without the functions are we opening ourselves back up to including systems that do not control BES?
- Clarify BES cyber system and cyber system functions
- Develop the modification methodology for the categorization of BES cyber systems

a. 1st Version Proposed by Phil Huff

Attachment 2 and Attachment 1 should be combined into a single set of criteria. The subject of each criterion is the BES Cyber System and the verb would be the function being performed (the Criteria is the Span of Control).

Acceptability Ranking Scale	***4** = acceptable, I agree*	***3** = acceptable, I agree with minor reservations*	***2** = not acceptable unless major reservations addressed*	***1** = not acceptable*	***AVG.***
	2	**9**	**9**	**0**	**2.65 of 4**

SDT Comments after Ranking

- Cyber system inherits categorization of attachment 1 – concern is for the tie to attachment 1 rather than connectivity
- Categorization is based on what the system does
- Like the concept of merging 1 and 2 but needs to be criteria of BES system – cyber system needs to be a subsystem – remove “cyber” and remove last parenthetical for me to support
- Not sure what the parenthetical meant

- Huge effort to map the span of control back to the substation gear – we tried to map functions back to bright lines and it was too complicated
- I like idea of combining, but the criteria may be a problem
- There is a way to address criteria noted in comments from EPSA
- Too complex.
- This might be a way of reintroducing the serial exemption.
- Too many permutations.
- Is it possible to move forward without resolving this issue?
- Attachment 2 is complex in itself –
- Is it the fact there are criteria or is it what the criteria are? The latter we can work on together – if the former then we have a fundamental question.
- Comments said we need criteria – general agreement in industry that we need criteria – but not on what the criteria should be.
- Span of control concept seems to be the source of most concern here.
- Can we turn to others to establish the criteria?
- We had agreement that the type of communication needed to be included.
- Informal survey question to the industry? Given we want a bright line, what criteria should we use to set the bright line?
- Can we extend beyond our industry?
- How would survey question differ from Question 8 we already asked? Look to those comments for guidance and suggestions.

b. 2nd Version Proposed by Phil Huff

Attachment 2 and Attachment 1 should be combined into a single set of criteria. The subject of each criterion is the BES Cyber System and the verb would be the function being performed. ~~(the Criteria is the Span of Control).~~

Acceptability Ranking Scale	***4** = acceptable, I agree*	***3** = acceptable, I agree with minor reservations*	***2** = not acceptable unless major reservations addressed*	***1** = not acceptable*	***AVG.***
	1	**11**	**6**	**1**	**2.4 of 4**

Comments after Ranking

- We need to understand what we are going to do with the attachments to move forward – cannot write requirements without the attachments.

c. Revised Concept of Combining Attachment #1 #2.

On Friday morning, Dave Revill presented concept of combining Attachment 1 & 2 that was discussed overnight by a group including John Lim, Phil Huff, Dave Revill, Rich Kinas, Patrick Leon, Joe Deotzel and Dave Norton. He noted that under the proposal:

- Attachment 2 becomes more of a guidance document
- Res shall categorize its BES cyber systems by applying criteria in CIP 002 Attachment 1
- Changed ~~BES Subsystems~~ to <u>BES Cyber Systems</u>

- Changed Generation ~~Subsystem~~ in Attachment 1 to Generation facility.
- Move attachment 2 to a guidance document to identifying what immediate effect on real-time operations means

This proposal combines Attachment 1 and Attachment 2 by tying the criteria in Attachment 1 to BES Cyber Systems that immediately (i.e. 15 minutes or less) affect real-time operation. Attachment 2 is moved to a guidance document for identifying Cyber Systems that immediately affect real-time operations. (including the connectivity matrix)

Acceptability Ranking Scale	***4** = acceptable, I agree*	***3** = acceptable, I agree with minor reservations*	***2** = not acceptable unless major reservations addressed*	***1** = not acceptable*	***AVG.***
	8	**10**	**1**	**0**	**3.4 of 4**

Comments after Ranking

- Don't believe connectivity should be at the categorization level but should be at the controls level,
- 2= could vote a 3, but the "how" has a problem
- John L., Dave R, Rich K. and Jackie C will continue to work on the revisions to 002-4 and will pull themselves off of the control sub-teams to work on this in the short term.

R1. As a step in identifying appropriate security controls for its assets, each Responsible Entity shall categorize its BES ~~Subsystems~~ Cyber Systems ~~under its ownership~~ by applying the criteria in *CIP-002-Attachment 1 – Criteria for BES Impact Categorization of BES* ~~Subsystems.~~ *Cyber Systems*. (*Violation Risk Factor: High*)

Attachment 1: Criteria for BES Impact Categorization of BES Cyber System
Cyber Systems that would immediately effect real-time operations for:

- Generation ~~subsystem facilities~~ with aggregate rated name-plate generation of 2,000 MVA or more.
- Etc.

Move Attachment 2 to a guidance document to identifying what *Immediate effect on realtime operations* means.

Acceptability Ranking Scale	***4** = acceptable, I agree*	***3** = acceptable, I agree with minor reservations*	***2** = not acceptable unless major reservations addressed*	***1** = not acceptable*	***AVG.***
	15	**6**	**1**	**0**	**3.6 of 4**

SDT Discussion of the Proposal

- Doesn't matter where facility is if it is doing real time operations.
- Not vastly different than what we do today – big pro of this is that some of the vague terms like BES subsystem are gone – looking at cyber systems with real time impact.

- Now coming up with categorization based on some rating of facilities (a defined NERC term).
- Not changing anything in Attachment #1 except subsystem to facility – same criteria – still have to produce all generation, transmission, control center information for the auditor.
- R1 provides bright lines of generation of X name-plate rating – smaller entities do not have to jump through all the hoops.
- Do we trust entities to identify all the functions that impact real time operations?
- Problem with "facility" – introduces a new challenge for defining it – not just what is inside the fence.
- "facility" is not capitalized (i.e. in the NERC glossary) which is dangerous –
- It should be capitalized to be a defined term – but that presents new issues given the definition – it does not sound like a plant or substation – also nuclear industry has different definition that includes inside the fence.
- Can we say "generation facility or combination of facilities?"
- A BES cyber system that can affect more than 2000 of generation – strike the term "facility"
- Levels of categorization? What are the systems that will go into the list?
- This is meant as one example for high – others need to be included for generation, transmission, etc.
- What is the method for coming up with other criteria?
- Focused on the proposed concept – criteria the same as today
- "Real time"? Operating horizon criteria? It is a term defined in NERC glossary? We will need more detail.
- If use Attachment #1 how do we come up with things in main category if looking at cyber systems first? How do we know it impacts a high generation thing if we do not already identify high generation thing first?
- Doesn't really matter if we understand what generation is and what transmission is – how much of the generation is impacted – gets you off the hook for documenting all generation and making it subject to an audit.
- Careful to use accurate terms – have to identify a complete list of BES cyber systems and then determine high and medium base on criteria to be developed.
- Real time is a time horizon – "done within one hour"
- Like that it focuses on real time and brings in connectivity – may still need to tweak Attachment #1 language regarding cyber systems into h/m/l
- "Immediate"? Included to respond to industry comments,
- This concept removed ambiguous terms and provides a bottom – does not include everything in North America with a chip in it.
- Connectivity is implied somewhere?
- It would be in the table or matrix developed yesterday
- Connectivity could be left as an aspect of the controls – this does not start off with a huge inventory list which is a good thing.
- Not directly connected, but are collaterally connected to devices that are connected directly – how do we handle those?

- Where does a system that maintains targets on relays that can modify settings come in?
- These are real-time questions that we need to account for.
- Worried industry will not understand where the bright lines are with this concept.
- We may be cutting off options too soon – like to see us work with this and other options as sounding boards.
- Have to have a starting point for auditors can start with – 69 KRB might work.

D. Small Group Review of CIP-002-4 Industry Comments

The SDT reviewed group preferences for working in small groups to address the industry responses to CIP-002-4. The small groups agreed to meet together starting Wednesday morning to draft potential changes to draft 002-4 in addressing comments based on plenary discussion today and draft possible responses to comments then review suggested changes with the full team during the afternoon. It was agreed the SDT needed more work on the points of disagreement as guidance to the small groups looking at 003-009 controls. Group B and D need a better understanding of Questions #5 and #2/3 in order to do their job.

- **Group A- Definitions, Purpose and Other Comments** (Questions 1, 2) Review industry comments (overview) and agree/disagree/confusion items: Frank Kim(1), Jeff Hoffman(1), Scott Rosenberger(1), Sharon Edwards(1)
- **Group B Attachment 1- Criteria for Categorizing BES Cyber Systems** (Question #3,4,8 & 12) Review industry comments (overview) and agree/disagree/confusion items: Doug Johnson(1), John Varnell (1), John Lim (1) Jim Brenton
- **Group C VRFs, VSLs** (Question #7) **and Measures.** Review industry comments (overview) and agree/disagree/confusion items: Joe Doetzl, Phil Huff, Dave Revill, Dave Norton
- **Group D Standard Requirements** (Question #6) **(R1-3)** Review industry comments (overview) and agree/disagree/confusion items: Gerry Freese(1), Patricio Leon, Jay Crib (1), Jon Stanford (1), Bill Winters (1), Rich Kinas(1)
- **Group E External Oversight** (Question #8) Review industry comments (overview) and agree/disagree/confusion items: Keith Stouffer (2), Kevin Sherlin (2)

Bob Jones reviewed the breakout groups noting that each team should have a group report and that question 8 would go to Group E (Kevin and Keith). Each group would look at industry comments and the Team's discussion to draft potential changes in CIP 002-4 (for full team consideration later this afternoon).

SDT Comments on the CIP-002-4 Small Group Charges

- Not sure how we incorporate the models we just expressed support for?
- Can't write criteria at this point – Group C, once done may need to divide up among other groups
- What should group B try to address?
- Question 8 is under B and E? Should question 4 be assigned to E? Assign Group E to look over comments in Questions 1, 4 and 8

- May need to reorganize the groups and topics – Group C cannot address VRFs without clearer direction on criteria.
- Group C could develop a potential concept for how to develop VRFs based on review of the industry comments.
- Group B should look at comments on actual values and structure from the industry.
- Group D should draft or change requirements we have reviewed based on the SDT comments.
- Group A will need to struggle with possible definition of BES cyber system.
- Are we being asked to draft general responses? Assignment is not to draft summary response yet – take notes for later – assignment now is to refine CIP 002-4
- Bring back suggestions for changes to 002-4 – don't get too bogged down in refining the language or resolving all issues/questions

Small group sessions took place during the early afternoon followed by a plenary reports and reviews of their work.

1. **Group A: Definitions Report**

- Incorporate definitions into the attachment #1
- Intent to move them in as a descriptor
- Cascading is a glossary term
- Cyber system and BES cyber system combine into one definition
- with note that this is determined by the criteria in attachment #1
- do we need to scale it down to control systems? We may need to formally define control system rather than just describe it – may be very difficult to come to agreement on definition
- Can you clarify the note?
- Non-critical cyber assets inside an ESP – work in progress
- BES subsystem definition revised with separate definitions for generation, transmission and control center definitions (To be determined)
- Generation – can we reference the ad hoc NERC groups work last fall?
- May not want to reference, not exactly on point and has not yet been approved
- SAR just opened and group not yet appointed
- Need to loop in the requirement for interconnections – generation/owner question
- Add facilities needed to connect the generation to the transmission system
- Control center in control of multiple generation sites – combined units because they share the control system? May be covered by control center definition
- In effort to be consistent use generator facilities ratings, not the output
- Do we need to define generator subsystem? Is it covered by cyber system definition?

- If aggregate based on control center then each site takes on the level of the control center?
- The key is the risk
- Did not finish the control center definition – do question whether substations should be included
- Would take a few more hours to finish

2. Group B: Attachment #1 Report

- Question 8
- Reviewed action items
- Drop back to two tiers – leave open until controls work complete
- Use the nameplate or rating to prevent gaming
- Criterion should be separated into two with one for Protection System for which the voltage distinctions would apply and second for SPS and RAS for which the voltage distinction has no meaning.
- Change language to all control centers to get around issue of only Bas and TOPs required to have backup control centers
- Add requirement for engineering assessment approval
- Special protection systems – careful how we use it given the glossary definition and what it includes – may include more than we intend
- Engineering assessment – key is who gets to validate the assessment and does the model cover cyber systems – can't write your own rules to get the results you are seeking
- May be unintended consequences from alternative of just having bright lines
- Inner workings of cyber system placed on top of the generation system – expertise available in each but not necessarily both – the key in the assessment is what is the problem statement and who creates that statement
- Requiring all control centers to have backup control centers? No, simply need to clarify the language

3. **Group C: VSLs Report**

- Determined the percentage approach would be the best – current CIP version is binary, miss one and it is severe –
- Premature to develop VSLs until you determine the requirements

4. Group D: Standards Requirements Report

- Need to know impact of CIP 003-009 – added to schedule
- Need for an engineering analysisi and a regional authority should approve it
- A regional authority should approve eng. Analysis
- Change? Impact to the categorization

- Engineering analysis shall cover by CIPs information protection requirements
- There is no need for a master list of all BES subsystems. However BES subsystems definitions is required

SDT Comments and Questions?

- Who is the regional authority? What about region to region?
- RE will be responsible to comply with requirements – owns and operates will be toned down, know they have a protocol but not what cyber systems cover
- Where there are owner/operator relationships, need to work out responsibility and capture in their contracts
- The person that is operating the equipment understands capabilities and should have responsibility
- Becomes a compliance liability issue and who has to pay the fine – cannot avoid – assign to someone – may need to look to other standards for examples of how the issue is handled
- Currently compliance varies – there is not one way to do it
- Can flow down requirements to help meet responsibility but can't pass on the responsibility
- This is a legal problem for others to determine

5. Group E, External Oversight- Report

- Oversight is problematic (varied approaches and issues offered in the industry comments) – no
- RC needs to be involved in establishing the criteria for the engineering analysis or approving the assessments
- Engineering assessment is married to liability and needs to be resolved
- A 2 category approach may lessen the need for engineering analysis
- Clear bright lines for each region may lessen the need for engineering analysis
- Engineering analysis may be used to develop the bright lines

E. CIP-002-4 Next Steps

On Friday morning the SDT discussed next steps regarding refinements to CIP-002-4 and the development of a response document for the industry's consideration. The Chair proposed and the members agreed that a team of 4-6 members would be formed to work on refining 002-4 between now and the March meeting in Phoenix where they would present a new draft back to full team as well as a response document. The team may also continue after March.

SDT Comments on the Proposed Next Steps

- Are we setting sail without a rudder?
- Review two items of consensus – review of concept and the connectivity as a factor (and the combining attachment 1 & 2 without the parenthetical.

- Can we flesh out the concept model?
- Does concept model include the merging of the attachments 1 & 2?
- This also melded the communication concept into the model
- Concerned we did not fully address the concerns – feel we still have two models without fully understanding how they are melded together – danger of differing interpretations.
- May need to flesh out Jay's concept with phrases and words?
- Can we take a few of the criteria in attachment 1 and test them? Put requirement on paper.
- How you arrive at the h/m/l BES cyber system impact in terms of criteria is the key.
- Confusion on how h/m/l is used in Jay's concept versus the original proposal outlined by Scott Rosenberger. They seem different.
- Alternate ideas may offer more clarity – review as plus and minuses.
- Current attachment #1 is the top row of the original concept offered by Scott Rosenberger – an inherited model- title with "level of controls to be applied" – this is a site/facility concept.

III. CIP-003-009 SECURITY CONTROLS REQUIREMENTS

A. Security Controls Requirements Sub-teams Progress Reports

Personnel and Physical Security	CIP-004 – R1, R2, R3, CIP-006 R1 through R6 DHS 2.3 Personnel Security, DHS 2.11 Security Awareness and Training DHS 2.4 Physical and Environmental Security,	Doug Johnson(Lead), Rob Antonishen, Patrick Leon, Kevin Sherlin

The report was delivered by Doug Johnson who noted they have reviewed 006 and 004 and that they need to coordinate with the electronic access groups going forward. He reported they did get through the DHS items.

Recovery and Response	CIP-008 R1 & R2 CIP-009 R1 through R5 Incidence Response and Contingency Planning	Scott Rosenberger (Lead), Joe Doetzl, *Observer Participants: Jason Marshall*

Scott Rosenberger reported on the Subteam's progress noting he had met with Jeri Domingo Brewer to review the efforts in Tucker and the Subteam had difficulty meeting as a team since the January meeting. They have however completed an initial shot at h/m/l and will be working forward.

Access Control and Auditing	CIP-003 R5; CIP-005 R2; CIP-007 R5; CIP 004 R4 DHS 2.15 Access Control DHS 2.16 Audit and Accountability	Sharon Edwards (Lead), Jeff Hoffman, Frank Kim *Observer Participants: Sam Merrell*

Sharon Edwards reported on the Sub-team's work. They had one interim meeting together then each member has worked on assignments which are almost complete. They met one night meeting in Austin and plan another in a week before combining into one document. They have developed a collaborative site to review documents.

SDT Questions

- Is there a format we should be using? Jay's or Rob's A. document from Tucker meeting? Want to combine the 25 separate documents they have into a common format other teams are using
- Rob's was a summary document
- Spreadsheet did not work for John Varnell's group – they put in to a different format – can't put text into Rob's spreadsheet document

Change Management, System Lifecycle and Information Management	CIP-003 R6; CIP-007 R1, R7 CIP-003 R4; CIP-005 R5.1.1, R5.1.3 DHS 2.5 System and Services Acquisition, DHS 2.6 Configuration Management and System Lifecycle, DHS 2.10 System Development and Maintenance DHS 2.9 Information and Document Management, DHS 2.13 Media Protection	Keith Stouffer, Dave Revill, Phil Huff (Lead) *Observer Participants: John Fridye*

Dave Revill provided the report noting they don't have a collaborative site to share documents but they are mapping controls to the existing CIP requirements and analyzing the difference between CIP and other standards.

Security Governance	CIP-003 – R1, R2, R3; CIP-005 R4, CIP-007 R8 DHS 2.1 Security Policy, DHS 2.2 Organizational Security, DHS 2.7 Strategic Planning, DHS 2.17 Monitoring and Reviewing Control System Security Policy, DHS 2.18 Risk Management and Assessment, DHS 2.19 Security Program Management	Jon Stanford (Lead), Jerry Freese, Dave Norton

No report was given for this subteam.

Operations Security	CIP-005 R1, R3 CIP-007 R2, R3, R4, R6 DHS 2.8 System and Communication Protection DHS 2.14 System and Information Integrity	Jay Cribb (Lead), Jim Brenton, Jackie Collette, John Varnell

Jay Cribb reported on this group's effort including one meeting where they reviewed portions of CIP 005& 007 and reviewed corresponding DHS and other catalogue of controls. Finally they developed four high level questions for additional guidance to all the groups

B. Guidance Questions for the Security Controls Requirements Sub-teams

Following the Tucker meeting, the Drafting Principles were revised by Phil Huff based on team discussion and sent back around to team members. Phil reviewed the steps in the team process and proposed deliverables (separate document) for the sub team work on the proposed control requirements, 003-009, with impact and environment applicability

Jay Cribb introduced and reviewed the four questions the Operations Security group had developed noting, in essence, the NERC CMEP and ROP have the SDT in a very constrained

box currently. We've got a CIP-002 structure that is on a path that won't fit in that box. He suggested we need some determinations on these things before we get too far down the road and hit a roadblock.

1) **How we are going to handle writing requirements that apply to 'BES Cyber Systems' rather than 'Critical Cyber Assets'?**
   The object to which requirements are applied has changed rather drastically and we need to determine how an entity takes a requirement applied to a 'cyber system' and knows what to do to what components of that system in a clear, repeatable, auditor-must-come-to-the-same-conclusion kind of way.

SDT Discussion Points

- Access control – we each have different systems that join into one organism – components of the whole.
- How do you apply virus protection to one component and not to another connected component? How do you write requirement to apply to operating systems that can be compromised without bringing in other components?
- Don't need protection on every relay or printer – may need to do a better job of writing the requirements in the future.
- Authorizing access to a cyber system? If so, is that access to every component? Authorized access to a system may not include physical access.
- Do we need to stratify for new and old systems? The latter were not designed for the current cyber system.
- How much of the details are in the guidance? Is there something between requirements and guidance? Such as specifics on password protection.
- May need to get more granular than just h/m/l to fit in the wide variety of circumstances – a risk management system.
- Have to get more granular, more prescriptive in tables – any guidance will be treated as required in practice – otherwise may need an engineering study to say why you did not follow guidance to avoid liability – may not be able to answer this question
- TFEs – address in question three.
- Talked about using tables to outline the specifics.
- Access control – the extent or reach of the controls can become expensive and time consuming as we move out to remote sites.
- At least three or four levels of access you can make work – but be clear how far the access goes.
- Controls need to be applied to the system.
- We want to go to "specific" rather than "prescriptive" – the latter is telling you how to do that – need to be specific to be clear for audits.
- Are there other documents or bodies we can reference or build on for our use?
- Moving forward apply at a high level and note where specificity may be needed
- Compliance is more difficult in virtual world where harder to separate pieces – not dealing with physical items as much as before

- How we chose to use words and what words we chose to use will matter to allow clarity for audits – struggle to write appropriate requirements and measures.
- Many different compliance methodologies for the same requirement – auditors recognize different solutions across the industry.
- We use language differently – legalese, cyberese, etc.
- Make sure requirements and measures can stand the test of time.
- Most standards are not working to a prescriptive measure.
- Helpful to know if standards development allows for more flexibility.
- Referring to other documents and tying them to the requirement will not work because those other documents could be changed outside or independently of our process – can go into guidance but not the requirements
- Want to change the NERC process for setting standards measures – why continue with a broken system.
- We can use examples as part of the guidance.
- What is our direction as a team as to the guidance and measures? How do we go about developing engineering based measures in our standards? We need a body that can certify approaches? We need to get to measurability and we do not have way to certify measures
- Staff will go back to NERC to try and figure out how we can justify the thresholds or measures we use in the standards
- Putting in bright lines in 002 but removing some of the brightness in 003-009 – currently have bright yes/no requirements but moving toward more flexibility in how we meet measures
- Can clarify the what but not the how – the how is a compliance issue

2) **At what level are we to write the requirements?**
We have some that are taking the DHS controls and tweaking based on CIP. We have some taking the CIP requirements and tweaking based on the DHS controls. But the two are written at vastly different levels. Which is it? Should we:
    - Take the DHS controls and tweak them based on CIP; or
    - Take the CIP requirements and tweak them based on the DHS controls

SDT Discussion Points
- Right at the correct level – may be the best answer to the previous questions
- Have to get to a higher level or end up writing 100 pages for every contingency in each requirement
- Requirements should apply to either 1. The BES cyber System as a whole or 2) components of the BES Cyber System. When a requirement only applies to specific types of components, describe those types of components to determine where component classes exist. Requirements specific to boundary protection or ESP can be written to the interface of the BES Cyber System
- Just meant to guide sub teams in writing requirements for review at the next meeting – drafting guidance –

- Answer to second from discussion of the first may by be the second bullet to take the CIP requirements as the base
- Taking CIP language to a higher level, changes the words and may be harder to measure
- Not all of the subject areas need the same level or amount of change – also may not be a one size fits all – some may be approached better from CIP and some from DHS
- Utilize the words that are there, change the ones we need to and start with either CIP or DHS as appropriate
- Careful about unintended consequences – everyone understood TFEs but ended up with unintended consequence
- Any base of information coming back from audit spot checks that highlights issues we need to incorporate into our rewrite?
- Can we request a summary from the regional auditors working group?
- Be sure we are not just taking one view point or opinion
- CCWG is such a regional group that would give a broader view than just a few individuals – trends, problems and issues they would like for us to be aware of as we move forward
- Asking for information on what difficulties they face, not asking for their direction

3) We've got to have some kind of ruling on the topic of compensating controls in a NERC CMEP world.

- Are we writing requirements at a detailed level with very discrete measurement and where compensating controls are not allowed (or just simply known as TFE's)? If so, are we going to add "where technically feasible" language like the current NERC ROP requires us to do on every requirement so that TFE's can even be requested?

  or

- Are we stating a control objective and how the entity meets it is up to them?

SDT Discussion Points

- Addressed in part above
- We may only be able to carefully craft the words of the requirements because that is what you will be held accountable for in an audit
- Compensating controls – NERC did not take it off the table but suggested need careful oversight methods for accountability
- May need to educate FERC that there are no guarantees in cyber protection – they want yes or write us a check –
- Definition of "within"? How do we comply if we are not sure what it means?
- This is not a SDT issue to resolve – careful how we write requirements – have to leave at level of implement a boundary protection, but not the how to do it

4) We need a standard way to not only handle the difference in impact and environment (CC/Gen/Tran), but the difference in cyber system/device class.

Control Centers, Plants, and Substations all can have Windows based HMI's for example. But plants typically have PLC's, and substations have IEDs. We need a standard way to handle the device classes so that we don't write requirements for the "IT style" cyber assets

that end up generating TFE's for every other device class.

- How should we handle the difference in impact and environment (CC/Gen/Tran)?
- How should we hand the different in cyber system/device class?

SDT Discussion Points

- Some overlap with earlier discuss
- Have to write controls to apply to the class of device
- What are the standard device classes and definition of each?
- Better off avoiding too high a level of control
- Difference in environment? Cost benefit analysis troubles me as a tool due to variables between entities and environments
- Need more than a cafeteria approach of what looks good or appealing

C. Additional Sub-Team Drafting Guidance Statements

Based on the SDT discussion the following guidance statements were proposed to be added to those developed at the Tucker meeting:

Underlined Added Guidance from February 19 SDT Discussion

For the purpose of maintaining consistency across the teams and capturing interim decisions and change documentation, each team should utilize the following development process.

1. **DHS Catalogue of Controls:** Begin by identifying applicable controls that are enumerated in the *DHS Catalog of Control System Security Recommendations* for High Impact Cyber Systems.
2. **Cross Reference CIP Version 3 Requirements/sub-Requirements:** For each security control identified in step 1, cross reference the CIP version 3 Requirement/sub-Requirement or validate previous mapping work.
3. **Specific not prescriptive:** As a general rule, be specific but not prescriptive in writing the requirements.
4. **"What" not "How":** In general, seek to draft a "what" requirements, not "how" requirements.
5. **Develop the requirement language** for each security control identified in step 1.

a. When mapping to existing CIP requirements, use language from CIP, making improvements where needed.
b. When no associated requirement from CIP exists, develop the new requirement using language from the *DHS Catalog.*

6. **Document significant changes to CIP Standards:** Document significant changes made to previous versions of the CIP Standards. Conceptual or broad changes can be captured by a single statement.
7. **Incorporate existing CIP requirements not mapped to the *DHS Catalog*.** If a requirement is no longer necessary because the intent was captured elsewhere, then include this in the change documentation.
8. **Address specific directives from FERC Order 706** that may be applicable to the requirement.

9. **Analysis and Determination of Requirements for Medium and Low Impact:** In the analysis and determination of applicability of requirements to Medium and Low Impact Cyber Systems, ~~on the basis of~~ consider the cost ~~vs.~~ in relation to the security benefits (i.e., a minimal cost requirement that significantly mitigates risk would apply to *ALL* Cyber Systems. Similarly, a significant cost requirement that minimally reduces risk or provides little additional security may apply only to *HIGH* impact Cyber Systems).
10. **Specify Applicability to Environments:** Specify applicability of a requirement to Generation, Transmission, and/or Control Center environments.
11. **Apply Requirements to BES Cyber System:** Requirements should apply to either:
    (a) The BES Cyber System as a whole, or
    (b) Components of the BES Cyber System. However, when a requirement only applies to specific types of components, Sub-Teams should describe those types of components to determine where component classes exist.
    (c) Requirements specific to boundary protection or ESP can be written to the interface of the BES Cyber System.
12: **Level of Requirements:** Sub-Teams should generally write the requirements at a high enough level to avoid applicability of specific technology. Where there are applicable CIP requirements, start with the CIP words and tweak if needed to include some DHS language/concept. However, the "level" of the requirements text should be raised, if needed.

IV. NEXT STEPS

The Chair reviewed the progress made at the meeting and the need for the sub-teams to continue to meet between Austin and the Phoenix meeting to bring draft language for the security controls for review by the full team. He also noted the agreement on a revised schedule and the formation of a Team to take the CIP-002-4 draft and make refinements and develop a response document to the industry comments.

The Vice Chair agreed to work with the facilitators to revise the Sub-team drafting guidance statements based on this discussion and circulate them in advance of the March meeting.

The meeting adjourned at 12:15 p.m.

_____

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Appendix # 1— Meeting Agenda

Project 2008-06 Cyber Security Order 706 SDT
Draft 19th Meeting Agenda
February 16, 2010, Tuesday- 1 PM to 5 PM CST
February 17, 2010 Wednesday- 8 AM to 5 PM CST
February 18, 2010 Thursday- 8 AM to 5 PM CST
February 19, 2010 Friday- 8 AM to 2 PM CST
ERCOT Austin MET Center
7620 Metro Center Dr.
Austin, Texas 78744

NOTE:
1. Agenda Times May be Adjusted as Needed during the Meeting
2. Drafting Group Meetings May Not Have Access to Telephones and Ready Talk

Proposed Meeting Objectives/Outcomes

- Review the CSO 706 SDT 2010 Work plan
- Receive updates on other related cyber security initiatives
- Receive a NERC update on implementing the CIP Communication Plan
- Review, discuss industry comments and identify issues raised to be addressed in refinements;
- Review, refine and adopt a revised CIP 002-4 for posting
- Receive progress reports and review assignments for Security Control Sub-Teams
- Agree on next steps and assignments

Draft Agenda

Tuesday	**February 16, 2009**
1:00 p.m.	Welcome and Opening Remarks- *John Lim, Chair & Phil Huff, Vice Chair* Roll Call; NERC Antitrust Compliance Guidelines Facilitator review and SDT acceptance of January 19-22, 2010 Tucker SDT meeting summary
1:10	Review of Meeting Objectives, Agenda and Meeting Guidelines- *Bob Jones*
1:15	Review of CSO 706 SDT Workplan- February-December, 2010- *Stu Langton*
1:20	Updates on other related cyber security initiatives- *NERC Staff and SDT Members*
1:30	Update on CIP Communication Plan, including Webinar Report
1:45	Review of needed CIP-002-4 Documents for posting: Introduction, Comment Form, Requirements, Attachments, Implementation Plan.
2:00	Overview of the Industry Comments on the CIP-002-4 *John Lim and Phil Huff*
2:45	*Break*
3:00	Identification of Key CIP 002-4 Issues Raised by Industry Responses to Comment form Questions (1-13)
4:30	Review and Initial Discussion of Other Proposed Approaches to CIP-002-4 *(Dave Norton etc.)*

5:25	Review of Proposal for Wednesday's Agenda
5:30	*Recess*

Wednesday	**February 17, 2010**
8:00	Welcome and Agenda Review- *John Lim & Phil Huff*
8:10	Discussion and Consensus Testing of Concepts and Responses to Industry Comments and Critiques
10:15	Break
10:30	Discussion and Consensus Testing of Concepts and Responses to Industry Comments and Critiques
12:00	*Working Lunch*
12:45	Review and Agree on How to Refine CIP 002-4 *(Full Group or Drafting Sub-Groups)*
1:15	Clarify Issues and Begin Draft Possible CIP 002-4 Refinements *(Full Group or Drafting Sub-Groups)*
4:00	If Sub Team Formed- Initial Reports and Flagging Issues Needing Full Team Guidance
4:55	Review Assignments and Thursday Agenda
5:30	*Recess*

Thursday	**February 21, 2010**
8:00	Welcome and Agenda Review- *John Lim & Phil Huff*
8:05	Approve Tucker Meeting Summary Approve Revised CSO 706 SDT Schedule
8:15	Review Proposal from Last Night's Categorization Alternatives Discussion (*Beer Brigade)Scott Rosenberger (Jon Stanford, Frank Kim, John Lim, Dave Norton Brian Newell)* Review Proposal for Combining Attachment 1 and 2 *Phill Huff*
10:00	Convene Drafting Groups to Complete CIP-002-4 Refinements
12:00	*Working Lunch*
3:15	Break
3:30	Drafting Group Reports and Full Team Consideration and Consensus Testing
5:15	Review CIP 002-4 Assignments and Friday Agenda
5:30	*Recess*

Friday	**February 22, 2010**
8:00	Welcome and Agenda Review- *John Lim & Phil Huff*
8:05	Review and Agreement on CIP 002-4 Proposal from Last Night's Drafting Group- Formation of a CIP 002-4 Drafting Team and Next Steps
9:15	Communications Plan- Gerry Adamski
9:30	Brief Security Controls Requirements Subteam Progress Reports Review of Drafting Principles and Guidance (from Tucker meeting) Review of Key Questions Security Controls 003-009- Operations Security Sub-Team and suggestions for refinements of the Principles and Guidance document
10:00	*Break*
10:15	Continue Review of Key Questions and Answers

12:00	Review and Agree on Next Steps for Developing Security Controls (CIP 003-009) and Work plan for March 2010 Meeting on Security Controls and CIP 002-4 Review Meeting Evaluation
12:15	*Adjourn*

Appendix # 2 Attendees List
February 16-19, 2010, Austin, Texas

Attending in Person — SDT Members and Staff

1. Jim Brenton (Wed-Fri.)	ERCOT
2. Jay S. Cribb	Information Security Analyst, Southern Company Services
3. Joe Doetzl (Wed)	Manager, Information Security, Kansas City Pwr. & Light Co.
4. Sharon Edwards	Duke Energy
5. Jeff Hoffman	U.S. Bureau of Reclamation, Denver
6. Gerald S. Freese	Director, Enterprise Info. Security America Electric Pwr.
7. Phillip Huff, Vice Chair	Arkansas Electric Coop Corporation
8. Doug Johnson	Exelon Corporation – Commonwealth Edison
9. Frank Kim	Ontario Hydro
10. Rich Kinas	Orlando Utilities Commission (Wed.)
11. Patricio Leon	Southern California Edison
12. John Lim, Chair	CISSP, Department Manager, Consolidated Edison Co. NY
13. David Norton	Entergy
14. David S. Revill	Georgia Transmission Corporation
15. Scott Rosenberger	Luminant Energy
16. Kevin Sherlin	Sacramento Municipal Utility District (Wed. Thurs.)
17. Jonathan Stanford	Bonneville Power Administration
18.Keith Stouffer	National Institute of Standards & Technology
19. John D. Varnell	Technology Director, Tenaska Power Services Co. (Wed. Thurs)
20. William Winters	Arizona Public Service, Inc.
Roger Lampilla	NERC
Scott Mix	NERC
Howard Gugel	NERC
Gerry Adamski (Fri by phone)	NERC
Joe Bucciero	NERC/Bucciero Consulting, LLC
Robert Jones	FSU/FCRC Consensus Center
Hal Beardal	FSU/FCRC Consensus Center
Stuart Langton	FSU/FCRC Consensus Center

SDT Members Attending via ReadyTalk and Phone

21. Rob Antonishen	Ontario Power Generation (Thurs)
22. Jackie Collett	Manitoba Hydro (Wed/Thurs)

Others Attending in Person

Jason Marshall	Midwest ISO

Others Attending via WebEx and Phone

Stacy	Bresler	sbresler@wecc.biz
Chuck	Coulter	ccoulter@wecc.biz
Bryn	Wilson	wilsonwb@oge.com
Rod	Hardiman	rchardim@southernco.com
Annette	Johnston	ajjohnston@midamerican.com
Bryn	Wilson	wilsonwb@oge.com
Jerome	Farquharson	jfarquharson@burnsmcd.com
Bill	Glynn	bill.glynn@westarenergy.com
Bill	Keagle	william.a.keagle.jr@constellation.com
Keith	Walters	step@eei.org
Joshua	Axelrod	jmaxelrod@gmail.com
Steve	Newman	srnewman@midamerican.com
Justin	Kelly	Justin.Kelly@ferc.gov
Don	Schopp	donald.schopp@constellation.com
Bryn	Wilson	wilsonwb@oge.com
Jack	Vranish	jack.vranish@pacificorp.com
Bob	Chambers	robert.chambers@ferc.gov
Rod	Patterson	rnpatterson@midamerican.com
Laura	Hussey	laura_hussey@selgs.com
Bob	Chambers	robert.chambers@ferc.gov
Bryn	Wilson	wilsonwb@oge.com
Keith	Walters	step@eei.org

Appendix # 3 — NERC Antitrust Compliance Guidelines

I. General

It is NERC's policy and practice to obey the antitrust laws and to avoid all conduct that unreasonably restrains competition. This policy requires the avoidance of any conduct that violates, or that might appear to violate, the antitrust laws. Among other things, the antitrust laws forbid any agreement between or among competitors regarding prices, availability of service, product design, terms of sale, division of markets, allocation of customers or any other activity that unreasonably restrains competition.

It is the responsibility of every NERC participant and employee who may in any way affect NERC's compliance with the antitrust laws to carry out this commitment.

Antitrust laws are complex and subject to court interpretation that can vary over time and from one court to another. The purpose of these guidelines is to alert NERC participants and employees to potential antitrust problems and to set forth policies to be followed with respect to activities that may involve antitrust considerations. In some instances, the NERC policy contained in these guidelines is stricter than the applicable antitrust laws. Any NERC participant or employee who is uncertain about the legal ramifications of a particular course of conduct or who has doubts or concerns about whether NERC's antitrust compliance policy is implicated in any situation should consult NERC's General Counsel immediately.

II. Prohibited Activities

Participants in NERC activities (including those of its committees and Subroups) should refrain from the following when acting in their capacity as participants in NERC activities (e.g., at NERC meetings, conference calls and in informal discussions):

- Discussions involving pricing information, especially margin (profit) and internal cost
- information and participants' expectations as to their future prices or internal costs.
- Discussions of a participant's marketing strategies.
- Discussions regarding how customers and geographical areas are to be divided among competitors.
- Discussions concerning the exclusion of competitors from markets.
- Discussions concerning boycotting or group refusals to deal with competitors, vendors or suppliers.

III. Activities That Are Permitted

From time to time decisions or actions of NERC (including those of its committees and

Subroups) may have a negative impact on particular entities and thus in that sense adversely impact competition. Decisions and actions by NERC (including its committees and Subroups) should only be undertaken for the purpose of promoting and maintaining the reliability and adequacy of the bulk power system. If you do not have a legitimate purpose consistent with this objective for discussing a matter, please refrain from discussing the matter during NERC meetings and in other NERC-related communications.

You should also ensure that NERC procedures, including those set forth in NERC's Certificate of Incorporation and Bylaws are followed in conducting NERC business. Other NERC procedures that may be applicable to a particular NERC activity include the following:

- Reliability Standards Process Manual
- Organization and Procedures Manual for the NERC Standing Committees
- System Operator Certification Program

In addition, all discussions in NERC meetings and other NERC-related communications should be within the scope of the mandate for or assignment to the particular NERC committee or Subroup, as well as within the scope of the published agenda for the meeting.

No decisions should be made nor any actions taken in NERC activities for the purpose of giving an industry participant or group of participants a competitive advantage over other participants. In particular, decisions with respect to setting, revising, or assessing compliance with NERC reliability standards should not be influenced by anti-competitive motivations.

Subject to the foregoing restrictions, participants in NERC activities may discuss:

- Reliability matters relating to the bulk power system, including operation and planning matters such as establishing or revising reliability standards, special operating procedures, operating transfer capabilities, and plans for new facilities.
- Matters relating to the impact of reliability standards for the bulk power system on
- electricity markets, and the impact of electricity market operations on the reliability of the bulk power system.
- Proposed filings or other communications with state or federal regulatory authorities or other governmental entities.
- Matters relating to the internal governance, management and operation of NERC, such as nominations for vacant committee positions, budgeting and assessments, and
- employment matters; and procedural matters such as planning and scheduling meetings.

Any other matters that do not clearly fall within these guidelines should be reviewed with NERC's General Counsel before being discussed.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

APPENDIX # 4
CSO 706 SDT MEETING SCHEDULE
JANUARY –DECEMBER 2010

Preliminary, Draft, Unofficial Schedule for CIP-002-4

CIP-002 Task	CIP 2 Milestone Date	Week-of	Date	CIP-003 -- CIP-009 Task
		1/18/10		SDT Meeting - Work on requirement language
		1/25/10		sub-team meetings
		2/1/10		sub-team meetings
Informal Comment Period closes	2/12/10	2/8/10		sub-team meetings
SDT Meeting - React to comments		2/15/10		
Post for 45-day formal comment; form ballot pool	2/25/10	2/22/10		sub-team meetings
		3/1/10		sub-team meetings
		3/8/10		SDT Meeting - Work on requirements
		3/15/10		post initial unofficial draft (aid in CIP-002 ballot process)
		3/22/10		sub-team meetings
Initial Ballot start	4/2/10	3/29/10		sub-team meetings
		4/5/10		sub-team meetings
Initial ballot close; SDT Meeting - respond to comments	4/12/10	4/12/10		
		4/19/10		sub-team meetings
Recirc Ballot start	4/30/10	4/26/10		sub-team meetings
		5/3/10		sub-team meetings
Recirc ballot close; SDT meeting - respond to comments	5/10/10	5/10/10		
Re-recirc ballot start	5/16/10	5/17/10		sub-team meetings
Re-recirc ballot close; BoT Approval	5/25/10	5/24/10		sub-team meetings
File with Regulators	5/31/10	5/31/10		sub-team meetings
		6/7/10		SDT Meeting - Work on requirements
		6/14/10		
		6/21/10		
		6/28/10		
		7/5/10		
		7/12/10		SDT Meeting
		7/19/10		
		7/26/10		
		8/2/10		

CSO 706 SDT WORKPLAN TO DATE
OCTOBER, 2008 –DECEMBER 2010

DEVELOPMENT OF CIP VERSION 2 AND NEW VERSION FRAMEWORK
OCTOBER 2008–JULY 2009

1. October 6–7, 2008 — Gaithersburg, MD Reviewed CIP-002-CIP-009, Agreed on Version 2 approach.
2. October 20–21 —Sacramento, CA CIP-002-CIP-009 Version 2 development
3. November 12–14, 2008 — Little Rock, AR CIP-002-CIP-009 Version 2 adoption for comment and balloting; CIP-002-CIP-009 New Version process reviewed.
4. December 4–5, 2008 — Washington D.C. CIP-002-CIP-009 Version 3 reviewed and debated, SDT member white "working" papers assigned, Technical Feasibility Exceptions white paper reviewed and refined.
5. January 7–9 — Phoenix, AZ, Reviewed Technical Feasibility Exceptions white paper**,** reviewed industry comments on CIP-002-CIP-009 Version 2 products — established small groups to draft responses, reviewed New Version white "working" papers.
January 15 — WebEx meeting(s) Small group drafted responses to industry Version 2 comments.
January 21 — WebEx meeting(s) Small group drafted responses to industry Version 2 comments.
6. February 2–4, 2009 — Phoenix, AZ Update on NERC Technical Feasibility Exceptions process**,** VSL process and SDT role**,** review of Version 3 White papers, strawman and principles**,** reviewed and adopted SDT responses to industry comments on Version 2 and Version 2 Product Revisions.
7. February 18–19, 2009 — Fairfax, VA Update on Version 2 process**,** NERC TFE process and VSL Team process; reviewed, discussed and refined Version 3 CIP-002 White papers, strawman, and principles.
8. March 10–11, 2009 — Orlando, FL Update on NERC TFE and VSL and VRF Team process and review and refine Version 3 CIP-002 Strawman Proposals
March 2–April 1, 2009 — 30-day Pre Ballot
Mid-March — NERC posts TFE draft Rules of Procedure for industry comment
March 30, 2009 — WebEx meeting(s) White Paper Drafting Team
April 1–10 — NERC Balloting on Version 2 Products
April 6, 2009 — WebEx meeting — White Paper Drafting Team
April 8, 2009 — WebEx meeting(s) — White Paper Preview- Full SDT Conference Call
April 11, 2009 — Version 2 Ballot Results (Quorum: 91.90% Approval: 84.06%) and Industry Comments
9. April 14–16, 2009 — Charlotte NC Update on NERC TFE process, VSL Team process and NERC Critical Assets Survey; agreed and adopted responses for Version 2 industry comments for recirculation ballot; reviewed and refined Version 3 whitepaper and consensus points and progress report to NERC Member Representative Committee (MRC) May meeting.
April 28 and May 6, 2009 — White Paper Drafting Team Meetings and WebEx
April 17–27, 2009 — Recirculation Results: Quorum: 94.37% Approval: 88.32%
May 5, 2009 — NERC MRC Meeting, Arlington, VA- SDT progress report.
10. May 13–14, 2009 — Boulder City NV Reviewed MRC presentation and further SDT refinement and discussion of the Version 3 White Paper.
June 8 and June 15, 2009 — Working Paper Drafting Team Meetings and WebEx
11. June 17–18, 2009 — Portland OR Further SDT refinement of the draft CIP Version 3 Working Paper(s), reviewed SDT development process for June-December 2009; discussed potential SDT subcommittee structure and deliverables.

- *June — WebEx meeting(s)*
- *Working Paper drafting group sessions including inputs from selected industry personnel to help establish BES categorization criteria*

CIP-002 DEVELOPMENT OF REQUIREMENTS, MEASURES, ETC. JULY-DECEMBER 2009

12. July 13–14, 2009 in Vancouver, B.C., Canada

SDT reviewed, refined, and adopted SDT Working Paper. SDT adopted its response to NERC for Interpretation of CIP-006-1. SDT reviewed and adopted a proposal for CIP-002 Subgroups and Deliverables and convened subgroup organizational meetings to develop work plans. SDT adopted 2010 Meeting Schedule.

- *July–August Interim Conference call meeting(s)*
- *CIP-002 Subgroup meetings*
- *CIP-002 Coordination Team meeting*
- *August 3–5, 2009 in Winnipeg, Manitoba **NERC Member Representative Committee**. Progress Report and presentation on new CIP Version 3 Working Paper-Concept- Reliability Standards on Cyber Security for MRC input.*

13. August 20–21, 2009 in Charlotte, NC. SDT reviewed and responded to MRC input on Working Paper/CIP-002 Concepts and convened SDT Subgroup and plenary meetings to develop CIP-002 requirements and "proof of concept" control (s).

- *July–September — 45-day Industry Comment Period on CIP-002 Concept Working Paper*
- *NERC Webinar- August–September Interim Conference Call meeting(s)*
- *CIP-002 Subgroup meetings (as ne*
- *CIP-002 Coordination Team meeting*

14. September 9–10, 2009 in Folsom, CA. SDT reviewed and considered industry comments on the Working Paper and CIP-002 concepts and their application to the subgroup work and addressed coordinating issues through joint subgroup meetings. SDT agreed on meeting dates and proposed locations for January–December 2010 September–October Interim WebEx meeting(s)

- *FERC Version 3 Urgent Action SDT conference call meetings*
- *CIP-002 Coordination Team meeting*

CIP VERSION 3 RESPONSE TO FERC ORDER, OCTOBER-DECEMBER, 2009

15. October 20–22, 2009 in Kansas City, MI. Reviewed new FERC Order and urgent action CIP Version 3 process; discussed key issues raised by SDT CIP 002 Subgroups, small group meetings and agreement on refinements to the CIP 002-009 schedule and drafting process for CIP 002-4.

- *October–November Drafting Team meeting(s)*
- *CIP-002 Coordination Team meeting*

16. November 16–19, 2009 in Orlando, FL

- SDT review, refine and adopt Version 3 "industry response" document.
- SDT plenary and drafting group session(s) — to draft, review and refine CIP-002-4 standard, requirements, measures and controls and related documents.
- November–December Interim Conference call meeting(s)
- Drafting teams as needed to finalize draft CIP 002-4 documents
- CIP-002 Coordination Team meeting
- *CIP 002-4 Drafting Team produces next draft based on Orlando Meeting input.*
- *December 2 CSO 706 SDT Version 3 Consideration of Comments Draft Conference Call*
- *December X, CSO 706 SDT CIP 002-4 Preview Conference Call*

17. December 15–16, 2009 in Little Rock AK

- SDT scenario "walk through" to test flow of CIP 002-4.
- SDT plenary and drafting group session(s) to review, refine, and agree on and adopt CIP-002-4 standard, requirements, measures and controls and related documents.
- Agree on initial posting of draft CIP-002-4 for industry review and comment.
- Agree on next steps and 2010 Workplan and schedule

CIP Version 3 Key Steps/Schedule

1. *Post for Industry Comment 10-13-09 to 11-12-09*
2. **November 13 SDT Conference Call- Review of Industry Comments and Response**

3. **November 16, SDT 706 Meeting in Orlando, Monday, 5:00 p.m.- through dinner- SDT 706 Response Document to Industry Comments**
4. **November 17**, Tuesday, SDT 706 Meeting, Orlando, Complete and Adopt Industry Response Document.
5. **November 18**, Wednesday, Post Response Document and Ballot
6. **November 27**, Friday *(after Thanksgiving)* Deadline for Votes and Comments
7. **November 30, Monday, SDT 706 - Conference Call- finalize Industry Response document.**
8. **December 1- 10,** Recirculation Ballot.
9. **December 11,** BoT Approval
10. **December 29, 2009,** FERC Filing

CIP 002-4 Key Steps/Schedule (October-December 2009)

1. **November 1:** Jackie Collett, Phil Huff, John Lim and John Varnell, the chairs of the 4 CIP 002 Subgroups will form the CIP 002 Strawman Drafting Group (SDG).
2. **November 1:** All CIP 002 "meta groups" and subgroups will forward to the Strawman Drafting Group their standards text drafts including any guidance language**.**
3. Joe Doetzl will coordinate the work of the Controls Drafting Group (CDG) members: Jim Brenton, Keith Stouffer, Bill Winters, Jon Stanford. They will produce several recommended sample controls to illustrate high/medium/low concepts in CIP 002 as well as recommendations on whether the SDT should request guidance from the Standards Committee on referencing a 'catalogue of security requirements', for circulation to the SDT **by Friday, November 13, 2009**.
4. The SDG will prepare a strawman draft by **November 13, 2009** for review by the SDT in advance of November 16-19, 2009 SDT meeting.
5. The SDT will utilize the strawman draft to organize its **November 16-19 meeting** and determine at the conclusion of the meeting if the SDT will continue to aim for the December adoption of CIP 002 draft on **December 16** for posting for industry comment.
6. The SDG and the CDG will present their 2nd drafts at a SDT conference call the **first week in December**.
7. The SDT will refine and circulate a strawman Draft #3 prior to the **December 15-16** SDT 706 meeting in Little Rock.
8. **December 15-16** will refine, finalize and adopt the CIP 002 posting for the industry.

- December 28, 2009 SDT Conference Call on CIP 002-4
- December 30, 2009 SDT Leadership Call- Security Controls Survey Draft
- January 6, 2010, SDT Conference Call- Review Security Controls Draft Principles and Schedule and Appoint Drafting Team to bring strawman to January SDT Meeting in Tucker.

CSO SDT 706 2010 MEETING SCHEDULE

18. January 19–22 — Tuesday-- Friday, Tucker, GA (GTC)	24. July 13–16, Tuesday-–Friday, Pittsburgh, PA (CERT)
19. February 16-19 Tuesday–Friday, Austin TX (ERCOT)	25. August 10--13, Tuesday—Friday, TBD
20. March 9–12 — Tuesday–Friday, Phoenix, AZ (APS)	26. September 7–10, Tuesday—Friday, Winnipeg, Canada
21. April 13–16 — Tuesday-Friday, Atlanta GA (SouthernCo)	27. Oct. 12–15, Tuesday-Friday, TBD
22. May 11-14 — Tuesday-Friday, Dallas TX (Luminant)	28. November 16–19, Tuesday-Friday, TBD
23. June 8–11 — Tuesday-Friday, Sacramento CA (SMUD)	29. December 14–17, Tuesday-Friday, TBD

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Appendix #5

Security Controls Sub-Team
Principles and Drafting Guidance

CSO 706 SDT SECURITY CONTROLS SUB-TEAM DRAFTING PRINCIPLES

(ADOPTED BY CSO 706 SDT, JANUARY, 2010)

1. Applicability [NERC ROP] Each reliability standard shall clearly identify the functional classes of entities responsible for complying with the reliability standard, with any specific additions or exceptions noted.	**9.Practicality** [NERC ROP] – Each reliability standard shall establish requirements that can be practically implemented by the assigned responsible entities within the specified effective date and thereafter.
2.Reliabiliy Objective [NERC ROP] Each reliability standard shall have a clear statement of purpose that shall describe how the standard contributes to the reliability of the bulk power system.	**10. Consistent Terminology** [NERC ROP] To the extent possible, reliability standards shall use a set of standard terms and definitions that are approved through the NERC reliability standards development process.
3.Performance Requirement or Outcome (NERC ROP) Each reliability standard shall state one or more performance requirements, which if achieved by the applicable entities, will provide for a reliable bulk power system, consistent with good utility practices and the public interest.	**11. Commensurate Controls for BES Impact Categories.** Security controls shall be commensurate with the identified level of BES impact categories.
4. Measurability (ROP) Each performance requirement shall be stated so as to be objectively measurable by a third party with knowledge or expertise in the area addressed by that requirement.	**12. Change Documentation.** Changes from prior versions of CIP Standards have clear rationale. These include the following types of changes: a. Above and beyond the current standards; b. Removal of requirements; and c. Major formatting changes.
5.Technical Basis in Engineering and Operations [NERC ROP] Each reliability standard shall be based upon sound engineering and operating judgment, analysis, or experience, as determined by expert practitioners in that particular field.	**13. Reduce Administrative Overhead**. Administrative documentation shall be kept to the minimum that is necessary
6. Completeness (NERC ROP) Reliability standards shall be complete and self-contained. The standards shall not depend on external information to determine the required level of performance.	**14. Priority.** Implementation plans for the Standards are prioritized according to level of BES impact.
7. Consequences for Non-Compliance [NERC ROP] In combination with guidelines for penalties and sanctions, as well as other ERO and regional entity compliance documents, the consequences of violating a standard are clearly presented to the entities responsible for complying with the standards.	**15. Eliminate or Minimize TFEs.** Security controls shall eliminate or at least minimize the need for TFEs. Allow for compensating controls to mitigate the need for a TFE.
8. Clear Language [NERC ROP] – Each reliability standard shall be stated using clear and unambiguous language. Responsible entities, using reasonable judgment and in keeping with good utility practices, are able to arrive at a consistent interpretation of the required performance.	

SECURITY CONTROLS SUB-TEAM
PROCESS AND DRAFTING GUIDANCE AND DELIVERABLES

Guidance from the January, 2010 Tucker Meeting and the February 2010 Austin Meeting

For the purpose of maintaining consistency across the teams and capturing interim decisions and change documentation, each team should utilize the following development process:

12. **DHS Catalogue of Controls:** Begin by identifying applicable controls that are enumerated in the *DHS Catalog of Control System Security Recommendations* for High Impact Cyber Systems.
13. **Cross Reference CIP Version 3 Requirements/sub-Requirements:** For each security control identified in step 1, cross reference the CIP version 3 Requirement/sub-Requirement or validate previous mapping work.
14. **Specific not Prescriptive:** As a general rule, be specific but not prescriptive in writing the requirements.
15. **"What" not "How":** In general, seek to draft a "what" requirements, not "how" requirements.
16. **Develop the requirement language** for each security control identified in step 1.
    a. When mapping to existing CIP requirements, use language from CIP, making improvements where needed.
    b. When no associated requirement from CIP exists, develop the new requirement using language from the *DHS Catalog*.
17. **Document significant changes to CIP Standards:** Document significant changes made to previous versions of the CIP Standards. Conceptual or broad changes can be captured by a single statement.
18. **Incorporate existing CIP requirements not mapped to the *DHS Catalog*.** If a requirement is no longer necessary because the intent was captured elsewhere, then include this in the change documentation.
19. **Address specific directives from FERC Order 706** that may be applicable to the requirement.
20. **Analysis and Determination of Requirements for Medium and Low Impact:** In the analysis and determination of applicability of requirements to Medium and Low Impact Cyber Systems, consider the cost in relation to the security benefits (i.e., a minimal cost requirement that significantly mitigates risk would apply to *ALL* Cyber Systems. Similarly, a significant cost requirement that minimally reduces risk or provides little additional security may apply only to *HIGH* impact Cyber Systems).
21. **Specify Applicability to Environments:** Specify applicability of a requirement to Generation, Transmission, and/or Control Center environments.
22. **Apply Requirements to BES Cyber System:** Requirements should apply to either:
    (a) The BES Cyber System as a whole, or
    (b) Components of the BES Cyber System. However, when a requirement only applies to specific types of components, Sub-Teams should describe those types of components to determine where component classes exist.
    (c) Requirements specific to boundary protection or ESP can be written to the interface of the BES Cyber System.

12: **Level of Requirements:** Sub-Teams should generally write the requirements at a high enough level to avoid applicability of specific technology. Where there are applicable CIP requirements, start with the CIP words and tweak if needed to include some DHS language/concept. However, the "level" of the requirements text should be raised, if needed.

Appendix # 6
CSO 706 SDT DRAFTING SUB-TEAMS

Additional members may be necessary for teams that have a large number of requirements or FERC directives allocated.

Sub-Team	NERC Standards and DHS Control Families	Team Members
Security Governance	CIP-003 – R1, R2, R3; CIP-005 R4, CIP-007 R8 DHS 2.1 Security Policy, DHS 2.2 Organizational Security, DHS 2.7 Strategic Planning, DHS 2.17 Monitoring and Reviewing Control System Security Policy, DHS 2.18 Risk Management and Assessment, DHS 2.19 Security Program Management	Jon Stanford (Lead), Jerry Freese, Dave Norton
CIP 002-4	Draft revisions to CIP-002-4, and Summary of Responses to Industry comments	John Lim, Dave Revill, Rich Kinas, Jim Brenton, Jackie Collett, Bill Winters, Dave Norton *Rod Hardiman (Observer)*
Personnel and Physical Security	CIP-004 – R1, R2, R3, CIP-006 R1 through R6 DHS 2.3 Personnel Security, DHS 2.11 Security Awareness and Training DHS 2.4 Physical and Environmental Security,	Doug Johnson(Lead), Rob Antonishen, Patrick Leon, Kevin Sherlin
Operations Security	CIP-005 R1, R3 CIP-007 R2, R3, R4, R6 DHS 2.8 System and Communication Protection DHS 2.14 System and Information Integrity	Jay Cribb (Lead), Jim Brenton, Jackie Collette, John Varnell
Recovery and Response	CIP-008 R1 & R2 CIP-009 R1 through R5 Incidence Response and Contingency Planning	Scott Rosenberger (Lead), Joe Doetzl, *Observer Participants: Jason Marshall*
Access Control and Auditing	CIP-003 R5; CIP-005 R2; CIP-007 R5; CIP 004 R4 DHS 2.15 Access Control DHS 2.16 Audit and Accountability	Sharon Edwards (Lead), Jeff Hoffman, Frank Kim *Observer Participants: Sam Merrell*
Change Management, System Lifecycle and Information Management	CIP-003 R6; CIP-007 R1, R7 CIP-003 R4; CIP-005 R5.1.1, R5.1.3 DHS 2.5 System and Services Acquisition, DHS 2.6 Configuration Management and System Lifecycle, DHS 2.10 System Development and Maintenance DHS 2.9 Information and Document Management, DHS 2.13 Media Protection	Keith Stouffer, Phil Huff (Lead) *Observer Participants: John Fridye*

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Agenda
Cyber Security Order 706 SDT — Project 2008-06

March 9, 2010 | 1 PM to 5:30 PM MST
March 10, 2010 | 8 AM to 5 PM MST
March 11, 2010 | 8 AM to 5 PM MST
March 12, 2010 | 8 AM to 12 PM MST

Arizona Public Service CHQ
400 N. 5th St.
Phoenix, AZ 85004

NOTE:
1. Agenda Times May be Adjusted as Needed during the Meeting
2. Drafting Team Meetings May Not Have Access to Telephones and Ready Talk

Proposed Meeting Objectives/Outcomes

- Review the revised CSO 706 SDT 2010 Work plan and Convergence Schedule Proposal
- Receive updates on other related cyber security initiatives
- Receive a NERC update on implementing the CIP Communication Plan and May 2010 Technical Workshop
- Review, discuss industry comments and identify issues raised to be addressed in revised CIP-002-4
- Review, refine and test consensus on a revised draft CIP 002-4 and Industry Response Document
- Receive progress reports for Security Controls Requirements Sub-Teams
- Develop and Test Sub-Team Security Controls Requirements
- Agree on next steps and assignments

Draft Agenda

Tuesday	**March 9, 2009**
1:00 p.m.	Welcome and Opening Remarks- *John Lim, Chair & Phil Huff, Vice Chair* Roll Call; NERC Antitrust Compliance Guidelines Facilitator review and SDT acceptance of February 16-19, 2010 Austin SDT meeting summary
1:10	Review of Meeting Objectives, Agenda and Meeting Guidelines- *Bob Jones*
1:15	Review and Discussion of CSO 706 SDT Workplan and Convergence Schedule - March-December, 2010- *Stu Langton*
1:45	Updates on other related cyber security initiatives- *NERC Staff and SDT Members*

1:55	Update on CIP Communication Plan and May 2010 Technical Workshop - *Carl Dombek*
2:15	Review of Revised CIP-002-4 Draft based on Industry and SDT Response to Industry Comments- *Draft CIP-002 Drafting Team, John Lim et al.*
3:00	*Break*
3:15	Continue review and discussion of revised draft CIP 002-4
5:25	Review of Proposal for Wednesday Agenda
5:30	*Recess*

- *Possible Security Controls Requirements Sub Team Meetings- Evening*
- *If needed, CIP-002 Drafting Team to meet to finalize draft and present for adoption Wednesday morning.*

Wednesday **March 10, 2010**

8:00	Welcome and Agenda Review, Roll Call and Antitrust Guidelines- *John Lim, Phil Huff, Joe Bucciero*
8:10	Review and Consideration of draft CIP-002-4 as revised and the Industry Comments Response Document
9:00	Sub-team Progress Reports and SDT Discussion of Key and Any Overlapping Issues

- Security Governance
- Personnel and Physical Security
- Operations Security
- Recovery and Response
- Access Control and Auditing
- Change Management, System Lifecycle and Information Management

10:30	Break
11:00	Review of Guidance and Overall Format for Security Controls Requirements Sub-teams
10:45	Sub-team Progress Reports and SDT Discussion of Key Issues- *Continued*
11:45	Security Controls Sub-Teams
12:00	*Working Lunch*
1:00	Security Controls Sub-Teams
4:55	Review Assignments and Thursday Agenda
5:00	*Recess*

- *Possible Security Controls Requirements Sub Team Meetings- Evening*

Thursday **March 11, 2010**

8:00	Welcome and Agenda Review, Roll Call and Antitrust Guidelines- *John Lim, Phil Huff, Joe Bucciero*
8:10	Security Controls Sub-Teams
10:00	Break
10:15	Security Controls Sub-Teams
12:00	*Working Lunch*
1:30	Sub-Team Reports and Full Team Consensus Testing on Refinements
3:00	Break
3:15	Sub-Team Reports and Full Team Consensus Testing on Refinements-*Continued*
4:45	Review Any Drafting Assignments and Friday Agenda

5:00	*Recess* ▪ *Possible Security Controls Requirements Sub Team Meetings- Evening*
Friday	**March 12, 2010**
8:00	Welcome and Agenda Review, Roll Call and Antitrust Guidelines- *John Lim, Phil Huff, Joe Bucciero*
8:10	Sub-Team Reports and Full Team Consensus Testing on Refinements-*Continued*
10:15	*Break*
10:30	Sub-Teams Reconvene to Review Refinements, Schedule and Assignments
11:00	Next Steps CIP 002 Drafting Group
11:15	Review of May 2010 Technical Workshop Planning and Preparation
11:45	Review and Agree on Next Steps and Meeting Evaluation
12:00	*Adjourn & Lunch*

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

PROJECT 2008-06 CYBER SECURITY ORDER 706 SDT MEMBERS

1. Rob Antonishen	Ontario Power Generation
2. Jim Brenton	ERCOT
3. Jackie Collett	Manitoba Hydro
4. Jay S. Cribb	Information Security Analyst, Southern Company Services
5. Joe Doetzl	Manager, Information Security, Kansas City Pwr. & Light Co.
6. Sharon Edwards	Duke Energy
7. Gerald S. Freese	Director, Enterprise Info. Security America Electric Pwr.
8. Jeff Hoffman	U.S. Bureau of Reclamation, Denver
9. **Phillip Huff, Vice Chair**	Arkansas Electric Coop Corporation
10. Doug Johnson	Exelon Corporation – Commonwealth Edison
11. Frank Kim	Ontario Hydro
12. Rich Kinas	Orlando Utilities Commission
13. Patricio Leon Alvarado	Southern California Edison
14. John Lim, Chair	CISSP, Department Manager, Consolidated Edison Co. NY
15. David Norton	Entergy
16. David S. Revill	Georgia Transmission Corporation
17. Scott Rosenberger	Luminant
18. Kevin Sherlin	Sacramento Municipal Utility District
19. Jonathan Stanford	Bonneville Power Administration
20.Keith Stouffer	National Institute of Standards & Technology
21. John D. Varnell	Technology Director, Tenaska Power Services Co.
22. William Winters	Arizona Public Service, Inc.
Roger Lampila	NERC
Scott Mix	NERC
Dave Taylor	NERC
Howard Gugel	NERC
Joe Bucciero	NERC/Bucciero Consulting, LLC
Robert Jones	FSU/FCRC Consensus Center
Hal Beardal	FSU/FCRC Consensus Center
Stuart Langton	FSU/FCRC Consensus Center

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

CSO 706 SDT MEETING SCHEDULE- CONVERGENCE PROPOSAL
APRIL –DECEMBER 2010 *(To be discussed on Tuesday)*

Schedule Convergence: Full CIP V4 Package (*Feb. 27, 2010)*		
Date	**Week of**	**CIP Task**
SDT Meeting- Atlanta (4-13-16)	4/12/2010	Present Controls draft for full team review and comment. Sub team drafting. Finalize draft for Informal Comment, Full Package
4/20/2010	4/19/2010	*Informal Comment Posting for full package starts*
~~*5/1/2010*~~ *5/3/2010*	*4/26/2010*	~~*Informal Comment Posting for full package starts*~~ *Webinar*
SDT Meeting- Dallas, (5-11-14)	5/10/2010	
	5/17/2010	Technical Workshop??
	5/24/2010	
6/4/2010	*5/31/2010*	*2nd Informal comment period ends*
SDT Meeting, Sacramento (6-8-11)	6/7/2010	SDT Meeting: Comment review, response process, drafting
	6/14/2010	Sub team meetings
	6/21/2010	Sub team meetings
	6/28/2010	Sub team meetings. SDT interim online meeting.
	7/5/2010	Candidate responses, package modifications to SDT
SDT Meeting, TBD, 7-13-16	7/12/2010	Finalize posting for 45 day formal comment period
~~*7/22/2010*~~	*7/19/2010*	~~*45 Day formal comment period starts/Ballot Pool formation*~~ *NERC Prepares Materials/Seeks SC Approval*
7/26/2010	7/26/2010	*45 Day formal comment period starts/Ballot Pool formation*
	8/2/2010	
SDT Meeting, TBD, (8-10-13)	8/9/2010	SDT Meeting

	8/16/2010	
8/24/2010	8/23/2010	*30 Ballot Preview/Initial Comment Preview ends*
8/31/2010	*8/30/2010*	~~*Formal Comment Period/Ballot ends*~~ *Initial Ballot Starts*
SDT Meeting TBD, 9-7-10	9/6/2010	Respond to comments. Drafting.
	9/9/2010	Initial Ballot Ends
	9/13/2010	Sub team meetings
	9/20/2010	Sub team meetings
	9/27/2010	Sub team meetings. Full SDT on-line meeting
	10/4/2010	Sub team meetings
SDT Meeting TBD, 10-12-15	10/11/2010	Finalize responses and 2nd ballot version (NERC staff expects to start work on posting candidate on 10/12??)
~~*10/20/2010*~~ *10/19/2010*	*10/18/2010*	*2nd ballot starts*
~~10/30/2010~~ 10/29/2010	10/25/2010	*2nd ballot ends*
	11/1/2010	Compile comments - On-line meetings
	11/8/2010	~~Compile comments - On-line meetings~~
SDT Meeting TBD, 11-16-19	11/15/2010	Respond to comments/Draft 3rd Ballot Postings
	11/22/2010	~~*Finalize Posting version for 3rd Ballot - On-line meetings*~~ *NERC finalizes ballot package*
11/24/2010		*3rd Ballot Begins*
~~*11/30/2010*~~	*11/29/2010*	~~*3rd Ballot Begins*~~
~~*12/10/2010*~~ *12/6/2010*	*12/6/2010*	*3rd Ballot Ends*
SDT Meeting TBD, 12-13-17	12/13/2010	SDT Meeting
	~~*12/20/2010*~~ *12/28/2010*	*Submit for Regulatory Approval*

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

CSO 706 SDT WORKPLAN TO DATE
OCTOBER, 2008 –DECEMBER 2010

DEVELOPMENT OF CIP VERSION 2 AND NEW VERSION FRAMEWORK
OCTOBER 2008–JULY 2009

1. October 6–7, 2008 — Gaithersburg, MD Reviewed CIP-002-CIP-009, Agreed on Version 2 approach.
2. October 20–21 —Sacramento, CA CIP-002-CIP-009 Version 2 development
3. November 12–14, 2008 — Little Rock, AR CIP-002-CIP-009 Version 2 adoption for comment and balloting; CIP-002-CIP-009 New Version process reviewed.
4. December 4–5, 2008 — Washington D.C. CIP-002-CIP-009 Version 3 reviewed and debated, SDT member white "working" papers assigned, Technical Feasibility Exceptions white paper reviewed and refined.
5. January 7–9 — Phoenix, AZ, Reviewed Technical Feasibility Exceptions white paper**,** reviewed industry comments on CIP-002-CIP-009 Version 2 products — established small groups to draft responses, reviewed New Version white "working" papers.
January 15 — WebEx meeting(s) Small group drafted responses to industry Version 2 comments.
January 21 — WebEx meeting(s) Small group drafted responses to industry Version 2 comments.
6. February 2–4, 2009 — Phoenix, AZ Update on NERC Technical Feasibility Exceptions process**,** VSL process and SDT role**,** review of Version 3 White papers, strawman and principles**,** reviewed and adopted SDT responses to industry comments on Version 2 and Version 2 Product Revisions.
7. February 18–19, 2009 — Fairfax, VA Update on Version 2 process**,** NERC TFE process and VSL Team process; reviewed, discussed and refined Version 3 CIP-002 White papers, strawman, and principles.
8. March 10–11, 2009 — Orlando, FL Update on NERC TFE and VSL and VRF Team process and review and refine Version 3 CIP-002 Strawman Proposals
March 2–April 1, 2009 — 30-day Pre Ballot
Mid-March — NERC posts TFE draft Rules of Procedure for industry comment
March 30, 2009 — WebEx meeting(s) White Paper Drafting Team
April 1–10 — NERC Balloting on Version 2 Products
April 6, 2009 — WebEx meeting — White Paper Drafting Team
April 8, 2009 — WebEx meeting(s) — White Paper Preview- Full SDT Conference Call
April 11, 2009 — Version 2 Ballot Results (Quorum: 91.90% Approval: 84.06%) and Industry Comments
9. April 14–16, 2009 — Charlotte NC Update on NERC TFE process, VSL Team process and NERC Critical Assets Survey; agreed and adopted responses for Version 2 industry comments for recirculation ballot; reviewed and refined Version 3 whitepaper and consensus points and progress report to NERC Member Representative Committee (MRC) May meeting.
April 28 and May 6, 2009 — White Paper Drafting Team Meetings and WebEx
April 17–27, 2009 — Recirculation Results: Quorum: 94.37% Approval: 88.32%
May 5, 2009 — NERC MRC Meeting, Arlington, VA- SDT progress report.
10. May 13–14, 2009 — Boulder City NV Reviewed MRC presentation and further SDT refinement and discussion of the Version 3 White Paper.
June 8 and June 15, 2009 — Working Paper Drafting Team Meetings and WebEx
11. June 17–18, 2009 — Portland OR Further SDT refinement of the draft CIP Version 3 Working Paper(s), reviewed SDT development process for June-December 2009; discussed potential SDT subcommittee structure and deliverables.

- *June — WebEx meeting(s)*
- *Working Paper drafting group sessions including inputs from selected industry personnel to help establish BES categorization criteria*

CIP-002 DEVELOPMENT OF REQUIREMENTS, MEASURES, ETC. JULY-DECEMBER 2009

12. July 13–14, 2009 in Vancouver, B.C., Canada

SDT reviewed, refined, and adopted SDT Working Paper. SDT adopted its response to NERC for Interpretation of CIP-006-1. SDT reviewed and adopted a proposal for CIP-002 Subgroups and Deliverables and convened subgroup organizational meetings to develop work plans. SDT adopted 2010 Meeting Schedule.

- *July–August Interim Conference call meeting(s)*
- *CIP-002 Subgroup meetings*
- *CIP-002 Coordination Team meeting*
- *August 3–5, 2009 in Winnipeg, Manitoba* ***NERC Member Representative Committee****. Progress Report and presentation on new CIP Version 3 Working Paper-Concept- Reliability Standards on Cyber Security for MRC input.*

13. August 20–21, 2009 in Charlotte, NC. SDT reviewed and responded to MRC input on Working Paper/CIP-002 Concepts and convened SDT Subgroup and plenary meetings to develop CIP-002 requirements and "proof of concept" control (s).

- *July–September — 45-day Industry Comment Period on CIP-002 Concept Working Paper*
- *NERC Webinar- August–September Interim Conference Call meeting(s)*
- *CIP-002 Subgroup meetings (as ne*
- *CIP-002 Coordination Team meeting*

14. September 9–10, 2009 in Folsom, CA. SDT reviewed and considered industry comments on the Working Paper and CIP-002 concepts and their application to the subgroup work and addressed coordinating issues through joint subgroup meetings. SDT agreed on meeting dates and proposed locations for January–December 2010

September–October Interim WebEx meeting(s)

- *FERC Version 3 Urgent Action SDT conference call meetings*
- *CIP-002 Coordination Team meeting*

CIP VERSION 3 RESPONSE TO FERC ORDER, OCTOBER-DECEMBER, 2009

15. October 20–22, 2009 in Kansas City, MI. Reviewed new FERC Order and urgent action CIP Version 3 process; discussed key issues raised by SDT CIP 002 Subgroups, small group meetings and agreement on refinements to the CIP 002-009 schedule and drafting process for CIP 002-4.

- *October–November Drafting Team meeting(s)*
- *CIP-002 Coordination Team meeting*

16. November 16–19, 2009 in Orlando, FL

- SDT review, refine and adopt Version 3 "industry response" document.
- SDT plenary and drafting group session(s) — to draft, review and refine CIP-002-4 standard, requirements, measures and controls and related documents.
- November–December Interim Conference call meeting(s)
- Drafting teams as needed to finalize draft CIP 002-4 documents
- CIP-002 Coordination Team meeting
- *CIP 002-4 Drafting Team produces next draft based on Orlando Meeting input.*
- *December 2 CSO 706 SDT Version 3 Consideration of Comments Draft Conference Call*
- *December X, CSO 706 SDT CIP 002-4 Preview Conference Call*

17. December 15–16, 2009 in Little Rock AK

- SDT scenario "walk through" to test flow of CIP 002-4.
- SDT plenary and drafting group session(s) to review, refine, and agree on and adopt CIP-002-4 standard, requirements, measures and controls and related documents.
- Agree on initial posting of draft CIP-002-4 for industry review and comment.
- Agree on next steps and 2010 Workplan and schedule

CIP Version 3 Key Steps/Schedule

1. *Post for Industry Comment 10-13-09 to 11-12-09*
2. **November 13 SDT Conference Call- Review of Industry Comments and Response**

3. **November 16, SDT 706 Meeting in Orlando, Monday, 5:00 p.m.- through dinner- SDT 706 Response Document to Industry Comments**
4. **November 17**, Tuesday, SDT 706 Meeting, Orlando, Complete and Adopt Industry Response Document.
5. **November 18**, Wednesday, Post Response Document and Ballot
6. **November 27**, Friday *(after Thanksgiving)* Deadline for Votes and Comments
7. **November 30, Monday, SDT 706 - Conference Call- finalize Industry Response document.**
8. **December 1- 10,** Recirculation Ballot.
9. **December 11,** BoT Approval
10. **December 29, 2009,** FERC Filing

CIP 002-4 Key Steps/Schedule (October-December 2009)

1. **November 1:** Jackie Collett, Phil Huff, John Lim and John Varnell, the chairs of the 4 CIP 002 Subgroups will form the CIP 002 Strawman Drafting Group (SDG).
2. **November 1:** All CIP 002 "meta groups" and subgroups will forward to the Strawman Drafting Group their standards text drafts including any guidance language**.**
3. Joe Doetzl will coordinate the work of the Controls Drafting Group (CDG) members: Jim Brenton, Keith Stouffer, Bill Winters, Jon Stanford. They will produce several recommended sample controls to illustrate high/medium/low concepts in CIP 002 as well as recommendations on whether the SDT should request guidance from the Standards Committee on referencing a 'catalogue of security requirements', for circulation to the SDT **by Friday, November 13, 2009**.
4. The SDG will prepare a strawman draft by **November 13, 2009** for review by the SDT in advance of November 16-19, 2009 SDT meeting.
5. The SDT will utilize the strawman draft to organize its **November 16-19 meeting** and determine at the conclusion of the meeting if the SDT will continue to aim for the December adoption of CIP 002 draft on **December 16** for posting for industry comment.
6. The SDG and the CDG will present their 2nd drafts at a SDT conference call the **first week in December**.
7. The SDT will refine and circulate a strawman Draft #3 prior to the **December 15-16** SDT 706 meeting in Little Rock.
8. **December 15-16** will refine, finalize and adopt the CIP 002 posting for the industry.

- December 28, 2009 SDT Conference Call on CIP 002-4
- December 30, 2009 SDT Leadership Call- Security Controls Survey Draft
- January 6, 2010, SDT Conference Call- Review Security Controls Draft Principles and Schedule and Appoint Drafting Team to bring strawman to January SDT Meeting in Tucker.

CSO SDT 706 2010 MEETING SCHEDULE

18. January 19–22 — Tuesday-- Friday, Tucker, GA (GTC)	24. July 13–16, Tuesday-–Friday, Pittsburgh, PA (CERT)
19. February 16-19 Tuesday–Friday, Austin TX (ERCOT)	25. August 10--13, Tuesday—Friday, TBD
20. March 9–12 — Tuesday–Friday, Phoenix, AZ (APS)	26. September 7–10, Tuesday—Friday, Winnipeg, Canada
21. April 13–16 — Tuesday-Friday, Atlanta GA (SouthernCo)	27. Oct. 12–15, Tuesday-Friday, TBD
22. May 11-14 — Tuesday-Friday, Dallas TX (Luminant)	28. November 16–19, Tuesday-Friday, TBD
23. June 8–11 — Tuesday-Friday, Sacramento CA (SMUD)	29. December 14–17, Tuesday-Friday, TBD

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Notes

Cyber Security Order 706 SDT — Project 2008-06

March 9, 2010 I 1 PM to 5 PM EDT
March 10, 2010 | 8 AM to 5 PM EDT
March 11, 2010 | 8 AM to 5 PM EDT
March 12, 2010 | 8 AM to 1 PM EDT

Robert Jones, Stuart Langton, and Hal Beardall
Facilitation and Meeting Design
FCRC Consensus Center, Florida State University

Joe Bucciero, Bucciero Consulting, LLC

http://www.nerc.com/filez/standards/Project_2008-06_Cyber_Security.html

116-390 Village Blvd.
Princeton, NJ 08540
609.452.8060 | www.nerc.com

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

CSO706 SDT March 9-12, 2010 Meeting Summary Contents

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

CSO706 SDT MARCH 9-12, 2010 MEETING
EXECUTIVE SUMMARY

On Tuesday afternoon, the Chair, John Lim welcomed the members and Joe Bucciero conducted a roll call of members and participants in the room and on the conference call. The host Bill Winters, a SDT member, welcomed everyone to the facilities and covered logistics. The Chair reviewed the meeting objectives and Bob Jones, facilitator, reviewed the proposed meeting agenda. On Friday morning the SDT approved without objection the meeting summary for the February, 2010 SDT session in Austin Texas. Mr. Bucciero reviewed the need to comply with NERC's Antitrust Guidelines.

He suggested the Team was at a crossroads in terms of getting some of our product out to the industry and getting beyond conceptual discussions. He noted we need to have complete draft CIP package at the end of our April Meeting for posting for informal comment in early May. He suggested the focus needed to be on getting things done and that once the SDT has agreed then it needed to move forward and not revisit previous discussions.

Stu Langton presented a proposed CSO 706 SDT schedule which was circulated within a day of the meeting and made adjustments in the process to allow for NERC reviews and formatting of materials. On day two, Stu Langton reviewed the SDT schedule sent out yesterday from Scott Mix. He noted that this is our 20th meeting over past eighteen months and the SDT has faced four core challenges:

- Over 200 items in 706;
- High visibility issue in the industry and Congress;
- Large team formed in effort to represent points of view of the industry; and
- Two different cultures addressing cyber security-- engineering/production backgrounds and engineering/cyber security backgrounds.

John Lim introduced Carl Dombek the new NERC communications director and asked him for a progress report on the communication plan for the drafting team activities and drafting of the standards.

On Wednesday, Howard Gugel, NERC, presented an overview with guidance for the Team on drafting standards and requirements which he and Maureen prepared. He noted the overall move towards performance based standards and described the general process for writing a standard. He suggested starting with the end in mind and FERC's criteria for approval:

- Achieves a specified reliability goal,
- Is applicable to all regions and entities, and

- Considers costs but not at expense of reliability.

It is important for the Team to build consensus at every step. As the Team has experienced first hand this is most difficult to develop at the concepts and assumptions level first, before addressing the drafting of requirements, then measures and compliance element.

John Lim provided a progress report on the Subteam's work since Austin noting that Dave Revill has worked on a strawman set of requirements to work with using criteria posted as a starting point. Jackie has done some more work on Attachment #2. John reviewed with the Team the following issues the CIP 002 Sub-team has been grappling with:

- Definitions
- Drafting Language
- Control room vs. control center.
- Legacy.
- Multiple facilities.
- Control system.
- Added 4.1.10 Distribution Provider (with qualification)

Dave Revill presented the concept of breaking requirements into two components:
1.1 Uniquely identify and document assets
1.2 Identify types of data communication into five technologies: routable, non-routable, dial-up, serial or not networked
- Definitions build on the attachment
- Created matrix using the five categories of communication technology including:
- And assigned high-medium-low as compared with BES impact rating

John Lim then presented an overview of the approach taken in the attachments and the SDT discussed the following issues:
- Real Time
- Audits, Standards and Guidance
- Functions.
- Disturbance to the BES.
- Addressing Industry Comments.

During the course of the first day's discussion a number of issues were noted in a "parking lot" for sub-teams to return to. Based on a review of the parking lot issues, the Team agreed to the following drafting assignments over night:
- Control System – Produce a list of examples
- Matrix Group – "connected/not connected"
- Real Time Operation/Cyber System affecting "immediate impact"

- Attachment 2 – guidance, matrix

The drafting groups then reported back to the SDT on Wednesday morning. Following their reports the SDT tested the level of support for the following guidance for the CIP 002 sub-team

1. Redraft CIP-002 to remove the connectivity options and handle them in the controls
   Y= 15 N = 5
2. Keep CIP-002 as drafted yesterday and let cip-002 sub-team handle modifications to the matrix (Austin)
   Y= 4 N= 16

The Team acknowledged they may need to revisit if in developing controls we find we cannot address the connectivity issue.

John Lim reported on Thursday the Sub-Team's efforts. On Friday the Sub-team reported on the changes made to the requirements and attachments.

- BES Cyber System definition
- Control Center
- Terms to be retired from the *Reliability Standards Glossary of Terms* once the standards that use those terms are replaced: Critical Assets; Critical Cyber Assets; Cyber Assets.
- The inclusion of Distribution Provider remains an open issue.
- "Multiple locations" definition- concerns whether it is needed?
- "Cyber security definition"?
- Distribution provider?
- R1-3. If 2 requirements
- Attachment #1 included a list of functions which the SDT reviewed and suggested refinements
- Attachment #2 provided a draft list of high, medium and low impact ratings which the SDT reviewed and suggested refinements.

On Wednesday the Sub-teams presented brief status reports before breaking into sub-team meetings. On Thursday each Sub-Team presented their draft requirements.

Personnel and Physical Security	CIP-004 – R1, R2, R3, CIP-006 R1 through R6 DHS 2.3 Personnel Security, DHS 2.11 Security Awareness and Training DHS 2.4 Physical and Environmental Security,	Doug Johnson(Lead), Rob Antonishen, Patrick Leon, Kevin Sherlin

The Sub-Team report was delivered by Doug Johnson and covered drafting on the following areas:

- Personnel
- Awareness programs
- Training
- Personnel Risk Assessment
- Physical
- Physical Security Plan
- Physical Access Control
- Monitoring Physical Access
- Logging
- Visitor Control Program
- Maintenance and Testing
- Protection of Electronic Access Control Systems

Recovery and Response	CIP-008 R1 & R2 CIP-009 R1 through R5 Incidence Response and Contingency Planning	Scott Rosenberger (Lead), Joe Doetzl,

Scott Rosenberger reported on the Sub-team's progress reviewing draft language covering:

- Response
- Recovery Plans CIP 009
- DHS New Requirements

Access Control and Auditing	CIP-003 R5; CIP-005 R2; CIP-007 R5; CIP 004 R4 DHS 2.15 Access Control DHS 2.16 Audit and Accountability	Sharon Edwards (Lead), Jeff Hoffman, Frank Kim *Observer Participants: Sam Merrell*

Sharon Edwards reported on the Sub-team's work including update on work, future tasks for the sub-team and areas of coordination with other Sub-teams.

Change Management, System Lifecycle and Information Management	CIP-003 R6; CIP-007 R1, R7 CIP-003 R4; CIP-005 R5.1.1, R5.1.3 DHS 2.5 System and Services Acquisition, DHS 2.6 Configuration Management and System Lifecycle, DHS 2.10 System Development and Maintenance DHS 2.9 Information and Document Management, DHS 2.13 Media Protection	Keith Stouffer, Dave Revill, Phil Huff (Lead) *Observer Participants: John Fridye*

Phil Huff reported on the Sub-Team's work reviewing the Change Management requirements worksheet. He noted that the Sub-team's work focused on the language itself, not on applicability. They still have to go through FERC order review. The have modified table/worksheet to track open issues/complications. They now have drafted most of the objectives and changes to CIP language and covered:

- Baseline Configuration
- Configuration control
- Access restrictions for configuration changes.
- Configuration assets-
- Information Protection
- Protection Program.
- Maintenance
- Media protection CIP 7 R7-

Operations Security	CIP-005 R1, R3 CIP-007 R2, R3, R4, R6 DHS 2.8 System and Communication Protection DHS 2.14 System and Information Integrity	Jay Cribb (Lead), Jim Brenton, Jackie Collette, John Varnell

Jay Cribb reported on this group's effort covering:

- Boundary Protection/ESP
- Electronic Access Monitoring.
- Communications Integrity
- Remote and Accessible Services (Port and Services)
- Flaw Remediation (i.e. DHS for Patch Management)
- Malicious Software Prevention.

Security Governance	CIP-003 – R1, R2, R3; CIP-005 R4, CIP-007 R8 DHS 2.1 Security Policy, DHS 2.2 Organizational Security, DHS 2.7 Strategic Planning, DHS 2.17 Monitoring and Reviewing Control System Security Policy, DHS 2.18 Risk Management and Assessment, DHS 2.19 Security Program Management	Jon Stanford (Lead), Jerry Freese, Dave Norton

Jon Stanford reported on the Sub-Team's work reviewing the Requirements Worksheet. He noted that the right hand side includes the current CIP and covered:

- Security Policy and Procedures
- Control System Security Plan
- Security Plan Update
- Control System Connections
- Vulnerability Assessment and Awareness.

The SDT reviewed the plans for the May 2010 Technical Workshop including Gerry Adamski's email. Gerry Adamski has offered to be the "general facilitator" for the workshop.

The Chair and Vice Chair noted that the Team had made a lot of progress over the course of the meeting. They reviewed the short term schedule for the Sub-teams. They will be meeting weekly as will the Sub-Team Leads to help coordinate the development of the drafts. There is a lot of work to complete. Sub-teams may be scheduling additional working sessions and coordinating with Joe Bucierro. The SDT needs to enter its April meeting with a good draft
Sub-team should use Howard Gugel early and often.

The SDT requested that Friday sessions should clearly note if noon is the adjournment time so that members can make travel arrangements accordingly.

The Chair and Vice Chair and the SDT thanked Bill Winters for his excellent hosting and great facilities. Bill offered to host later in the year and will follow up with Joe Bucciero.

The meeting adjourned at 12:15 p.m.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

CSO 706 SDT MARCH 9-12, 2010
PHOENIX, ARIZONA

MEETING SUMMARY

I. AGENDA REVIEW, WORKPLAN, UPDATES AND COMMUNICATION PLAN

A. Agenda Review

On Tuesday afternoon, the Chair, John Lim welcomed the members to the SDT's 20th meeting noting the Vice Chair Phil Huff would join the meeting on Wednesday morning. Joe Bucciero conducted a roll call of members and participants in the room and on the conference call *(See appendix #2*). The host Bill Winters, a SDT member, welcomed everyone to the facilities and covered logistics. The Chair reviewed the following meeting objectives:

- Review the revised CSO 706 SDT 2010 Work plan and Convergence Schedule Proposal
- Receive updates on other related cyber security initiatives
- Receive a NERC update on implementing the CIP Communication Plan and May 2010 Technical Workshop
- Review, discuss industry comments and identify issues raised to be addressed in revised CIP-002-4
- Review, refine and test consensus on a revised draft CIP 002-4 and Industry Response Document
- Receive progress reports for Security Controls Requirements Sub-Teams
- Develop and Test Sub-Team Security Controls Requirements
- Agree on next steps and assignments

He suggested the Team was at a crossroads in terms of getting some of our product out to the industry and getting beyond conceptual discussions. He noted we need to have complete draft CIP package at the end of our April Meeting for posting for informal comment in early May. He suggested the focus needed to be on getting things done and that once the SDT has agreed then it needed to move forward and not revisit previous discussions.

Bob Jones, facilitator, reviewed the proposed meeting agenda *(See appendix #1*). On Thursday morning the SDT approved without objection the meeting summary for the February 16-19, 2010 SDT session in Austin, Texas.

Mr. Bucciero reviewed the need to comply with NERC's Antitrust Guidelines *(See*

Appendix #3). He urged the team and other participants in the process to carefully review the guidelines as they would cover all participants and observers. He urged all to avoid behaviors or appearance that would be anti-competitive nature and also reminded the group of the sensitive nature of the information under discussion.

B. Workplan Schedule Review

Stu Langton presented a proposed CSO 706 SDT schedule which was circulated within a day of the meeting and made adjustments in the process to allow for NERC reviews and formatting of materials. Joe Bucierro suggested the SDT might want to review this overnight and take up first thing on Wednesday morning.

On day two, Stu Langton reviewed the SDT schedule sent out yesterday from Scott Mix He noted that this is our 20th meeting over past eighteen months. The SDT has faced four core challenges:

- Over 200 items in 706;
- High visibility issue in the industry and Congress;
- Large team formed in effort to represent points of view of the industry; and
- Two different cultures addressing cyber security-- engineering/production backgrounds and engineering/cyber security backgrounds.

The SDT handled initially the TFEs. In Fall of 2009 the SDT responded to a FERC ninety day order. The SDT experienced a change in leadership and a 25% change in team membership. The SDT has experienced high pressure to shorten the schedule and work more intensely. We added an additional day to most of our 2010 meetings. The SDT has gotten CIP versions 1 and 2 out to industry and broadly accepted and have continued to meet deadlines successfully. The SDT has developed meeting protocols that let members speak and also observers which can be frustrating as we try to afford airtime for everyone. The Team recognizes that we have been asked to address potentially significant changes for the industry. The team has created straw documents which we have been able to respond to a make progress and has developed good quality products. We have used small drafting groups and polling and consensus testing to help group move forward. We get knocked off pace when members feel a the need to offer illustrative examples in order to test concepts that often are tied to particular views or narrow areas of operation. We occasionally get bogged down with disagreements and differences. The key has been to offer improvements not just challenges as we have key deadlines we must meet.

Scott Mix and Joe Bucierro reviewed a schedule Gant chart and Joe's is a matrix for comparison – both are very helpful and provide a game plan that may have to be adapted to respond to additional changes and challenges. Between now and next meeting is important challenge to getting the first draft done. The proposed process involves five key steps:

1. Informal comment period of thirty days for industry to review in May-June, 2010.
2. Formal 45 comment period from July 26 to mid-September.
3. Followed by up to three ballots of ten days each
4. A NERC board decision in December to adopt the new CIP; and
5. Send to FERC by end of December.

Our next meeting is on April 13-16 in Atlanta where we will adopt a draft for industry comment which will then be posted on May 3. We will meet 5/11-14 in Dallas to develop guidance documents and prepare for the Industry workshop the following week in Dallas. On June 8-11 we will review comments on first draft from the industry and the workshop and refine the CIP. On July 13-16 we will finalize and approve documents for posting for formal comment period. This new schedule builds in time for NERC review and work followed by drafting team approval. This schedule will be made available as part of the meeting summary – has already been sent out to the list and includes two webinars as part of communication plan to the industry. The Technical workshop is part of the process for collecting comments as part of informal comment periods. Any comments received during member presentations to key groups should be consistently requesting comments in writing so we do not have to respond to those from memory. The official record needs written comments to capture.

C. Communication Plan

John Lim introduced Carl Dombek the new NERC communications director and asked him for a progress report on the communication plan for the drafting team activities and drafting of the standards. He thanked the Chair for the introduction and noted there would be a broad spectrum of materials and opportunities to consider. They are planning to brief reporters from the various trade dailies bringing them up to speed on purpose of a performance based system. There would need to be more communication to particular groups to make them aware of webinars, perhaps more targeted advisories as opposed to general notices – impressing on them the importance of participating in the process.

SDT Member Comments

- Workshop – any planning for it? Want to do it in mid May – technical workshop to follow the filing in early May to clarify questions and develop better understanding
- Should it be in conjunction with Board of Trustees meeting? Or separate event?
- The Team is proposing a separate event the week of May 17.
- Carl will get with Gerry Adamski to review details and explore new ways of getting participation.
- Where should the workshop venue be? Washington? He suggested it may depend on the number of people attending and he offered to look into that and suggested discussing the specifics offline.

D. Standards Drafting 101

On Wednesday, Howard Gugel, NERC, presented an overview with guidance for the Team on drafting standards and requirements which he and Maureen prepared. He noted the overall move towards performance based standards and described the general process for writing a standard. He suggested starting with the end in mind and FERC's criteria for approval:

- Achieves a specified reliability goal,
- Is applicable to all regions and entities, and
- Considers costs but not at expense of reliability.

It is important for the Team to build consensus at every step. As the Team has experienced first hand this is most difficult to develop at the concepts and assumptions level first, before addressing the drafting of requirements, then measures and compliance element.

SDT Discussion

- What happened to measures – are they going away? Not yet.
- How much leeway does group have to set zero based risk factors? VSLs and VFRs are filed separately, not as part of standard itself.
- Will we have the ability to pick the thresholds? Team will draft those for industry comment, it will be part of the record but not technically part of the ballot, and will be filed separately.
- Industry does not understand that VSLs and VFRs are filed separately.
- In the example rewrite, where does updating the documentation fit? As part of R1 sub-part 3 or as R2?
- Why have update if you are required to have documentation – doesn't that include updating?
- Could we say "continually" document? Then there would have to be an interpretation of "continually"
- The less we leave room for interpretation the better off we will be for purposes of auditing.
- Careful in our requirements that we do not cross the line into the how to do it.
- The audit model we will use seems to assume we are guilty until we can prove our innocence through documentation in the audit process.

II. REVIEW OF REFINEMENTS OF CIP-002-4

A. Initial Review of CIP-002-4

John Lim provided a progress report on the Subteam's work since Austin (*Dave Revill, Rich Kinas, Jim Brenton, Jackie Collett, Bill Winters, Dave Norton) Rod Hardiman*

(Observer) They met two times last week. Dave Revill has worked on a strawman for us to use and has developed a good set of requirements to work with using criteria posted as a starting point. Jackie has done some more work on those. Rich Kinas is working on the comments – will use the discussion of the team from last meeting.

He reviewed with the Team the following issues the CIP 002 Sub-team has been grappling with:

- **Definitions**
- Definitions of BES cyber system?
- What is meant by "Misuse"? Throw it into the list of things that can cause harm to the system?
- What is compromised if not misused? Just adding to be sure the link between the two is understood by all – 706 said to put misuse into the categorization.
- Do we need a definition of what we are going to protect in order to develop criteria – if we are not going to do that, why don't we create a list of implementation scenarios and work back toward a definition as opposed to tweaking a definition by finding exceptions – work it in the opposite direction – we have a definition that does not work.
- need operations folk to take the lead because they know how it works
- if bright lines need definitions, then figure out the situations it will be applied
- letting impact of generation facility meet the definition because of the impact it has
- **Drafting Language**
- "such as" – in a standard is this inclusive, illustrative or what as a guideline? "Such as" is repetitive and redundant – suggest dropping
- **Control room vs. control center.**
- Control center concept may be going the way of the dinosaur but it is not quite there yet.
- Also control room versus control center – the latter includes the operators – we went to one room.
- Replace center with system which can be in one or multiple places?
- Trying to resolve conflict between geography and functions.
- **Legacy.** How do we deal with "legacy" and the need to move forward and assure the spectrum of needs are protected?
- This is not part of the standard.
- Currently using as an example – but what is in the glossary makes a huge difference on compliance – need to be sure we know and the auditors know what it means and agree on that definition
- **Multiple facilities.** Point to the highlighted additions as added since the last comment period: "multiple locations" and "Real Time"
- "Multiple facilities" and "multiple locations" keeps it from being limited to one site or single generation issue.

- We dropped the location concept in the requirements because it was too easy to get wrapped around the axle.
- Need to be sure we don't get caught with unintended consequences.
- **Control system.** just calling it a control system doesn't cover the need
- do we need this. If we do, should we add "digital control system"?
- it is needed because we have a bright line criteria that addresses this issue
- "binary" not just digital
- Modified guidelines on alarm monitoring to focus on power operations
- Most generator systems have a fire suppression system
- That is fire that impacts operations or restoration functions – that fits operational concept

Added 4.1.10 Distribution Provider (with qualification) –

- Need to clarify what is included in bulk provider definition
- "with BES assets" instead of "qualification" would clarify
- tie to regional reliability organization or its equivalent – existing standards already have appropriate language – see PRC-8 and PRC-10 – to replace language above

5.1

- Take out the parenthetical marks and include the language
- Disclaimer of other group working on defining what is under NERC jurisdiction
- Does "Facility" need to be capitalized? Yes, it is in the NERC Glossary
- is there a separate plan for covering nuclear facilities?
- We have to have an implementation plan for version 3 – still working on developing version 4 for filing at end of December and it must include implementation schedule for everything under NERC jurisdiction

Dave Revill presented the concept of breaking requirements into two components:

1.3 Uniquely identify and document assets

1.4 Identify types of data communication into five technologies: routable, non-routable, dial-up, serial or not networked

- Definitions build on the attachment
- Created matrix using the five categories of communication technology including:
- And assigned high-medium-low as compared with BES impact rating

SDT Discussion

- Why is serial called out specifically? Is it captured by non-routable?
- Do we consider it legacy? It is different from non-routable – actually it is included
- Do we need to call out wireless as a separate family?
- Do not apply the same controls to legacy serial as other non-routable – that is why it is called out
- Mixing topology and protocol – our attempt at creating bright lines may be in trouble –

- I am interested in protecting interconnected systems regardless of the protocols
- Routable at the top because it is the most vulnerable – what are we including in the non-routable?
- Legacy protocols were not point to point, they were multi-drop?
- We will have three sets of controls – there is another dimension for environment – is there a third dimension too?
- Original idea --across the top was if I get to it how much damage can I create and the down the side was how easy is it to reach (connectivity) – not getting into the transport
- We may be digging ourselves deeper into controls – need to keep this separate from the requirements.
- How can you use the cyber system to bring a chuck of the BES down? Industry just wants to know what they have to do – practically talking about someone from the outside patiently, persistently breaking in using routable protocol or a disgruntled insider
- Routable, non-routable and stand alone – we used these categories in Austin/
- We did build consensus on connectivity, and but not on the protocols – broke the connected into routable and dial-up - protocols should be done in the controls
- Propose we are after connectivity – color code the first four lines and discuss what if any break out needs to be included –
- Two categories of connected and not connected?
- Confusing protocols with access – it is the access that makes system vulnerable

After a break, facilitator Stu Langton pointed out the tensions the Team has experienced has been balancing three things: getting the task done on time; doing it well; and building consensus among the team to move forward. He noted in Austin the SDT seemed to have a degree of consensus on three tiers: connectivity/routable/dial-up, non-routable, and not connected. What was discussed before break is a continuance of that discussion. The Team may not need to retest the earlier agreement but simply flesh out what is included in each category. The Team agreed to ask the CIP 002 sub-team in light of the discussion to test where this would or would not work and bring back refinements or alternatives that address questions.

Final SDT Discussion Points on CIP 002 Requirements

- May need a full team approach to refining the requirements?
- Connectivity/routable/dial-up are not all inclusive, dial-up could be included in non-routable too – need various perspectives to test these categories – I am concerned about non-authorized access
- Category should just be "connectivity." But we need to clarify "connectivity"
- Maybe we need to use "accessible" – then define as remotely, local and not accessible
- It is good, we just need to move forward with it by refining it – not locking into these terms and need to refine them using the Sub-team group

- When we have an issue and we don't have a definition we can simply ask each person what the term means to them to try and build a higher degree of understanding

CIP 002 Attachments

John Lim then presented an overview of the approach taken in the attachments.

SDT Discussion

- Is "essential to the reliability of the BES" the same thing as "supporting the reliable operation of the BES system"?
- Suggest changing to "reliable operation of the BES"

Real Time

- "Real Time"? Do we need to clarify?
- Need to be sure we are using terms consistently across NERC standards.
- Is there a catch phrase we can use that captures the concern? Real time operations?
- Within a period of time?
- It means right now up to thirty minutes? Or is it an hour cutoff, the point it must be reported?
- This may have to do with how many megawatts is lost over what period of time that impacts the system
- Within fifteen minutes (or X# of minutes) would cause a disruption of the system – concern is for the condition of the system
- Default Disturbance Recovery Period is fifteen minutes – from the glossary
- Allowed thirty minutes to recover
- This is an example of two different standards we are drawing upon for two different requirements – can NERC help identify applicable comparable standards?
- Note that the thresholds for reporting something and time for correcting it may be different for the same standard.
- Looking at other standards from other teams is a novel concept for most drafting teams.
- 30 minutes for IROLs in three different requirements – supports using that time frame
- Concept of time horizons of reporting and correcting are not germane to protecting the BES.
- "Real time" captures it even if it is a fuzzy term.
- Does this mean you have to prove to an auditor that you can anticipate all the possibilities?
- IROLs are part of the reliability coordinators role.
- Part of developing standards is the need for setting time horizons for severity of violations.
- Real time is action required within one hour to prevent further damage to the BES – comes from guidance document for establishing time horizons.

- Putting in specific times may not be needed here – "real time" for purposes of auditing may be too wishy-washy.
- Should we test with a vote and move on?
- Leave as is and then when we write the requirement say "real time operations" that then refers back to the NERC guidance.
- Do we need to specifically reference here the real time operations in the requirement?
- Put in parenthesis since it is not in the requirement but in the guidance
- An ad hoc team was asked to address: including Howard Gugel, Doug Johnson, Dave Revill and John V. Boxtel.
- Issue may not be not real time operations but the definition of immediate impact

Audits, Standards and Guidance

- All this is part of the standard as an attachment? Or is this only guidance?
- If the former then I need to be prepared to address the sixty or so bullets as possible items for audits? I have to prove everything in the attachment if part of the standard.
- Thought we were moving it to guidance
- Have we switched the numbers of attachment one and attachment two from the last meeting? Yes.
- We have two attachments even though at the last meeting we agree to meld into one attachment and moving much of the old two into guidance?
- Keep the opening paragraph under dynamic response and move the bullets to guidance?
- That may be worse.
- But we have to define this somewhere.
- We are here to protect reliable bulk power not simply to make compliance clear.
- We have to identify critical functions and how we will protect those functions.

Functions.

- Functions ended up in the definitions then pulled back out as being too broad for the definitions and were put back into the attachment
- Functions have never been incorporated into what we are trying to do – our approach to reliability is to look at how much a system impacts the grid – concerned we are arguing about the same concepts as six months ago
- Functions for reliability must come first – the level of controls will come from table 1

Disturbance to the BES.

- Are we really talking about anything that can cause a Disturbance to the system? Reviewed the definition of "Disturbance" – only functions of significance are those that can cause a "Disturbance to the BES"
- But that does not include situational awareness
- Can we use an existing NERC term and build on it?
- Do we want to leave vague terms and leave it up to auditor for interpretation or drill down into the details?

- I would like to use existing terms like "Disturbance"
- Can we throw ideas out about how to address the concept of combining into one attachment and the rest to guidance?
- We have already posted a version of comments and changing based on comments not trying to rewrite the standard completely –
- There was no comment about removing functions from attachment – there were comments about removing examples – if repost radically different standard we will get a whole new set of comments.
- We do have the ability in this new CIP standards process to offer changes.
- The primary issues are the scope to be addressed – hopefully building a significant yes around this table will help build a significant yes in the industry –
- Can we spend time on BES cyber system scoping? What is the context of effect and the context of time and connectivity – I like drawing on existing definitions if possible.
- Disturbance plus: for purpose of defining the scope of applicability of SIP standards, the functions of relevance are only those which could cause a Disturbance to the BES, restrict control and operation of the BES, or affect situation awareness of the BES
- Can we just define a list of systems that do the things we want to cover such as for situational awareness and determine a list of what to protect?
- Concerned that we are not building on success but only re-discussing the same issues – the industry wants to clarity
- Anything in NIST that can be used as a starting point?
- Nobody has come up with anything that should not be in attachment 2 – IT does not know what is vital for protecting the reliability of the BES – bulk produces determine what is essential and cyber can help figure out how to protect.
- What we have here is an effort to provide clarity – this is the stuff to protect
- Lets take this and make clearer what we are trying to protect
- Situational awareness may take more effort since it is a little squishy – but much of the rest is concrete enough to work with
- Those in the control world can look at the list and see if it can be made more concrete – others can work on the connectivity box – then see if we can jell them together
- Defer where it goes until after we set what we need
- Will we end up with anything different than the list we already have?
- We are describing things by functions
- List essential functions and leave it to entity to determine which meet that and offer guidance on what you think – serves as an interim step
- I like idea of moving sub bullets out to guidance, leave in functions with a matrix
- That puts focus on each group creating the list they need then cross reference to the IT guys to help figure out how to protect it

Addressing Industry Comments.

- Need to go back and read some of the comments that were offered. What are they telling us about Attachment 2?
- Regarding Attachment 1 and 2 – industry wanted more specifics of what is to be protected so we provided the attachments – now they comment back that they don't like specifics – industry will not be happy because it will have to spend money and resources to address it
- What does the statement above mean to an auditor?
- Jay pulled out and read from a comment a draft definition that might address the issue
- The bullets added clarity while the general definition offered to cover the breadth of situations.
- We have not discussed the suggestions for refining offered in the comments – those could be part of a brainstorming effort to addressing the question.
- If we take into account all the comments offered we will end up with the standard you have now because industry doesn't want to change because it will cost them resources.
- We cannot make radical changes to the documents we have posted and expect to build consensus or broad base of support.
- Looking for members to pull forward key concepts from the comments for group consideration
- We did not do justice to the comments by only reviewing summaries and only considering them in small groups or just asking members to read them on their own.

B. CIP 002-4 "Parking Lot" Issues

During the course of the first day's discussion the following issues were noted, but not resolved, for sub-teams to return to:

1. Multiple Locations – concerns raised re: rationale
2. Cyber Security Incident Definition
3. Distribution Provider – concerns regarding inclusion
4. Presence of R1 and R2 could present double jeopardy concerns
5. Define "change in BES" (R3) Long term? Etc.
6. How does one audit R3? Is there an implied requirement of maintaining a list of changes?
7. Clarify the link between Attachment 1 (R1) and Attachment 2 (R2) and where to capture the link (Guidance? Standards?)
8. Distribution (used as stabilizing load during restoration) for Blackstart?
9. Standard in development of High impact system – reference: Project 2009-09
10. My comment agreed was that 1.11 effectively includes all BES Facilities greater than 300kV. An option might be to delete 1.11 and include something like the following in every other item (using 1.1 as an example):

11. APP #2: 1.11 effectively includes all BES Facilities greater than 300kV. An option might be to delete 1.11 and include something like the following in every other item (using 1.1 as an example):
12. APP #2: 1.1: Generation Facilities, and their associated Protection Systems, singularly or in combination...
13. BES Cyber System vs. Cyber System?
14. John Ciufo – Standard in Development – High impact system – reference Project 2009-07

Based on a review of the parking lot issues, the Team agreed to the following drafting assignments:

1. **Control System** – Produce a list of examples – Rich Kinas

On Day 2 Rich presented a draft list of examples for control systems.

SDT Discussion

- Only to the low side? This is what the industry does now – what they are thinking – we need to fit in or make clear what we are talking about to avoid confusing the industry
- Some of the industry does go further
- This is a means or tool to the end of clarifying intent
- May be part of guidance document
- May want to include other ways industry is addressing – these are not exhaustive, only initial thoughts

2. **Matrix Group – "connected/not connected**" – Jon S., Jackie, Bill, Jay, Rich, Patricio (John V. Boxtel)

Jon Stanford provided an overview of the points of agreement after the group reviewed the list of points from discussion yesterday in its discussion the night before.

- Bright line was a good idea and effort but may not work after testing several examples. It could be counter productive
- In CIP 002 it is important to get object or target of protection.
- Applying connectivity can become very complicated.
- Entity has to decide what is a BES – cannot cut systems up into small pieces – so we all should "get over it."
- The low baseline needs to be those controls/requirements that provide the highest value to mitigate risk.
- We shouldn't let "audit fears" limit our ability to develop meaningful standards, instead let auditing adapt to the new standards.

- We shouldn't' be afraid of if/then/else application of some controls/requirements as appropriate.
- The team had consensus that control work should move forward in parallel to the 002 work – i.e. we should develop catalogue in tandem not in sequence.
- The team agreed there needs to be more guidance to sub teams
- This will capitalize on work already done by sub teams in developing controls.

SDT Discussion

- Does this apply to controls not requirements? We cannot put "if then" in the requirements.
- Still to be determined in the language to be developed. Most of this discussion is about controls and writing requirements – apply focus on practicality, lot of industry comment referenced routable protocols.
- Putting "if/then/else" introductory language before the "shall" phrase may be workable and has precedent in other standards.
- Auditors will audit to what the requirement says – need to capture words in the requirement that we want them to audit to – crisp accurate language so industry knows what will be audited and auditors will know what to audit too.
- Sub group work needs to use consistent language across the standards – need a common language whether it is h-m-l or something else
- Confident if the right things coming out of 002 then we can set the right "bright lines"
- 002 is an identification exercise – current standards do not allow you to take into account how assets are deployed – this new approach does if controls written properly.
- 002 will identify the important things to protect and the assets related to those regardless of type of connection. We understand that technology will change and the standards will need to incorporate and adjust to those changes over time.
- Does this take away the connectivity piece of the evaluation? Closer to what we had before? Need to decide and start drafting controls.
- Can still include routable protocols in 002 if it would provide the best industry response and compliance if that is the way the industry thinks.
- Yes, we need to put stake in the ground –but it is not either or – can we address connectivity in the controls? Need more discussion of how many controls will be in the "low", may be a small number
- NRC guideline effort struggles with the same issue – they have an appendix B "mandatory" controls and appendix A technical security controls with an exceptions process – you would have to show auditor you do not have "connectivity"
- Good concept but a few things bother me. "Don't be afraid of audits? Not afraid, but not sure how to accomplish
- Take the language "with a grain of salt"– starting the discussion, not meant to be inflammatory.

- What I want to happen is that anything out of 002 should address making the system more secure – don't care if high or low but whether or not adequate protection is provided certain controls
- Lot more common ground than at first appears – want to consider impact on the BES, the connectivity, and how we apply controls – trying to get the same end of controls appropriate for the environment
- Common on the end result – still struggling how it is understood by the industry which sees their world changing.
- Does it make more sense to come up with complete list in 002? If industry concerned about increasing scope to non-routable you need to explain the intent to them – also addresses Congressional concern past standards did not address everything – explain to industry that not everything is high and that listing into low where appropriate helps focus efforts on the important things.
- Problem with government NIST system is that too much is low with little more in medium and little more in high.
- Too many are avoiding updates by using the non-routable as an out.
- Federal low is not there because of IP – the low is too high – and the enhancements in the high category are significant to the most focused items. This may not be good optics, but we need to educate the industry and congress on the issue.
- Entities are not moving forward and are pulling routable protocols out to take advantage of non-routable exceptions and may be impacting protection of the system.
- Setting the routable protocol as the bright line can thus be counter productive to protecting the system.
- NIST is modeled for a different system than the private sector industry - also CIPs are not written for special situations but for the majority of the industry.
- Non-routable is not a loophole and may be reducing exposure and improving security if can remove the routable protocol.
- The NIST is offered to show why it will not work and why we are offering a more tailored approach applicable to the industry.
- All still getting to the same level of security and controls to apply – the end of 002 is not a list of h-m-l impacts but identifying the appropriate level of controls to apply.
- We are not advocating applying 853 – just illustrating the approach.
- Also trying to address unintended consequences and trying to avoid spending money on things that will not improve security of the system.
- Each of us heads off in different directions to fit our world –
- Let the 002 sub-team do their work and let the other teams begin developing the base line rather than the high first, develop the universe then look at how to apply connectivity.
- This is an example of how this team struggles to make decisions without seeing details – can we draft security controls without looking at connectivity?
- Two main concerns – is non-routable in 002, if so, are they now addressed?
- If artificially in low or high will have to spend money unnecessarily to protect. We may need to figure out what is in the h-m-l first.

- Everything starts out as at least low – should connectivity be addressed in the standard or in the controls?
- I think we do have a non-applicable category too – a bottom to the standard is set by applying the real time function
- Industry is spooked about making an inventory of all assets – we are proposing an inventory of those functions impacting the reliability of the BES – that is good business practice

3. **Real Time Operation/Cyber System affecting "immediate impact"** – Dave Revill, Howard Gugel, Doug Johnson, (Jon Van Boxtel)

Howard Gugel presented the group's report making the following points:

- The group suggested that functions of relevance are those functions essential to reliability of the BES. If it affect situational awareness does it exclude anything?
- Read the definition of situational awareness. A unit, a station? That is the way it is defined if can affect reliability of the BES.
- Entities currently know what those are.
- Information that can cause a bad decision that impacts the BES reliability.

SDT Discussion

- "Restrict" control of operations? Need to clarify the term – affect or constrain?
- Every entity has a different situation they will need to be aware of – depends on who you are as to the level of awareness
- Is this a good subject for a glossary term? "situational awareness"?
- This is an effort to take the attachment one from yesterday and try to address situational awareness
- Need to make sure that if in the standard we have supporting language in guidance
- Situational awareness is organizational behavior but not necessarily BES function
- Can apply to many things beyond just functions
- The term is a major cause of problems in Florida and the 2004 blackout
- Proposed modification – display of data that could affect function – "which could adversely affect the performance of a reliability function" –
- Trying to address where "monkeyed" with
- Everything there could adversely affect yet none of them are designed to cause adverse affects

4. **Attachment 2** – guidance, matrix – Rich Kinas and John Lim.

On day 2 Rich presented a draft guidance document. He noted:

- Dynamic response example – spinning reserves might be GOP function;
- Created table to help entities figure out which functions to address.

SDT Discussion

- Is this the same as Real Time operations?

- This could be part of that group but not the intention.
- Under suggested improvements – collapse some of the categories?
- Specific requirements for TO and TOP – different roles and different companies may be addressing each
- Flushing this out should not take too much time but be sure architecturally sound
- One thing under current CIP we had to assign assets to individual functions – be sure we do not become overly proscriptive
- What do we need to document for registered entities and ties to others for assignment of functions?

C. CIP-002 Guidance

In conclusion the Chair and Vice Chair reminded members that the Team has a very tight time frame to get our work done and they need to emphasize and trust the small group work and giving them time to get products ready and test with hard breaks for moving forward. The Team recognizes that 22 members cannot collectively write the standards within the time limits

The Team tested the level of support for the following guidance to the CIP 002 sub-team:

3. **Redraft CIP-002 to remove the connectivity options and handle them in the controls**
   Y= 15 N = 5

4. **Keep cip-002 as drafted yesterday and let cip-002 sub-team handle modifications to the matrix (Austin)**
   Y= 4 N= 16

The Team acknowledged they may need to revisit if in developing controls we find we cannot address the connectivity issue.

D. CIP 002 Drafting Group Update Report

John Lim reported on Thursday the Sub-Team's efforts:

- 002 completed most of the work on the requirements.
- Attachment 1 is definitions of the functions.
- Working on attachment 2 applying functions- working on that tonight.

He suggested that on Friday the SDT should concentrate on the standard document itself.

E. CIP-002-4 Review and Consensus Testing

On Friday, John Lim presented the revisions to CIP 002. He asked the SDT to focus on the content and intent of the draft and not to engage in word-smithing noting that there were extensive and challenging discussions among the Sub-team over the past few days. Focus on content and intent of document.

- Will send to Howard for editing and review.
- New work on Attachment 2- levels.
- The Sub-team removed definitions of functions for reliability of BES and moved them to Attachment 1.

1. Definitions

- "One or more programmable electronic devices including hardware, software and data organized for the collection, storage, processing, maintenance, use, sharing, communication, disposition, or display of data, which if rendered unavailable, degraded, compromised, or misused could cause a Disturbance to the BES, restrict control and operation of the BES, or affect situational awareness of the BES."

SDT Comments

- Do we have to start with BES before cyber system?
- Definitions- should be stand alone. Context comes in the requirements.
- Clarify the purpose of standard and this definition?
- Will this be added to glossary? Control center length?
- c. Real time capitalized? b. no capitalized. Proposing to go in the NERC glossary.
- Only "Real-time" in glossary. "Present time as opposed to future time." Lower case "real time" in document.
- Would it affect definition to leave real time out?
- Might confused.
- Real space time. Some of operations- not now but 20 minute horizon.
- SM: did agree on the qualification "alarm monitoring and processing"
- Add to d. <u>specific to operation and restoration functions.</u>
- BW: is it better to use now "real time" as a qualifier.
- HG: glossary definition doesn't capture. Use lower case.
- JL will do a real time edit.
- RK: Quick search of other NERC standards.
- JC: definition developed.
- AL: why was multiple locations in the document?
- Retiring 3 terms.
- Terms to be retired from the *Reliability Standards Glossary of Terms* once the standards that use those terms are replaced:
- Critical Assets
- Critical Cyber Assets

- Cyber Assets

A. Introduction

1. Title: Cyber Security — BES Cyber System Categorization

2. Number: CIP-002-4

3. Purpose: To identify and categorize BES Cyber Systems that execute or enable functions essential to reliable operation of the BES for the application of cyber security requirements commensurate with the adverse impact that loss or compromise of those BES Cyber Systems could have on the reliability of the BES.

SDT Comments on changes?

- One issue we will have to do with it. Removing "critical cyber assets" and "electronic security perimeter." Will have to add definition for that term.

Distribution Provider

- Reference to PRC 5- distribution providing owns a transmission- this is a transmission Protection System.
- Cover in guidance document. 6-7 PRC standards talking about special protection systems, etc.
- Looked at all this. Need to put in there. Look at registration text, it includes all that information. Those standards deal with under voltage etc. It is covered by a functional definition.
- Provides for changes in regulations.
- The Sub-team didn't agree with this one. Put in the parking lot.

B. Requirements

R1. In order to identify appropriate BES Cyber Systems for the application of security requirements or controls, each Responsible Entity shall uniquely identify and document all BES Cyber Systems which execute or enable functions defined in *CIP-002 – 4 Attachment I – Functions Essential to the Reliable Operation of the BES*.

R2. In order to categorize the BES Cyber Systems identified in R1 to apply Cyber Security requirements or controls commensurate with the potential impact on the BES, each Responsible Entity shall categorize or re-categorize each BES Cyber System according to the criteria contained in *CIP-002-4 Attachment II – Impact Categorization of BES Cyber Systems.*

2.1. The Responsible Entity shall review its categorized list of BES Cyber Systems, as a result of any change in the electric system that it owns or operates that affects the categorization of the BES Cyber System, and update within 45 days of the completion of the change.

Controls standards will specify applicability to the BES Cyber Systems categorized in this standard.

SDT Discussion

- States the reliability benefit in the requirement.
- Can't have requirement that starts in the middle? Need BES before BES cyber.
- Clean up wording on requirements.
- Need BES- agree JV- Not clear these 2 requirements what have to put in BES.
- Is 2.1 is a separate requirement?
- Add "In order to maintain and keep current the list…."
- Change 45 days to 30 days to be consistent with FERC directions.
- Why 2 requirements? Is it possible identify and characterize as 1? Looks like a step to an end result.
- R1- identify all BES.
- R1- to id cyber systems based on your BES. It would be more confusing to combine.
- Howard Gugel noted that you could combine as 1 requirement or leave as 2 separate.
- Is there an issue of double jeopardy? Forgot to include one and not categorized correctly? Look to defining your VSLs.
- 2 separate lists because of 2 requirement? If expect 1 list then 1 requirement. If 2 lists then double jeopardy question may be raised.
- Change in R3- "change in the electric system"?
- The Sub-Team removed BES cyber systems from here. Assumed will be covered in Change Management group. Couldn't find mechanism for update.
- Howard Gugel suggested striking "that affects the categorization of the BES" instead. Anytime you add anything new to your BES cyber system you have to update.
- R1- likes the unique identification and document vs. make a list. Entities are using something similar to a list? R3 updating "your documentation"
- Suggest edit: ~~electric system~~ BES
- Pick up commissioning activities, changes in BES cyber system in change management. Do an annual review and update and capture changes in system 1 time a year and that will capture this.
- Need to define "changing electric system"- what does this mean?
- "Commissioning new assets"
- Don't like "any" change. What does this mean. Needs a qualifier. Updating the documentation specified to R1? Keep update the list.
- R2.1 separate? Wasn't under posted version.
- Any change? Long-term change? E.g. bringing new line on?
- Howard Gugel suggested: "When any BES ~~element~~ facilities is added to or retired from the BES that it owns or operates."
- What about "modify"?
- R3- refer to R1 documentation
- Simplify to going back to R1. Not separate

- Requirement is for reliability and not documentation.
- 45 days? FERC said 30 days. Will need justification.
- How do you audit R3?

Parking Lot
- "Multiple locations" definition- concerns whether it is needed?
- "Cyber security definition"?
- Distribution provider?
- R1-3. If 2 requirements

Data Retention
- Less than compliance time frame? Maintain as 1 year. "Keep for the compliance audit period, 3-6 years depending on what kind of entity." Global issue for every standard. SDT has to figure out whether we stick with it.
- NERC should do this.
- Full year or …… Clean up to make consistent.

Violation Severity Levels.
- Team used NERC guidelines for VSLs to make consistent.
- "Or" is for 2.1

SDT Comments
- VRFs? They will be put in. Both will be high
- First line- in terms of audit? Look at your diagrams and go through steps.
- Open to suggestions.
- Don't audit that item. Combine process.
- Comes out in an investigation and 3 level process
- The auditor looks at what you present and drafts a "potential violation". Audit process stops and goes to investigations and further analysis. Not an audit function triggering thresholds.
- That's why we left this as is.

CIP-002-4 Attachment I
Functions Essential to Reliable Operation of the Bulk Electric System

The following operating functions are defined to be Essential to Reliable Operation of the Bulk Electric System (BES):
- Dynamic response
- Balancing Load and Generation
- Controlling Frequency (real power)
- Controlling Voltage (reactive power)
- Managing Constraints
- Control & Operation
- Restoration of BES

- Situational awareness
- Inter-Entity coordination and communication

For purposes of defining the scope of applicability of CIP Standards, the functions of relevance are only those that affect real-time operation of the BES. Further qualification as to what constitutes Functions Essential to Reliable Operation of the BES can be found below.

- Will place and develop it in the guidance documents.
- Make sure consistent with "real-time" definitions and any other changes in definitions discussed.
- Actively performed functions not reactions.
- Had this under dynamic response.

Attachment II

John Lim reviewed the development of Attachment II which Jackie Collett help to develop.

1. High Impact Rating (H)

BES Cyber Systems that would immediately affect real-time operations for:

1.1. Generation Facilities, singularly or in combination, with aggregate higher of the most current and prior to the most current rated net demonstrated capability (MOD-024 and MOD-025) of 2,000 MVA or more.

1.2. Generation Facilities, singularly or in combination, whose aggregate rated net demonstrated capability, as defined in part 1.1 above, exceeds the largest value, for the 12 months preceding the categorization, of the Contingency Reserve or total of reserve sharing obligations for the Reserve Sharing Group.

1.3. Generation Facilities that are pre-designated as Reliability "must run" assigned units that have Wide Area reliability impacts.

1.4. Generation Facilities designated as blackstart resources in the regional blackstart capability plan.

1.5. Transmission Facilities operated at 300 kV or higher in the Eastern and Western Interconnections or operated at 200 KV or higher in other Interconnections. (3 or more …)

1.6. Facilities required to support a primary Cranking Path used in a Transmission Operator's restoration plan per EOP-005.

1.7. Transmission Facilities that, if destroyed, degraded or otherwise rendered unavailable, would violate one or more Interconnection Reliability Operating Limits (IROLs).

1.8. Transmission Facilities that if destroyed, degraded or otherwise rendered unavailable, would result in the loss of generation Facilities, singularly or in combination, with aggregate rated Net Demonstrated Capability (MOD-024-1) of 2,000 MVA (?? TOO LOW ??) or more

1.9. Transmission Facilities identified as essential to meeting (verify wording) Nuclear Plant Interface Requirements established in accordance with reliability standard NUC-001 for Nuclear facilities.
1.10. Transmission Facilities that, if destroyed, degraded or otherwise rendered unavailable, would result in voltage collapse, electric system collapse due to frequency related instability, or complete operational failure of the Transmission system or separation or Cascading outages. (linked to IROL criteria - wording)
1.11. Protection Systems for BES Facilities operating at 300 kV and above in the Eastern and Western Interconnections, or operating at 200 kV and above in other Interconnections. (Hardiman: establish 300 kV baseline)
1.12. Special Protection Systems (SPS), Remedial Action Schemes (RAS) or automated switching systems that operate BES Elements and that have wide-area impact.
1.13. BES Elements that perform automatic aggregate load shedding of 300 MW or more.
1.14. Primary Control Centers and any backup Control Centers performing Reliability Coordinator functions.
1.15. Primary Control Centers and any backup Control Centers performing Balancing Authority functions of Transmission Facilities or generation Facilities, singularly or in combination, of 2,000 MVA or more.
1.16. Primary Control Centers and any backup Control Centers Transmission Operator functions that remotely control 2 or more 300 kV or higher Transmission substations or switching stations.

SDT Comments

- Lead in sentence. Is the cart is before the horse-- the 1.1 piece. Say something about BES systems first.
- The Sub-Team removed all reference to systems. Now referred to "facility elements" from the NERC glossary.
- Referring to generator rating standards? MOD 24 and 25? No more "opt out" – rationale is reference to MOD 24 and 25, engineering studies already authorized. No good reason to have "authorized engineering study"
- Where do we address 2000 number? Went through event analysis category- Category 3. Talked solely about generation and supply.
- 1.1."Nameplate generation rating"- use something we already have- "current rated net demonstrated capability.
- 1.2- time limit-
- How do we link this to defining the BES functions? Where is the correlation? BES functions called out in R1- initial scoping. This is R2 piece that links- then you go through this criteria.
- Are all functions equally weighted? No weighting, just a scoping.
- The Sub-Team tried to take out anything that isn't essential to reliability.

- Operations manager of reliability center- "immediately affect real time operation" - will this place everything low?
- "Facilities"- h/m/l baskets. 3rd basket is things that are not facilities? Have to first determine what "facilities you have."
- BES is a defined term. Says that regions will define. "Generally operated ….."
- Defined by the IRO- have to go by this.
- What is the connection between Attachment 1 and 2? Functions then rating. Need to make this clearer.

1.5 Must run units.
1.6 Blackstart Capability plan.

SDT Comments

- Regional blackstart- includes distribution- used as a stabilizing load during restoration-- include in a guidance document.
- Does this bring into High lots of things not having to deal with transmission?
- Distribution SKADA systems? All? Some?
- This should be a "parking lot" issue.

1.7 "Transmission facilities"- 3 or more connected to station. Add back in.

SDT Comments

- Is 300 KV too low? This came from another document. Few if any industry comments about voltage level. People haven't thought through the impacts on the industry.
- Didn't focus on voltage. Commented on 3 lines being too low. More understanding 300 for a high? This will bring in a lot of locations and equipment.
- Optics- raise to 500 KV portions of interconnection that don't have any. Keep voltage level but adjust the number of lines.
- Consider throughput megawatt? Original draft- inappropriate measure for transmission? Use voltage.

1.8 Number of comments- clarified by referring to EOP -5
1.9 IROLs reference. Decided to stick only with IROLs.
1.10 Rewording of what it was before.

SDT Comments

- Linkage with 1.1? 1.8 is more far reaching than 1.1. 2000 MVA is too low. 2000 MVA may be good at the medium level?

1.11 "Essential to meeting"= (verify this wording)
1.12 Transmission facilities.

SDT Comments

- Without engineering analysis can you do this?
- Link to IRL- reference and work on wording.

1.13 Protection systems- now high- lot of discussion

- Comes from other standard

SDT Comments

- Part of 1.5? Every 300 KV has a protection system. Every 345 KV device that has protection device, 1.11 equivalent to 1.5.
- Inconsistencies related to actual impacts?
- SM: John Sykes- Systems Control committee- determining high impact systems. Standard isn't finished. Reference that when ready?
- Simplify and lump all together in terms of 300 KV?

1.14 Special Protection systems (SPS)

SDT Comments

- Use 1.3- language- "that have Wide Area reliability impacts."

SDT Comments

- Consider adding language: "If the BES operates at N-1 or higher, should field asset criteria indicate an inherently lower impact category than control centers.
- Aimed at T/G/CC- when have requirements that apply to G but not T. Met the criteria.

Medium

2. Medium Impact Rating (M)
   - 2.1. Generation Facilities, singularly or in combination, with aggregate higher of the most current and prior to most current rated net demonstrated capability (MOD-024 and MOD-025) of 1000 MVA or more not included in Section1 above.
   - 2.2. Generation Facilities that are pre-designated as Reliability "must run" assigned units that have local area reliability impacts.
   - 2.3. Transmission Facilities operated at 200 kV or higher in the Eastern and Western Interconnections, or 100 kV or higher in other Interconnections, not included in Section 1. (include 3 transmission lines)
   - 2.4. Transmission Facilities that if destroyed, degraded or otherwise rendered unavailable, would result in the loss of generation Facilities, singularly or in combination, with aggregate rated Net Demonstrated Capability (MOD-024-1) of 1,000 MVA (?? TOO LOW ??) or more, not included in Section 1.
   - 2.5. Protection Systems for BES Facilities operating at 200 kV and above in the Eastern and Western Interconnections, not included in Section 1, or operating at 100 kV and above in other Interconnections, not included in Section 1.
   - 2.6. Primary Control Centers and any backup Control Centers Transmission Operator functions that remotely control 2 or more 200 kV or higher Transmission substations or switching stations not included in Section 1. (generation control centers ??)

SDT Comments

- Write cyber security requirements apply to H/M/L – is there enough to make a difference in cyber security controls? "Decimal dust" difference.
- Is there a difference between moderate and low? If you draw line at moderate or at high?
- SDT members should go back home, next week a count of facilities that would meet the current criteria. How many are we talking about any of these buckets?
- Control generation? 2.6- generation control center?
- 2.6 would catch all transmission owners? Anything above 200 KV.
- Captures registration errors?
- Definition of BES Cyber Control System? Whether we do cyber system alone. Cyber system definition- to separate from BES cyber system.
- Always refer to BES cyber system.

3. Low Impact Rating (L)
   All other BES Cyber Systems on the list not mapped to Section 1 High BES Impact or Section 2 Medium BES Impact.

SDT Comments

- BES subsystems should be BES cyber systems

III. SECURITY CONTROLS REQUIREMENTS (CIP 003-009) REVIEW

A. Initial Sub-Team Progress Reports

On Wednesday the Sub-teams presented brief status reports before breaking into sub-team meetings. The chair and vice chair suggested the sub-teams should initially focus on setting the "low" for purposes of controls. Need to set a common agreement on where the low water mark is – wrestle with high and medium later.

SDT Discussion

- Do we have the buckets of lists for consideration?
- Support the idea of starting with the lows. This could be a good process and help sub-teams understand what they are addressing.
- Need to bring different perspectives to the task of identifying and establishing a common low water mark

- **Governance Sub-team.** Jon Stanford noted that the Governance Sub-team has nothing new to report but that they do have the list to review for consideration of the low water marks.

- **Access Control & Audits Sub-team**. Sharon Edwards reported on the Access Control & Audits Sub-team noting they have identified CIP requirements we are looking at as compared to DHS – some of the latter did not have a corresponding CIP requirement. They have also constructed template from individual worksheets including constructing requirement language to address missing DHS items. They have not yet distinguished h-m-l and did not yet review FERC order to be sure issues addressed. She suggested a need to coordinate some of the DHS items with the work of the other sub teams. They also added a column not in the template for all the groups – "CIP version 3 language."

- **Recovery and Response Sub-team** – Scott Rosenberger noted they had not made a complete review of DHS.

- **Personnel and Physical Security**
- Doug – have a spreadsheet and prepared down through h-m-l and initial pass through CIP, review as group today before cut and paste into the template

- **Change Management, System Lifecycle and Information Management.** Phil Huff noted they had gone through CIP language and added DHS security controls where appropriate and they determined initial applicability. They will be making an initial h-m-l determination for the controls. Putting in objectives now in at the time of writing the requirement may help in interpreting the intent later.

- **Operations Security.** Jay Cribb reported his sub-team had taken one stab at objectives but not h/m/l.

The facilitators noted the teams are at different levels of development – may want to test with those teams that are ready.

B. Sub-Team Reports on March 11, 2010

Personnel and Physical Security	CIP-004 – R1, R2, R3, CIP-006 R1 through R6 DHS 2.3 Personnel Security, DHS 2.11 Security Awareness and Training DHS 2.4 Physical and Environmental Security,	Doug Johnson(Lead), Rob Antonishen, Patrick Leon, Kevin Sherlin

The Sub-Team report was delivered by Doug Johnson.

Personnel
Awareness programs

- Policy? Expecting the Governance group to address.
- "establish, document, implement and maintain"? continue to use this with other Team? CIP Version 3- not removing it.
- "Information protection program," develop an incidence response procedures? As long as you can test it and demonstrate it works.
- Looking at a low level. If you have BES cyber systems, you will have an awareness program.
- Inter-connective of operations control – 706

Training

- "at a minimum" vs. "appropriate to personnel roles and responsibilities"

Personnel Risk Assessment

- 706 guidance- special circumstance that allow an exception to requirement for training prior to allowing access.
- Program has to specify the exceptional circumstance-
- Anyone with access to BES cyber system. Is that everyone down to the low levels?
- Any baseline opinion- Lows? Electronic or physical.
- Degrees?- cleaning crew.
- Lows?
- If you have physical access to a low impact BES cyber system, do you have to have a personnel risk assessment?
- If there is a requirement for physical access, have to have controls in place.
- Need to be tracking to have an issue.
- We should be thinking about this in terms of risk. Authorized users, maintainers of BES cyber systems. 2 communities here. Opportunity to split and get to risk.

- Interpretation- acceptable alternatives are…… E.g. social security number for verify identity.
- Identification issued by federal, state or provincial agencies.
- Don't worry about the methodology- worry about the right people and provide the level of granularity.
- NERC Interpretation- identify verification, risk assessment. Try to make clear. E.g. Janitor in control room-

Physical

- Physical Security Perimeter- revise current Glossary definition.
- New definition proposed. Limit it to being just a "border" and control access to border. You will have to define where it is and later what's in there.
- Only if you have a defined physical security perimeter.
- "All equipment comprising a BES cyber system shall reside within a defined PSP."

SDT Comments

- "within one or more PSPs?"
- That is better. Tweak to deal with the Hoover dam issue.
- E.g. a "laser field"-
- Leave the definition at a higher level.

Physical Security Plan

- Senior manager approval in new version?

SDT Comments

- 706 requires this.
- "Authorization" = standard language? Current doesn't say who authorized or designated.
- Addressing cross references- highlighting to coming back to. Flagging for now.
- In governance- senior management- remove subordinate references to SM? Talk about what they need to do not how. Let the program set that out.

Physical Access Control

- Controls- this will go off to a guidance document.

Monitoring Physical Access

- Blue will be the "how". Saying you will have it. Go to guidance document for the how.

Logging

- Same

Visitor Control Program

- Same.

Maintenance and Testing

- Need to get with Sub-team defining the perimeters to determine physical control. Keep that in this?
- Don't put in standards in terms of how to protect.

Protection of Electronic Access Control Systems

- Should move these out of standard.
- Are these part of the BES cyber system itself? Protect the system performing the functions.
- The Team needs more discussion- what is a BES cyber system, how to draw the line around these?

SDT Comments

- SM: 706 review? Partial. More discussion.
- Training the trainers- quality and consistency among them. Part of directive.
- Web based training- no instructors.

Recovery and Response	CIP-008 R1 & R2 CIP-009 R1 through R5 Incidence Response and Contingency Planning	Scott Rosenberger (Lead), Joe Doetzl,

Scott Rosenberger reported on the Sub-team's progress noting they made it through DHS requirements.

Response

- Draft 5 requirements: incidence response you do partially in high and low.
- All will have a plan. Identify actions; roles and responsibilities, reporting, reviewing your plan annually.
- R2: additional for high impacts- review plans based on changes. Communicating updates; Testing response plans annually.

SDT Comments

- Does this requirement apply to all cyber systems?
- This only applies to high. The plans dealing with high impact- add language: "for their high impact basis"

- CIP 008 Cyber Security Incidence- still to figure out.
- CIP 008- R3- document retention- all
- CIP 008 R4 (high) and R5 (low)

SDT Comments

- Annual= once every 12 months?
- BES Cyber assets? Not a new term. BES Cyber Systems-
- In Personnel training requirement- address once every 12 months.

Recovery Plans CIP 009

- If low don't have to have a recovery plan. Only applies to high.
- R2 Recovery Plan Training
- R3 Recover Plan Testing.

SDT Comments

- Place this into table/format with changes? Yes.
- Worked with Scott/Howard re formatting.

- Important to see whole standard together. Everyone had changes.
- Valuable effort- to see how this will sort out. E.g. 1 section for every one. Then some for high, low.
- Didn't see a control- Security of the back up configuration? Current standards- not part of system. Could store elsewhere unprotected? Is this a potential attack vector? 1.3 of CIP 009- back up storage and protection will address.
- Requirement to restore whole system and make sure it still functions (no corruption, passwords, etc.). Restore to as it was.
- Need to think through whether you want the same VRF for everything in requirement. Put in 1 requirement. If you want VRF differentiated, you will need to split the requirement out. E.g. if you have high, these things need to added to you apply.
- Where do you store backups?- Falls in information protection.
- Connectivity concept? Didn't include at all. Where to add? Whether connected or not still need to be restored.

DHS New Requirements

- Control centers- back ups- alternative locations. Didn't seem to apply to generation, transmission.

Access Control and Auditing	CIP-003 R5; CIP-005 R2; CIP-007 R5; CIP 004 R4 DHS 2.15 Access Control DHS 2.16 Audit and Accountability	Sharon Edwards (Lead), Jeff Hoffman, Frank Kim *Observer Participants: Sam Merrell*

Sharon Edwards reported on the Sub-team's work as follows:

Update

- Created the proposed requirements for all assigned CIP requirements that have a corresponding DHS control
- Reviewed the proposed requirements corresponding to CIP and identified which controls should apply at the H, M & L for (C, G. T)
- Created proposed requirements (where applicable) for additional DHS controls which do not have a corresponding CIP requirement
- We have not yet reviewed those to determine if they should apply at the high, medium or low level

Future Tasks

- Group will attempt to gather all the account management requirements currently found throughout CIP 005, CIP 007 and CIP 004 into one place
- Ensure the following are done for each assigned proposed requirement:
  - Identify FERC Order 706 paragraphs & how they are resolved
  - Ensure Objective has been documented
  - Ensure CIP changes have been documented

- Group has decided to determine applicable password thresholds utilizing the NIST password tables and determine what the High, Medium, and Low targets should be – Frank
- Review for impacts of Connectivity on the proposed requirements – Team assignment

Points of Coordination

- Coordinate with Ops Security re. log monitoring and log monitoring for failed log ins based on passwords. – Sharon

SDT Questions and Comments

- Access to Information- Talked to Phil Huff's team- they handle access to information.

Account Management

- High levels- applies at high and medium levels. May be time parameters may change at medium levels. E.g. revocation of access within 6 months., Not a compliance area.
- All will apply at the high, much applies at medium with time parameters relaxed, majority will not apply at the
- Revoke "remote" requirements? 2.15.3- R4- Doesn't meet requirements of 706- revoke 'immediately'? 24 hours too long? Especially for highs.
- High and low- look at total list of being low before making a determination on this?
- Similar issues with physical access and "immediate"- are we free to challenge FERC's order if we can justify rationale. DHS controls don't require immediate revocation.
- Timeframes should be consistent with the level of risk. Removing access? Do you need 6 months to do that?
- Keep in mind FERC directives are focused on the Version 1 standards. Directed to revise standards. Timeframes should be commensurate with risk through H/M/L. If speak to "immediate" we probably mean high.
- 6 months seems excessive.

Remote Access

- Controls apply across the board (215.24) pp 5.
- Pp 12- Passwords discussion- Frank's proposal- look at NIST material for password complexity and develop targets for h/m/l.

SDT Comments

- In Florida- interpretation of that requirement is that hardware enforces the password level.
- This is not in standards. Every requirement comes down to policy. NERC will need to address in the regions.
- Ask for unique (user name) identification and authentication? Remote access for high systems- low was just authentication.
- Use table- require a certain level of entropy etc.

- Caution the SDT in general against proposing a technology solution for high impact. Consider procedural mechanisms that may be stronger.
- New requirements pp 14- have no CIP corresponding requirement, e.g. authenticating management in DHS; mobile devices; wireless access in DHS; and time stamps for each group.

Change Management, System Lifecycle and Information Management	CIP-003 R6; CIP-007 R1, R7 CIP-003 R4; CIP-005 R5.1.1, R5.1.3 DHS 2.5 System and Services Acquisition, DHS 2.6 Configuration Management and System Lifecycle, DHS 2.10 System Development and Maintenance DHS 2.9 Information and Document Management, DHS 2.13 Media Protection	Keith Stouffer, Dave Revill, Phil Huff (Lead) *Observer Participants: John Fridye*

Phil Huff reported on the Sub-Team's work reviewing the Change Management requirements worksheet. He noted that the Sub-team's work focused on the language itself, not on applicability. They still have to go through FERC order review. The have modified table/worksheet to track open issues/complications. They now have drafted most of the objectives and changes to CIP language.

Baseline Configuration
- Baseline of how configured for change control, for incidents and unauthorized

Configuration control
- Includes CIP 003 and testing

Access restrictions for configuration changes.
- Beyond access control. From DHS.
- Access control sub team may be sufficient.

Configuration assets-
- Configuration management plan- into policies and procedures.

SDT Comments
- Looked at the NISTER document? Yes, looked at NRC documents as well.

Information Protection
- CIP 003- section causing problems. Don't apply full protection program. Small subset of security controls applied to information. Chose to go that way again.
- Don't have confidentiality. Controls within requirements they are developing. Just protect your information. A bit vague, but lived with it so far and FERC hasn't commented.

Protection Program.
- Handling a new DHS procedures.

- Confidentiality agreements among entities.
- Assessment of program.

SDT Comments

- Confidential agreement protections- probably can't require. FERC doesn't have jurisdiction to require.
- Requirement can obligate the registered entity to put in place. Can't hold other side for compliance. That would be a contract relationship with a 3rd party.
- Good e.g. in other controls relating to Federal model. E.g. Inter-connected security agreement. Caution to the SDT not to bring in additional requirements grounded in federal model. Need to be sensitive to this and keep it "nice and Cippy."

Maintenance

- Periodic system maintenance- will combine with configuration management controls.
- Maintenance tools- prevent malware- detox without applying CIP controls to it.
- Maintenance personnel- authorized to perform maintenance on the cyber system (not cleaning crew).
- Remote maintenance- security controls above remote access- vendors or others performing some form of system maintenance.

SDT Comments

- Controls for when vendors log in for maintenance? Logging into sub system from main office is "remotely"
- Clarify with Sub-team on access control related to system maintenance? These are on top of control access requirements? Point of coordination.
- Remote maintenance- focus on who has access. Should be in the operations security group.

Media protection CIP 7 R7-

- Could have removable media (e.g. USB thumb drive to configure control systems). Make sure physically stored and transported securely. Disposal and secure for reuse.
- Define "media"? Field personnel to maintain accountability in terms of transportation of piece of equipment to a secure location and be wiped? Difficult to talk about security of data.
- Order 706- ability to erase media- this in direct odds with NIST- look at that.
- Make sure what is in equipment is no longer available when disposing equipment.
- E.g. Send Switzer back as it was in the failed state. Can't trouble shoot without being the same. They then send back a new one.
- Introduction of stuff into system. When take out, must do various things depending on the state laws. Stay away from info itself. Focus on info pertinent to our security. Don't worry about all information.
- Disposal- sending back to mfg.- data we want to remove vs. all other settings.
- Editorial- don't introduce programmatic requirement on entities as they apply to BES cyber system.

Operations Security	CIP-005 R1, R3 CIP-007 R2, R3, R4, R6 DHS 2.8 System and Communication Protection DHS 2.14 System and Information Integrity	Jay Cribb (Lead), Jim Brenton, Jackie Collette, John Varnell

Jay Cribb reported on this group's effort including new BES cyber system component definition.

SDT Comment

- Discount unmanaged switches devices. Yes if a switch vs. a hub.

Boundary Protection/ESP

- New concept- problem with ESP- no such thing exists. Perimeter and access points.
- Only real things are the access point.
- Call "controlled boundary access points."
- ESP goes away.
- 1st Requirement
- Define boundary access points.

SDT Comments

- Boundaries between all BES cyber systems"? "Between each cyber systems and other systems"
- "Shared with other systems"? e.g. virtualized server environment.
- Around network switches- BES cyber system can't be existing in the same boundary as another cyber system. Substation e.g. Clarify this. Between BES cyber systems and non BES cyber systems.
- Trying to deal with this issue. ESP had bad traits for operations people. Flexible enough to be able to describe things as an entire system and looking at the boundaries between this. Addresses 706 order- more than perimeter- they talked about defense in depth. Boundaries not just a perimeter.
- Nice requirement. Simplified too much?
- First Requirements duplicates what is below. After shall: then all sub bullets and 2nd Requirement on boundaries.
- In/out is problematic word, however the intent is good.
- System definition will include the concept of a boundary. Don't want to have industry create boundaries don't exist.
- Applies to physical? Came from CIP 005- electronic boundaries.
- What does this mean in the physical sense?
- Clarify difference between ESP and boundary. Something to describe difference especially for industry that has spent resources identifying ESP.
- Need more "guidance" on what we mean by boundary.
- Will entity be free to describe how big or small that will be?
- "Boundary" may be viewed as a generic use of the term.

- Challenge trying to define a boundary (logically or physically). DHS says define the "external boundaries"- maybe that is enough.
- Cause confusion unless it clearly defines these terms. E.g. "shared component". Is boundary a filtering device?
- Clarify physical vs. electronic.
- Sub-Team tried to cover things at both the micro and macro levels.
- Change or rename the definition? Make sure boundary doesn't become a synonym for perimeter. "Access control points" is the focus.

Electronic Access Monitoring.
SDT Comment
- Manual process that logs and alerts unauthorized process? Consider taking out manual

Communications Integrity
- New under DHS catalogue and problematic.
- Clarify the objective
- Working connectivity into requirement.

SDT Comment
- CIP 004 Remote Access and CIP 007Account Management
- Some overlap regarding methods of authentification- Need to coordinate with Access Control group.
- Operation Security talks about where you need authentification. Access Control and Auditing sub-team will address how you do it?
- Mainly concerned with integrity of communication.
- Types of communication covered? "Wireless" good but some clarification of types.

Remote and Accessible Services (Port and Services)
- Objective
- R1
- R2 it is what it says today.

SDT Comment
- Strike technical since there might contractual.
- Document and implement compensating measures
- Issue of pre approval of compensating measures (TFE).

Flaw Remediation (i.e. DHS for Patch Management)
R1. Its what is there today with the terms re-named.
Malicious Software Prevention.
This requirements is a what. The "hows" are up to the entity. Will address in a guidance document.
Security Status Monitoring
R1- monitoring
R2- alerting (need applicability matrix here).
R3: Logging
R4 security event response

SDT Comments

- All events? All events related to cyber security.
- May not know until after.
- "Forensic"- may have legal implications. Maybe "post event analysis"
- Overlap with last one. Incident response team?

Security Governance	CIP-003 – R1, R2, R3; CIP-005 R4, CIP-007 R8 DHS 2.1 Security Policy, DHS 2.2 Organizational Security, DHS 2.7 Strategic Planning, DHS 2.17 Monitoring and Reviewing Control System Security Policy, DHS 2.18 Risk Management and Assessment, DHS 2.19 Security Program Management	Jon Stanford (Lead), Jerry Freese, Dave Norton

Jon Stanford reported on the Sub-Team's work reviewing the Requirements Worksheet. He noted that the right hand side includes the current CIP. He reviewed the opening checklist:

- Requirements are written at a high level. In general, seek to draft "what" and NOT "how", "specific" and NOT "prescriptive"
- Requirements have been developed using CIP-003-3 through CIP-009-3 as a starting point
- Applicable controls from the DHS Catalogue have been incorporated
- Changes from CIP-003-3 through CIP-009-3 have been documented
- Applicable directives from FERC Order 706 have been addressed

Security Policy and Procedures

- Overarching requirements- formal security policy(ies). Plural- One or more policies.
- a-d
- Capture DSH Management procedures and policies.
- XXX- subject area policies. Can place any policy language here.

Control System Security Plan

- One 1R with 3 subs: (a-c). Say what it is here. Go to security operations to get the details.
- 2R annually review each bes cyber system
- 3R- revise plan.

Security Plan Update

- Captured above

Control System Connections

- 1R: two parts.
- All connections authorized and documented.

Vulnerability Assessment and Awareness.

- 2 part Requirement.

SDT Comments on Governance

- Discreet requirements? Goal is a single policy. Is this a single requirement for a policy with bullets under requirements. Attachment providing elements?
- Each topical area could be listed by name or topic.
- Important thing: get senior management official managing the implementation requirements.
- Don't require only one policy and allow for internal program structure where it make sense.
- Eliminate overlap and duplication.
- No less than annually review your security plan for each cyber system? Didn't put update in.
- Security plan? Physical and electronic? No plan is for the BES cyber system.
- Look at your requirements- assume there are policies that say that will be done.
- Don't recreate policy statement.

IV. NEXT STEPS

The SDT reviewed the plans for the May 2010 Technical Workshop including Gerry Adamski's email. Gerry Adamski has offered to be the "general facilitator" for the workshop.

- How long? 1½ days. Move on location nailed and announcement to industry at large.
- Use the workshop- to have each sub-team- panel discussion 30-minute presentation. 30-45 minutes feed back.
- 12 hours of workshop time.
- Anticipate 500-1000 showing up to participate in the workshop.
- SDT team members show up. Planning day.
- Workshop objective is to get the SDT additional informal industry comment.

The Chair and Vice Chair noted that the Team had made a lot of progress over the course of the meeting. They reviewed the short term schedule for the Sub-teams. They will be meeting weekly as will the Sub-Team Leads to help coordinate the development of the drafts.
There is a lot of work to complete. Sub-teams may be scheduling additional working sessions and coordinating with Joe Bucierro. The SDT needs to enter its April meeting with a good draft
Sub-team should use Howard Gugel early and often.

The SDT requested that Friday sessions should clearly note if noon is the adjournment time so that members can make travel arrangements accordingly.

The Chair and Vice Chair and the SDT thanked Bill Winters for his excellent hosting and great facilities. Bill offered to host later in the year and will follow up with Joe Bucciero.

The meeting adjourned at 12:15 p.m.

Appendix # 1— Meeting Agenda

Project 2008-06 Cyber Security Order 706 SDT
Draft 20th Meeting Agenda
March 9, 2010, Tuesday- 1 PM to 5:30 PM MST
March 10, 2010 Wednesday- 8 AM to 5 PM MST
March 11, 2010 Thursday- 8 AM to 5 PM MST
March 12, 2010 Friday- 8 AM to 12 PM MST
Arizona Public Service CHQ
400 N. 5th St.
Phoenix, AZ 85004

NOTE:
1. Agenda Times May be Adjusted as Needed during the Meeting
2. Drafting Team Meetings May Not Have Access to Telephones and Ready Talk

Proposed Meeting Objectives/Outcomes

- Review the revised CSO 706 SDT 2010 Work plan and Convergence Schedule Proposal
- Receive updates on other related cyber security initiatives
- Receive a NERC update on implementing the CIP Communication Plan and May 2010 Technical Workshop
- Review, discuss industry comments and identify issues raised to be addressed in revised CIP-002-4
- Review, refine and test consensus on a revised draft CIP 002-4 and Industry Response Document
- Receive progress reports for Security Controls Requirements Sub-Teams
- Develop and Test Sub-Team Security Controls Requirements
- Agree on next steps and assignments

Draft Agenda

Tuesday	**March 9, 2009**
1:00 p.m.	Welcome and Opening Remarks- *John Lim, Chair & Phil Huff, Vice Chair* Roll Call; NERC Antitrust Compliance Guidelines Facilitator review and SDT acceptance of February 16-19, 2010 Austin SDT meeting summary
1:10	Review of Meeting Objectives, Agenda and Meeting Guidelines- *Bob Jones*
1:15	Review and Discussion of CSO 706 SDT Workplan and Convergence Schedule - March-December, 2010- *Stu Langton*
1:45	Updates on other related cyber security initiatives- *NERC Staff and SDT Members*
1:55	Update on CIP Communication Plan and May 2010 Technical Workshop - *Carl Dombek*
2:15	Review of Revised CIP-002-4 Draft based on Industry and SDT Response to Industry Comments- *Draft CIP-002 Drafting Team, John Lim et al.*

3:00	*Break*
3:15	Continue review and discussion of revised draft CIP 002-4
5:25	Review of Proposal for Wednesday Agenda
5:30	*Recess*

- *Possible Security Controls Requirements Sub Team Meetings- Evening*
- *If needed, CIP-002 Drafting Team to meet to finalize draft and present for adoption Wednesday morning.*

Wednesday **March 10, 2010**

8:00	Welcome and Agenda Review, Roll Call and Antitrust Guidelines- *John Lim, Phil Huff, Joe Bucierro*
8:10	Review and Consideration of draft CIP-002-4 as revised and the Industry Comments Response Document
9:00	Sub-team Progress Reports and SDT Discussion of Key and Any Overlapping Issues

- Security Governance
- Personnel and Physical Security
- Operations Security
- Recovery and Response
- Access Control and Auditing
- Change Management, System Lifecycle and Information Management

10:30	Break
11:00	Review of Guidance and Overall Format for Security Controls Requirements Sub-teams
10:45	Sub-team Progress Reports and SDT Discussion of Key Issues- *Continued*
11:45	Security Controls Sub-Teams
12:00	*Working Lunch*
1:00	Security Controls Sub-Teams
4:55	Review Assignments and Thursday Agenda
5:00	*Recess*

- *Possible Security Controls Requirements Sub Team Meetings- Evening*

Thursday **March 11, 2010**

8:00	Welcome and Agenda Review, Roll Call and Antitrust Guidelines- *John Lim, Phil Huff, Joe Bucierro*
8:10	Security Controls Sub-Teams
10:00	Break
10:15	Security Controls Sub-Teams
12:00	*Working Lunch*
1:00	Sub-Team Reports and Full Team Consensus Testing on Refinements
3:00	Break
3:15	Sub-Team Reports and Full Team Consensus Testing on Refinements-*Continued*
4:45	Review Any Drafting Assignments and Friday Agenda
5:00	*Recess*

- *Possible Security Controls Requirements Sub Team Meetings- Evening*

Friday	**March 12, 2010**
8:00	Welcome and Agenda Review, Roll Call and Antitrust Guidelines- *John Lim, Phil Huff, Joe Bucierro*
8:10	Sub-Team Reports and Full Team Consensus Testing on Refinements-*Continued*
10:15	*Break*
10:30	Sub-Teams Reconvene to Review Refinements, Schedule and Assignments
11:00	Next Steps CIP 002 Drafting Group
11:15	Review of May 2010 Technical Workshop Planning and Preparation
11:45	Review and Agree on Next Steps and Meeting Evaluation
12:00	*Adjourn & Lunch*

Appendix # 2 Attendees List
March 9-12, 2010, Phoenix, Arizona

Attending in Person — SDT Members and Staff

1. Rob Antonishen	Ontario Power Generation (Thurs)
2. Jay S. Cribb	Information Security Analyst, Southern Company Services
3. Jackie Collett	Manitoba Hydro (Wed/Thurs)
4. Sharon Edwards	Duke Energy
5. Jeff Hoffman	U.S. Bureau of Reclamation, Denver
6. Gerald S. Freese	Director, Enterprise Info. Security America Electric Pwr.
7. Phillip Huff, Vice Chair	Arkansas Electric Coop Corporation *(March 10-12)*
8. Doug Johnson	Exelon Corporation – Commonwealth Edison
9. Frank Kim	Hydro One Networks Inc.
10. Rich Kinas	Orlando Utilities Commission
11. Patricio Leon	Southern California Edison
12. John Lim, Chair	CISSP, Department Manager, Consolidated Edison Co. NY
13. David Norton	Entergy *(March 9)*
14. David S. Revill	Georgia Transmission Corporation
15. Scott Rosenberger	Luminant Energy
16. Kevin Sherlin	Sacramento Municipal Utility District
17. Jonathan Stanford	Bonneville Power Administration
18.Keith Stouffer	National Institute of Standards & Technology
19. William Winters	Arizona Public Service, Inc.
Roger Lampilla	NERC
Scott Mix	NERC
Howard Gugel	NERC
Joe Bucciero	NERC/Bucciero Consulting, LLC
Robert Jones	FSU/FCRC Consensus Center
Hal Beardal	FSU/FCRC Consensus Center
Stuart Langton	FSU/FCRC Consensus Center

SDT Members Attending via ReadyTalk and Phone

21. Jim Brenton	ERCOT
22. John D. Varnell	Technology Director, Tenaska Power Services Co.

SDT Members Not Participating

Joe Doetzl	Manager, Information Security, Kansas City Pwr. & Light Co

Others Attending in Person

John Van Boxtel	WECC
Brian Newell	AEP
Clyde Poole	TDITX
Sam Merrell	CERT

Others Attending via WebEx and Phone

Andres	Lopez	andres.lopez@usace.army.com
Rod	Hardiman	rchardim@southernco.com
John	Fridye	jfridye@rrienergy.com
Keith	Walters	step@eei.org
James	Bassett	james.bassett@invensys.com
Steve	Newman	srnewman@midamerican.com
John	Van Boxtel	jvanboxtel@wecc.biz
Maggy	Powell	margaret.powell@constellation.com
Bill	Keagle	william.a.keagle.jr@constellation.com
Steve	Newman	srnewman@midamerican.com
Bryn	Wilson	wilsonwb@oge.com
Ray	Andrews	randrews@involta.com
Sam	Merrell	smerrell@cert.org
andres	lopez	andres.lopez@usace.army.mil
William	Keagle	william.a.keagle.jr@constellation.com
Bill	Glynn	bill.glynn@westarenergy.com
John	Allen	john.allen@cityutilities.net
Annette	Johnston	ajjohnston@midamerican.com

Appendix # 3 — NERC Antitrust Compliance Guidelines

I. General

It is NERC's policy and practice to obey the antitrust laws and to avoid all conduct that unreasonably restrains competition. This policy requires the avoidance of any conduct that
violates, or that might appear to violate, the antitrust laws. Among other things, the antitrust laws forbid any agreement between or among competitors regarding prices, availability of service, product design, terms of sale, division of markets, allocation of customers or any other activity that unreasonably restrains competition.

It is the responsibility of every NERC participant and employee who may in any way affect
NERC's compliance with the antitrust laws to carry out this commitment.

Antitrust laws are complex and subject to court interpretation that can vary over time and from one court to another. The purpose of these guidelines is to alert NERC participants and employees to potential antitrust problems and to set forth policies to be followed with respect to activities that may involve antitrust considerations. In some instances, the NERC policy contained in these guidelines is stricter than the applicable antitrust laws. Any NERC participant or employee who is uncertain about the legal ramifications of a particular course of conduct or who has doubts or concerns about whether NERC's antitrust compliance policy is implicated in any situation should consult NERC's General Counsel immediately.

II. Prohibited Activities

Participants in NERC activities (including those of its committees and Subroups) should refrain from the following when acting in their capacity as participants in NERC activities (e.g., at NERC meetings, conference calls and in informal discussions):

- Discussions involving pricing information, especially margin (profit) and internal cost
- information and participants' expectations as to their future prices or internal costs.
- Discussions of a participant's marketing strategies.
- Discussions regarding how customers and geographical areas are to be divided among competitors.
- Discussions concerning the exclusion of competitors from markets.
- Discussions concerning boycotting or group refusals to deal with competitors, vendors or suppliers.

III. Activities That Are Permitted

From time to time decisions or actions of NERC (including those of its committees and Subroups) may have a negative impact on particular entities and thus in that sense adversely
impact competition. Decisions and actions by NERC (including its committees and Subroups) should only be undertaken for the purpose of promoting and maintaining the reliability and adequacy of the bulk power system. If you do not have a legitimate purpose consistent with this objective for discussing a matter, please refrain from discussing the matter during NERC meetings and in other NERC-related communications.

You should also ensure that NERC procedures, including those set forth in NERC's Certificate of Incorporation and Bylaws are followed in conducting NERC business. Other NERC procedures that may be applicable to a particular NERC activity include the following:

- Reliability Standards Process Manual
- Organization and Procedures Manual for the NERC Standing Committees
- System Operator Certification Program

In addition, all discussions in NERC meetings and other NERC-related communications should be within the scope of the mandate for or assignment to the particular NERC committee or Subroup, as well as within the scope of the published agenda for the meeting.

No decisions should be made nor any actions taken in NERC activities for the purpose of giving an industry participant or group of participants a competitive advantage over other participants. In particular, decisions with respect to setting, revising, or assessing compliance with NERC reliability standards should not be influenced by anti-competitive motivations.

Subject to the foregoing restrictions, participants in NERC activities may discuss:

- Reliability matters relating to the bulk power system, including operation and planning matters such as establishing or revising reliability standards, special operating procedures, operating transfer capabilities, and plans for new facilities.
- Matters relating to the impact of reliability standards for the bulk power system on
- electricity markets, and the impact of electricity market operations on the reliability of the bulk power system.

- Proposed filings or other communications with state or federal regulatory authorities or other governmental entities.
- Matters relating to the internal governance, management and operation of NERC, such as nominations for vacant committee positions, budgeting and assessments, and
- employment matters; and procedural matters such as planning and scheduling meetings.

Any other matters that do not clearly fall within these guidelines should be reviewed with NERC's General Counsel before being discussed.

APPENDIX # 4
CSO 706 SDT MEETING SCHEDULE
JANUARY –DECEMBER 2010

Schedule Convergence: Full CIP V4 Package		
Date	**Week of**	**CIP Task**
SDT Meeting-Atlanta, (4/13-16)	4/12/2010	**Present Controls draft for full team review and comment. Sub team drafting. Finalize draft for Informal Comment, Full Package**
	4/19/2010	**NERC Prepares Full Package for Industry Comment**
	4/26/2010	**SDT Reviews and Approved Full Package for 30-day Industry Comment Period**
5/3/2010	5/3/2010	***Informal Comment Posting for full package starts Completes on 6/2/2010***
SDT Meeting-Dallas, (5/11-14)	5/10/2010	**Prepare for Industry Workshop**
5/19 & 5/20/2010	5/17/2010	**1.5-day Industry Technical Workshop (Dallas, TX)**
	5/24/2010	**SDT Considers Comments from Workshop**
6/4/2010	*5/31/2010*	***2nd Informal comment period ends***
6/2/2010		***Comment Period Ends***
6/3-6/4/2010		***SDT Summarizes Comments Received***
SDT Meeting, Sacramento (6/8-11)	6/7/2010	**SDT Meeting: Comment review, response process, re-drafting, as needed**
	6/14/2010	Sub team meetings
	6/21/2010	Sub team meetings
6/29/2010	6/28/2010	Sub team meetings. SDT interim online meeting.
	7/5/2010	Subteams Package modifications into Standard documents
SDT Meeting, Pittsburgh, (7/13-16)	7/12/2010	**Finalize & Approve Documents for posting for 45 day formal comment period**

Schedule Convergence: Full CIP V4 Package		
Date	**Week of**	**CIP Task**
	7/19/2010	***NERC Prepares Materials/SDT Approves Revisions/NERC Seeks SC Approval for Ballot***
7/26/2010	7/26/2010	***45 Day formal comment period starts (completes 9/8/10) /Ballot Pool formation (completes 8/25/10)***
	8/2/2010	**Industry Comments on Standards**
SDT Meeting, TBD, (8/10-13)	8/9/2010	**SDT Meeting: Prepare for Industry Webinar**
8/18/10	*8/16/2010*	***Hold Industry Webinar***
8/25/2010	8/23/2010	***30 Ballot Preview/Initial Comment Preview ends/Ballot Pool formed***
8/30/2010	*8/30/2010*	***Initial Ballot Starts***
SDT Meeting Winnipeg, (9/7-10)	9/6/2010	**Respond to comments received. Drafting revisions. Review Ballot Results and Additional Comments**
	9/8/2010	**Initial Ballot Ends**
	9/13/2010	Sub team meetings
9/24/10	9/20/2010	Sub team meetings; Full SDT on-line meeting to adopt revised draft of documents
	9/27/2010	NERC Staff Review of Documents and SDT Approval for Re-ballot
10/4 to 10/13/10	10/4/2010	Re-Ballot Period Begins
SDT Meeting TBD, (10/12-15)	10/11/2010	**Prepare responses to 2nd ballot comments**
10/19/2010	*10/18/2010*	***Sub-teams meet to adjust requirements***
10/29/2010	10/25/2010	***Prepare & Finalize revisions to standards and responses to comments on standards***
	11/1/2010	NERC Staff Review of Documents and SDT Approval for Re-ballot
11/8 to 11/17/2010	11/8/2010	3rd Ballot Period Begins

Schedule Convergence: Full CIP V4 Package		
Date	**Week of**	**CIP Task**
SDT Meeting TBD, (11/16-19)	11/15/2010	**Prepare responses to 3rd Ballot comments**
	11/22/2010	*NERC & SDT finalize responses to ballot package*
	11/29/2010	*Seek SC & BOT Approval for Filing*
	12/6/2010	*Seek SC & BOT Approval for Filing*
SDT Meeting TBD, (12/13-17)	12/13/2010	**SDT Meeting to review Filing and Celebrate Project Completion**
	12/24/2010	*Submit for Regulatory Approval*

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Appendix #5

CSO 706 SDT DRAFTING SUB-TEAMS AND DRAFTING GUIDANCE

Sub-Team	NERC Standards and DHS Control Families	Team Members
Security Governance	CIP-003 – R1, R2, R3; CIP-005 R4, CIP-007 R8 DHS 2.1 Security Policy, DHS 2.2 Organizational Security, DHS 2.7 Strategic Planning, DHS 2.17 Monitoring and Reviewing Control System Security Policy, DHS 2.18 Risk Management and Assessment, DHS 2.19 Security Program Management	Jon Stanford (Lead), Jerry Freese, Dave Norton
CIP 002-4	Draft revisions to CIP-002-4, and Summary of Responses to Industry comments	John Lim, Dave Revill, Rich Kinas, Jim Brenton, Jackie Collett, Bill Winters, Dave Norton *Rod Hardiman (Observer)*
Personnel and Physical Security	CIP-004 – R1, R2, R3, CIP-006 R1 through R6 DHS 2.3 Personnel Security, DHS 2.11 Security Awareness and Training DHS 2.4 Physical and Environmental Security,	Doug Johnson (Lead), Rob Antonishen, Patrick Leon, Kevin Sherlin
Operations Security	CIP-005 R1, R3 CIP-007 R2, R3, R4, R6 DHS 2.8 System and Communication Protection DHS 2.14 System and Information Integrity	Jay Cribb (Lead), Jim Brenton, Jackie Collette, John Varnell
Recovery and Response	CIP-008 R1 & R2 CIP-009 R1 through R5 Incidence Response and Contingency Planning	Scott Rosenberger (Lead), Joe Doetzl, *Observer Participants: Jason Marshall*
Access Control and Auditing	CIP-003 R5; CIP-005 R2; CIP-007 R5; CIP 004 R4 DHS 2.15 Access Control DHS 2.16 Audit and Accountability	Sharon Edwards (Lead), Jeff Hoffman, Frank Kim *Observer Participants: Sam Merrell*
Change Management, System Lifecycle and Information Management	CIP-003 R6; CIP-007 R1, R7 CIP-003 R4; CIP-005 R5.1.1, R5.1.3 DHS 2.5 System and Services Acquisition, DHS 2.6 Configuration Management and System Lifecycle, DHS 2.10 System Development and Maintenance DHS 2.9 Information and Document Management, DHS 2.13 Media Protection	Keith Stouffer, Phil Huff (Lead) *Observer Participants: John Fridye*

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Security Controls Sub-Team Principles and Drafting Guidance

CSO 706 SDT SECURITY CONTROLS SUB-TEAM DRAFTING PRINCIPLES

(ADOPTED BY CSO 706 SDT, JANUARY, 2010)

1. Applicability [NERC ROP] Each reliability standard shall clearly identify the functional classes of entities responsible for complying with the reliability standard, with any specific additions or exceptions noted.	**9.Practicality** [NERC ROP] – Each reliability standard shall establish requirements that can be practically implemented by the assigned responsible entities within the specified effective date and thereafter.
2.Reliabiliy Objective [NERC ROP] Each reliability standard shall have a clear statement of purpose that shall describe how the standard contributes to the reliability of the bulk power system.	**10. Consistent Terminology** [NERC ROP] To the extent possible, reliability standards shall use a set of standard terms and definitions that are approved through the NERC reliability standards development process.
3.Performance Requirement or Outcome (NERC ROP) Each reliability standard shall state one or more performance requirements, which if achieved by the applicable entities, will provide for a reliable bulk power system, consistent with good utility practices and the public interest.	**11. Commensurate Controls for BES Impact Categories.** Security controls shall be commensurate with the identified level of BES impact categories.
4. Measurability (ROP) Each performance requirement shall be stated so as to be objectively measurable by a third party with knowledge or expertise in the area addressed by that requirement.	**12. Change Documentation.** Changes from prior versions of CIP Standards have clear rationale. These include the following types of changes: a. Above and beyond the current standards; b. Removal of requirements; and c. Major formatting changes.
5.Technical Basis in Engineering and Operations [NERC ROP] Each reliability standard shall be based upon sound engineering and operating judgment, analysis, or experience, as determined by expert practitioners in that particular field.	**13. Reduce Administrative Overhead**. Administrative documentation shall be kept to the minimum that is necessary
6. Completeness (NERC ROP) Reliability standards shall be complete and self-contained. The standards shall not depend on external information to determine the required level of performance.	**14. Priority.** Implementation plans for the Standards are prioritized according to level of BES impact.
7. Consequences for Non-Compliance [NERC ROP] In combination with guidelines for penalties and sanctions, as well as other ERO and regional entity compliance documents, the consequences of violating a standard are clearly presented to the entities responsible for complying with the standards.	**15. Eliminate or Minimize TFEs.** Security controls shall eliminate or at least minimize the need for TFEs. Allow for compensating controls to mitigate the need for a TFE.
8. Clear Language [NERC ROP] – Each reliability standard shall be stated using clear and unambiguous language. Responsible entities, using reasonable judgment and in keeping with good utility practices, are able to arrive at a consistent interpretation of the required performance.	

SECURITY CONTROLS SUB-TEAM
PROCESS AND DRAFTING GUIDANCE AND DELIVERABLES

Guidance from the January, 2010 Tucker Meeting and the February 2010 Austin Meeting

For the purpose of maintaining consistency across the teams and capturing interim decisions and change documentation, each team should utilize the following development process:

1. **DHS Catalogue of Controls:** Begin by identifying applicable controls that are enumerated in the *DHS Catalog of Control System Security Recommendations* for High Impact Cyber Systems.
2. **Cross Reference CIP Version 3 Requirements/sub-Requirements:** For each security control identified in step 1, cross reference the CIP version 3 Requirement/sub-Requirement or validate previous mapping work.
3. **Specific not Prescriptive:** As a general rule, be specific but not prescriptive in writing the requirements.
4. **"What" not "How":** In general, seek to draft a "what" requirements, not "how" requirements.
5. **Develop the requirement language** for each security control identified in step 1.
   a. When mapping to existing CIP requirements, use language from CIP, making improvements where needed.
   b. When no associated requirement from CIP exists, develop the new requirement using language from the *DHS Catalog.*
6. **Document significant changes to CIP Standards:** Document significant changes made to previous versions of the CIP Standards. Conceptual or broad changes can be captured by a single statement.
7. **Incorporate existing CIP requirements not mapped to the *DHS Catalog*.** If a requirement is no longer necessary because the intent was captured elsewhere, then include this in the change documentation.
8. **Address specific directives from FERC Order 706** that may be applicable to the requirement.
9. **Analysis and Determination of Requirements for Medium and Low Impact:** In the analysis and determination of applicability of requirements to Medium and Low Impact Cyber Systems, consider the cost in relation to the security benefits (i.e., a minimal cost requirement that significantly mitigates risk would apply to *ALL* Cyber Systems. Similarly, a significant cost requirement that minimally reduces risk or provides little additional security may apply only to *HIGH* impact Cyber Systems).
10. **Specify Applicability to Environments:** Specify applicability of a requirement to Generation, Transmission, and/or Control Center environments.
11. **Apply Requirements to BES Cyber System:** Requirements should apply to either:
    (a) The BES Cyber System as a whole, or
    (b) Components of the BES Cyber System. However, when a requirement only applies to specific types of components, Sub-Teams should describe those types of components to determine where component classes exist.

(c) Requirements specific to boundary protection or ESP can be written to the interface of the BES Cyber System.

12: **Level of Requirements:** Sub-Teams should generally write the requirements at a high enough level to avoid applicability of specific technology. Where there are applicable CIP requirements, start with the CIP words and tweak if needed to include some DHS language/concept. However, the "level" of the requirements text should be raised, if needed.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Agenda
Cyber Security Order 706 SDT — Project 2008-06

April 13, 2010 |1 PM to 5:30 PM EDT
April 14, 2010 | 8 AM to 6:15 PM EDT
April 15, 2010 | 8 AM to 5 PM EDT
April 16, 2010 | 8 AM to 2 PM EDT

Georgia Power
241 Ralph McGill Blvd
Atlanta, GA 30308

NOTE: 1. Agenda Times May be Adjusted as Needed during the Meeting
2. Drafting Sub-Team Meetings May Not Have Access to Telephones and Ready Talk

Proposed Meeting Objectives/Outcomes

- Review the CSO 706 SDT 2010 Work plan and Schedule
- Review, refine and adopt the Draft Final CIP-002-4 for NERC Staff Review in advance of Industry Informal Comment posting on May 3.
- Review, refine and adopt the Sub-Team Security Controls Requirements draft for NERC Staff
- Review in advance of Industry Informal Comment posting on May 3.
- Develop Related Documents including Comment Form and Cover Letter for Informal Comment Posting.
- Agree on next steps and assignments

Draft Agenda

Tuesday April 13, 2009

1:00 p.m.	Welcome and Opening Remarks- *John Lim, Chair & Phil Huff, Vice Chair* Roll Call; NERC Antitrust Compliance Guidelines - *Joe Bucciero* Facilitator review and SDT acceptance of March 9-12, 2010 Phoenix SDT meeting summary
1:10	Review of Meeting Objectives, Agenda and Meeting Guidelines — *Bob Jones*
1:15	Review and Discussion of CSO 706 SDT Workplan and Schedule - April-December, 2010- *Stu Langton*
1:20	Overview of CIP-002-4 & Security Controls Requirements Refinements
1:30	Review of Revised CIP-002-4 Draft Final and SDT Industry Response Document- *CIP-002-4 Drafting Team - John Lim, et al.*

3:00	Break
3:15	Continue Review of Revised CIP-002-4
4:15	Full Team Consensus Testing on Refinements of CIP 002-4 Draft Final and SDT Industry Response Document
5:15	Review of Wednesday's Agenda
5:30	Recess

- *Possible Security Controls Requirements Sub Team Meetings- Evening*
- *If needed, CIP-002 Drafting Team to meet to finalize draft and present for adoption Wednesday morning.*

Wednesday April 14, 2010

8:00	Welcome and Agenda Review, Roll Call and Antitrust Guidelines- *John Lim, Phil Huff, Joe Bucciero*
8:10	*(As Needed)* Review of Any Revisions and Adoption of CIP-002-4
9:00	Sub-Team Reports on Requirements Drafting and Any Overlaps
9:10	Security Governance Requirements
10:00	Break
10:15	Personnel and Physical Security Requirements and Guidance- Overview and Consensus Testing
11:00	Operations Security Requirements and Guidance - Overview and Consensus Testing
11:45	Recovery and Response Requirements- Overview and Consensus Testing
12:15	Working Lunch
12:45	Access Control and Auditing- Requirements- Overview and Consensus Testing
1:30	Change Management, System Lifecycle and Information Management- Requirements-Overview and Consensus Testing
2:15	*Security Controls Requirements Sub Team Meetings to Refine Documents for Thursday Review*
6:15	*Recess*

Thursday April 15, 2010

8:00	Welcome and Agenda Review, Roll Call and Antitrust Guidelines- *John Lim, Phil Huff, Joe Bucciero*
8:10	Security Governance Requirements
9:15	Personnel and Physical Security Requirements and Guidance- Overview and Consensus Testing
10:15	Break
10:30	Operations Security Requirements and Guidance - Overview and Consensus Testing
11:30	Recovery and Response Requirements- Overview and Consensus Testing
12:15	Working Lunch
12:45	Access Control and Auditing- Requirements- Overview and Consensus Testing
1:45	Change Management, System Lifecycle and Information Management- Requirements- Overview and Consensus Testing

2:45	Review of Progress and Drafting Assignments
3:15	*Possible Sub-Team and Ad Hoc Drafting Groups* Cover Letter, Comment Form, Implementation Plan, VSLs/VFRs Drafting Meetings
4:55	Review Any Drafting Assignments and Friday Agenda
5:00	Recess

- *As needed sub-team and ad-hoc drafting groups- Evening*

Friday April 16, 2010

8:00	Welcome and Agenda Review, Roll Call and Antitrust Guidelines- *John Lim, Phil Huff, Joe Bucciero*
8:10	Final Review of CIP Drafts for NERC Staff Review
10:15	*Break*
10:30	Final Review and Adoption of CIP Drafts for NERC Staff Review
12:15	Working Lunch
12:45	SDT Review of Document Preparation Schedule Proposed Sub-Team Lead meetings with NERC Staff April 21 & 26 SDT Teleconference Meeting week of April 29 to Review and Adopt Documents for Posting for Informal Industry Comment on May 3.
1:00	SDT Review of Plan to Draft CIP Guidance Documents on May Meeting
1:15	Review of Dallas SDT Agenda
1:25	May 2010 Technical Workshop Planning, Assignments, and Preparation, as needed
1:55	Agree on Next Steps and Meeting Evaluation
2:00	*Adjourn*

SCHEDULE CONVERGENCE: FULL CIP V4 PACKAGE		
Date	**Week of**	**CIP Task**
SDT Meeting- Atlanta, (4/13-16)	4/12/2010	**Present Controls draft for full team review and comment. Sub team drafting. Finalize draft for Informal Comment, Full Package**
	4/19/2010	**NERC Staff Prepares Full Package for Industry Comment**
4/21/2010	*4/19/2010*	*Proposed NERC Staff Meeting with SDT Sub-Team Leads- Mid-stream Review of Package Preparation*
4/26/2010	*4/26/2010*	*Proposed NERC Staff Meeting with SDT Sub-Team Leads- Final Review of Package Preparation*
4/29/2010	4/26/2010	**SDT Reviews and Approved Full Package for 30-day Industry Comment Period**
5/3/2010	5/3/2010	*Informal Comment Posting for full package starts Completes on 6/2/2010*
SDT Meeting- Dallas, (5/11-13)	5/10/2010	**Prepare for Industry Workshop- CIP Guidance Documents**
5/19 & 5/20/2010	5/17/2010	**1.5-day Industry Technical Workshop (Dallas, TX)**
	5/24/2010	**SDT Considers Comments from Workshop**
6/2/2010	*5/31/2010*	*2nd Informal comment period ends*
6/3-6/2010		*SDT Summarizes Comments Received*

SDT Meeting, Sacramento (6/8-11)	6/7/2010	**SDT Meeting: Comment review, response process, redrafting**
	6/14/2010	Sub team meetings
	6/21/2010	Sub team meetings
6/29/2010	6/28/2010	Sub team meetings. SDT interim online meeting.
	7/5/2010	Subteams Package modifications into Standard documents
SDT Meeting, Pittsburgh, (7/13-16)	7/12/2010	**Finalize & Approve Documents for posting for 45 day formal comment period**
	7/19/2010	*NERC Prepares Materials/SDT Approves Revisions/NERC Seeks SC Approval for Ballot*
7/26/2010	7/26/2010	*45 Day formal comment period starts (completes 9/8/10) /Ballot Pool formation (completes 8/25/10)*
	8/2/2010	**Industry Comments on Standards**
SDT Meeting, TBD, (8/10-13)	8/9/2010	**SDT Meeting: Prepare for Industry Webinar**
8/18/10	*8/16/2010*	*Hold Industry Webinar*
8/25/2010	8/23/2010	*30 Ballot Preview/Initial Comment Preview ends/Ballot Pool formed*
8/30/2010	*8/30/2010*	*Initial Ballot Starts*
SDT Meeting Winnipeg, (9/7-10)	9/6/2010	**Respond to comments received. Drafting revisions. Review Ballot Results and Additional Comments**
	9/8/2010	**Initial Ballot Ends**
	9/13/2010	Sub team meetings

9/24/10	9/20/2010	Sub team meetings; Full SDT on-line meeting to adopt revised draft of documents
	9/27/2010	NERC Staff Review of Documents and SDT Approval for Re-ballot
10/4 to 10/13/10	10/4/2010	Re-Ballot Period Begins
SDT Meeting TBD, (10/12-15)	10/11/2010	**Prepare responses to 2nd ballot comments**
10/19/2010	*10/18/2010*	*Sub-teams meet to adjust requirements*
10/29/2010	10/25/2010	*Prepare & Finalize revisions to standards and responses to comments on standards*
	11/1/2010	NERC Staff Review of Documents and SDT Approval for Re-ballot
11/8 to 11/17/2010	11/8/2010	3rd Ballot Period Begins
SDT Meeting TBD, (11/16-19)	11/15/2010	**Prepare responses to 3rd Ballot comments**
	11/22/2010	*NERC & SDT finalize responses to ballot package*
	11/29/2010	*Seek SC & BOT Approval for Filing*
	12/6/2010	*Seek SC & BOT Approval for Filing*
SDT Meeting TBD, (12/13-17)	12/13/2010	**SDT Meeting to review Filing and Celebrate Project Completion**

	12/24/2010	*Submit for Regulatory Approval*

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Notes
Cyber Security Order 706 SDT — Project 2008-06

April 13, 2010 | 1:00 PM to 5:00 PM EDT
April 14, 2010 | 8:00 AM to 5:00 PM EDT
April 15, 2010 | 8:00 AM to 5:00 PM EDT
April 16, 2010 | 8:00 AM to 1:00 PM EDT

Unanimously Adopted, May 13, 2010

Robert Jones, Stuart Langton, and Hal Beardall
Facilitation and Meeting Design
FCRC Consensus Center, Florida State University

Joe Bucciero, Bucciero Consulting, LLC

http://www.nerc.com/filez/standards/Project_2008-06_Cyber_Security.html

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

CSO706 SDT April 13-16, 2010 Meeting Summary Contents

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

CSO706 SDT APRIL 13-16, 2010 MEETING
EXECUTIVE SUMMARY

On Tuesday afternoon, the Chair, John Lim welcomed the members to the SDT's 21st meeting. Joe Bucciero conducted a roll call of members and participants in the room and on the conference call. The host Jay Cribb, a SDT member, welcomed everyone to the facilities and covered logistics. Bob Jones, facilitator, reviewed the proposed meeting agenda. On Friday morning the SDT approved without objection the meeting summary for the March 9-12, 2010 SDT session in Phoenix, Arizona. Mr. Bucciero reviewed the need to comply with NERC's Antitrust Guidelines.

Stu Langton presented a proposed CSO 706 SDT schedule which was circulated within a day of the meeting and made adjustments in the process to allow for NERC reviews and formatting of materials.

John Lim provided an overview of the revisions of CIP-002 Draft Final and SDT Industry Response Document since the Phoenix meeting. The SDT discussed the following topics:

- "Immediately affect real time operations."
- Interconnections.
- Attachment 2, Item 1.6- 3 or more transmission lines.
- VSLs
- Miscellaneous topics including functions, compliance issues,

The Chair noted that since the Phoenix meeting, much work has been done by the CIP 002 Sub-team responding to the input and suggestions received. The Team sent to NERC staff a preliminary draft for their input. However subsequent to submitting the drafts to NERC, the Sub-teams produced further refinements to their drafts. The Team agreed to review the NERC comments and consider them in relation to the current draft of CIP-010. Howard Gugel led the SDT discussion of the NERC staff comments on the earlier draft of CIP-002 as well as various proposed edits, such as using the term "requirements" throughout the documents, utilizing owner/operator vs. user, defining "immediate" and "situational awareness." The SDT reviewed all of CIP 002 requirements and Attachments #1 and #2 and took a number of polls on whether to accept the proposed NERC edits.

On Friday, John Lim reviewed CIP 002 Sub-team's redline version to address some of the issues raised earlier in the meeting and reviewed the proposed language on: Definition of BES Cyber System and the definition of "immediate"; High impact rating; and Transmission facilities.

On Wednesday, the SDT reviewed the work of the CIP 003-009 Sub-teams since the Phoenix meeting (including Change Management; Access Control and Auditing; Recovery and Response; Operations; and Personnel and Physical Security). The SDT

focused first on reviewing and refining the Security Governance requirements including the proposed 9 category areas.

Wednesday evening the Chair asked Howard Gugel to prepare a sample "proof of concept" for the access control requirements to inform a decision regarding format of the standards.

Thursday afternoon the SDT reviewed each of the sub-team's draft requirements as revised and refined in the sub-team meetings on Wednesday, offering guidance on various issues raised by the draft requirements.

The SDT reviewed and confirmed previous decisions to use tables in the new CIP standards and to formulate objective statements for each requirement. Sharon Edwards presented the work to date on access control including CIP-004 R4, CIP-005 R2, CIP-008 R5 and dispersed throughout the standard as a way to highlighting the presentation of different formats. Following this the SDT reviewed three format options:

- **Option 1.** Keep CIP-003 to-009 and work from there.
- **Option 2**: retire existing CIP standards and organize the new standards by the topics in sequence from CIP-010 on. (e,g,.,Access Control could be CIP-017).
- **Option 3:** One big standard document with 2 sections CIP-010 (formerly CIP-002) and CIP-011 (formerly CIP-003 to -009). All controls requirements would be together in one CIP standard, with CIP-011:
  - R1 (security policies) addressing all topics.
  - R2 implement per table
  - R3- table for access control
  - R4 implement 2nd table (account specifications)
  - etc.

The Team following the discussion of the pros/cons of the options, voted first on each of the three options indicating its acceptability. Following that each Team member voted to support the option they found most acceptable or preferable based on the discussion and their perspective.

Format Option 1: keep existing CIP 003 to 009 in its current form maintaining its existing logical construct (may involve minor movement of existing requirements between standards)

Yes	*No*	*Indifferent/could go either way*
8	**7**	**3**

Format Option 2: Retire 003 to 009, create new CIP 011-17 grouping according to small group assignments.

Yes	*No*	*Indifferent/could go either way*
12	**2**	**6**

Format Option 3: Collapse CIP 003-009 into a single standard that contains all requirements created/edits by the sub-teams and grouped according to sub-team assignments.

Yes	*No*	*Indifferent/could go either way*
12	**7**	**2**

The team then voted for one of the two highest ranked options under consideration:

- Option 2: Retire 003 to 009, create new CIP 011-17 grouping according to small group assignments.
  ***Yes*=6**
- Option 3 Collapse CIP 003-009 into a single standard that contains all requirements created/edits by sub-teams and grouped according to sub-team assignments.
  ***Yes*=10**
- *Abstained from voting for Option #2 or #3:* 4

At the end of Thursday, the Team took up the format issue again. The Vice Chair made a proposal that the Team use Option 2 (which would renumber the requirements using the topics to organize them).

The facilitators polled the team on their support for the **Option #2 (multiple standards) and 7 of 16 members** were in support of utilizing this as the format. An additional member joined and the Team then tested support for **Option 3 (putting all into single standard) and 9 of 17 supported using this format.** Neither format approach received sufficient support to make an SDT decision.

The Team then reviewed and tested support for each of the following propositions:

1. Change from existing CIP numbering system? Yes- 13 favor changing (of 17 = 76%)
2. Adopt the proposed headings for the requirements as the categories whether as one or multiple standards? Yes-13 (of 17 = 76%)

On Friday morning the SDT took up the final review of format options for the informal posting document(s) in order to make a decision.

The facilitator suggested the SDT use an acceptability ranking of the two possible format options that had been discussed and debated yesterday followed by clarification of concerns to see if they could be met and a requisite number of members could agree on the format to use for the informal posting.

- **Option #2 – Requirements in Multiple Standards.** Use the Topical areas discussed on Thursday and utilize multiple standards (example CIP 010 -020). CIP 002 also gets re-numbered.
  4**=3,** 3**=7,** 2**=6,** 1-**0** *(Avg. 2.81)*

- **Option #3 – Requirements all in One Standard.** Use the Topical areas discussed on Thursday, but one new standard is posted containing sections for all topics. 4=**6,** 3=**5,** 2=**3,** 1=**2** *(Avg. 2.93)*

The 17 SDT members present then voted for their preference for posting for informal comment between the two options with the following result:

- **Option #2** *(multiple standards)* **Yes= 6 (35%)**
- **Option #3** *(single standard)* **Yes= 11 (65%)**

The SDT agreed that while this decision to post for informal comment has a majority support (65%) but not the super majority (75%) of the members called for in the decision rules, the Team is asking for industry comment and input on the formats through the comment form before finalizing a format to present in the formal comment draft in July, 2010. The Team discussed that this approach is consistent with the spirit of the following consensus rule provision: "In instances where the Team finds that even 75% acceptance or support is not achievable, the Team's report will include documentation of any differences as well as the options that were considered for which there was greater than 50% support from the Team."

On Friday the Chair reviewed the schedule, assignments and next steps for the SDT to produce a final version for posting on May 3, 2010. Joe Bucciero will lead, with assistance from Howard Gugel, preparation of the draft of comment form with information provided by each of the Sub-team leads. A question will also be added based on the discussion on the format of the CIP Standards. The SDT will need to begin creating an implementation plan for posting in July for formal comment. A small group of SDT members needs to be formed to provide some framework for discussion at the May meeting (in Dallas) and to answer any questions at the May SDT Workshop in Dallas. Scott Mix will be looking for individuals to work with him to prepare the Implementation Plan, and this will occur after May 3. The SDT agreed that the cover letter for the informal May 3 posting of the draft CIP Standards should speak to the SDT's philosophy on implementing the plan. Jackie Collett, John Lim and Doug Johnson agreed to work with Scott Mix on developing a draft implementation plan.

The Chair reviewed and the SDT agreed on the schedule of activities from Monday, April 19, to posting of the draft CIP Standards on Monday, May 3. The Chair and Vice Chair and the SDT thanked Jay Cribb for his excellent hosting and Southern Company for the great facilities.

The meeting adjourned at 12:00 p.m.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

CYBER SECURITY ORDER 706 SDT- PROJECT 2008-06
21ST MEETING SUMMARY

April 13-16, 2010
Atlanta, Georgia

I. AGENDA REVIEW AND WORKPLAN

A. Agenda Review

On Tuesday afternoon, the Chair, John Lim welcomed the members to the SDT's 21st meeting. Joe Bucciero conducted a roll call of members and participants in the room and on the conference call *(See Appendix #2*). The host Jay Cribb, a SDT member, welcomed everyone to the facilities and covered logistics. The Chair reviewed the following meeting objectives:

- Review the revised CSO 706 SDT 2010 Work plan and Schedule
- Receive updates on other related cyber security initiatives
- Receive a NERC update on implementing the CIP Communication Plan and the May 2010 Technical Workshop
- Review, refine and adopt the Draft Final CIP-002-4 for industry informal comment
- Review, refine and adopt the Sub-Team Security Control Requirements draft for industry informal comment
- Develop related CIP 002 and Security Controls Requirements Guidance Documents
- Agree on next steps and assignments

Bob Jones, facilitator, reviewed the proposed meeting agenda *(See appendix #1*). On Friday morning the SDT approved without objection the meeting summary for the March 9-12, 2010 SDT session in Phoenix, Arizona.

Mr. Bucciero reviewed the need to comply with NERC's Antitrust Guidelines *(See Appendix #3).* He urged the team and other participants in the process to carefully review the guidelines as they would cover all participants and observers. He urged all to avoid behaviors or appearance that would be anti-competitive nature and also reminded the group of the sensitive nature of the information under discussion.

B. Workplan Schedule Review

Stu Langton presented a proposed CSO 706 SDT schedule which was circulated within a day of the meeting and made adjustments in the process to allow for NERC reviews and formatting of materials. Joe Bucciero suggested the SDT might want to review this overnight and take up first thing on Wednesday morning.

II. CIP 002 REQUIREMENTS

A. Overview of CIP-002 Requirements

John Lim provided an overview of the revisions of CIP-010 Draft Final and SDT Industry Response Document since the Phoenix meeting, noting the following:

- R1 changes: "Uniquely" changed to the adverb "discretely,"
- Member comments and suggestions included: take the adjective out. Consider "discretely" "distinctly" May not need this word. The call is document all; this may be "lawyer bait."
- R2- "appropriately: added.
- Attachment 2. Used terms defined in the glossary. Didn't change thresholds. 1.2- struck generation. Threshold too high. 1.6- before had separate criteria for protective systems. And protected at 350 or higher without any qualifications. Covered all substations at 350 KV. Not intended. Merged with 1.11 with 1.6.
- Medium: thresholds lower than before. Protection systems with 3 or more lines. Rest fall into the medium.
- Member comments: 2.5- no fax systems- everyone is high? This is an oversight.
- Low Impact: added to be consistent with high and medium.

SDT Comments on Overview

"Immediately affect real time operations."

- Short range planning impact issue? Other situational awareness but not in the "immediately affect real time operations" language? Does it include next day planning?
- John Lim noted that they didn't have a consensus in the group on this.
- "Immediately"- what does this mean? Week, day, now? Are they needed.
- Maybe we should distinguish from planning and real time operation.
- Since you refer to operations planning in part 1. In part 2 need to apply to operations planning.
- Look at beginning of Attachment #1 language.
- Attachment 2- 1.1- "facilities – why combine generation facilities?
- BES cyber system is subject which covers shared cyber system.

Interconnections.

- Texas- lower requirement for ERCOT? Why a separate requirement for ERCOT? Different size in terms of megawatt capability and mode.
- Why have spinning reserve requirements higher in ERCOT?
- This focuses on the Texas and Quebec interconnections.

- Did SDT December posting allowed for regional variation? Not by regional variations but by interconnection variations. Numbers come from category 3 events.
- Definition of control center? Lower threshold will bring in more things. E.g. 1.7 medium- primary and backup control centers? Are these defined? How are they distinguished from control centers? Shouldn't assume everyone understands these terms.
- Work is being done on a NERC back up facilities standard. Went through initial ballot but didn't get support on that proposal.

1.6- 3 or more transmission lines.

- 1.6- what was technical basis behind 3 lines?
- 1.6- 3 or more transmission lines? Individual connectors? What about DC circuit with 2 lines on the tower? One transmission line or referred to as conductors or phases.
- In the context of transmission planning studies, 2 or more would be ridiculous. 3 or more is a good place to draw a line.
- We have redundant subsystems. 3 line threshold may be too low some companies.
- 5 transmission lines would be hard to justify for a national standard. 300 kv above and higher.
- Multiple entities have asked for the technical basis for this. Need to respond if we leave it at 3.
- "Or that remotely control a BES asset with a high impact rating" Asset= facility? Hardware?

VSLs

- VSLs measure R1 in terms of how many you miss. Assumes auditors know the right total. How will this be computed. This is defined by the entity. These are squishy number to begin with.
- Auditors won't use this. This is not looked at part of the audit itself. Use only when there is an alleged violation. After a potential violation an investigation is conducted to confirm a violation and the circumstances associated with a violation. Then someone comes to do analysis what the count should have been.
- Every requirement must have a VSL or FERC won't accept.
- We can make this a number vs. a %. 1, 2 or 3. Have not been identified more than 3 high.
- Previous VSLs had numbers. Some entities have suggested 5 could be a small number.
- Don't see the difference between 1 and %. Issue is entity is identifying the cyber system. Investigator and entity work together to define- a number or % calculated.
- Are we spending too much time on VSLs? Difficult to correlate the auditing fine and the VSLs. What value is added by debating VSLs *ad naseum*.
- What about using "misidentified"
- Get rid of % but develop better definition of the BES cyber system

Miscellaneous

- Is the whole functions area a mush?

- BES cyber system identification is up to the entity. Entities will appropriately draw the line in different ways.
- This is where we need NERC compliance to weigh in to provide advice to the SDT.
- Concrete recommendation: Eliminate line 1 on chart since it is untenable since you can't calculate a %.
- This is not an audit tool to determine if you have met the requirement.
- Requirement is to identify all BES cyber systems.
- First step is to find if you find a BES cyber system that wasn't identified. The investigator will develop the list.
- Add "Additional"?
- From #2, on it presupposes you have a list.

B. NERC Suggested Edits for CIP 002-4 *(Including Maureen Long and Dave Taylor)*

The Chair noted that since the Phoenix meeting, much work has been done by the 002 Sub-team responding to the input . The Team sent to NERC staff a preliminary draft for their input. However subsequent to that the Sub-teams produced further refinements to their drafts. The Team agreed to review the NERC comments in relation to the current draft 002. Howard Gugel led the SDT discussion of the NERC staff comments on an earlier draft of the SDT.

SDT Comments and Polls

Definitions section.

- Functions sentence should remain.
- List doesn't have a proper introduction in Dave's edits.
- Computer systems themselves are control centers, not the dispatch arena etc.? Not supporting
- In the field- this is a control center.
- Is there a something out there- is a computer or a programmable controller.
- This is the first time the SDT is using "computer systems"- will be confusion on this.
- Remote data collection equipment as well.
- A control system vs. control center? Leery to tying back to computers.
- Does fix some physical security if only around computer systems.
- Tied back to EOP 8. Do you need to define control center?
- Go back to original wording. Not trying to define BES cyber system.
- "associated"
- Propose striking second sentence.
- EOP 8- strong linkages with other standards raise double jeopardy issues.
- **Retaining the SDT language:**

Y	N
15	0

- **Add "Functions that support"**

Y	N
15	0

- "typically" in the second sentence)-
- For a definition, we should remove the second sentence.
- "At a minimum"? No.
- Are we removing reference to real time operations?

- Retain the 2nd sentence and remove "typically"?
- Delete: "listed below" in first sentence.
- All agreed. 002 Sub-team will follow up with these changes.
- Purpose addition. OK
- "including the date the identification was performed"? OK no objections all agreed.

R-1

- The 1st thing NERC suggested was to make 1 and 2 a single requirement that has 2 parts.
- If you don't put criteria on correctly but come up with violation. If you have list and criteria. Violation for either part? Or if stick with separately changes for R1 and R2. This might eliminate struggles with VSL statement earlier.
- R1- from "all " to "each"? "One or more" If we use R1. Why not make R3 subset of R1?
- NERC had advised against doing sub-requirements?
- Sub points not sub requirements. All one requirement. This is very confusing.
- Leaning towards keeping current structure.
- This format is being used in other standards. Filed with FERC. May be obligated to use. Either way may be acceptable.
- Benefit to sub numbering format. Keeps together things by. Sub numbers help clarify the numbers intent.
- In favor: of **Sub numbers option**

Y	N
7	9

- NERC's suggestions on R1. Requirement is to "identify" and "all" vs. "each". Identify and document each.
- **Should we accept the NERC R-1 recommendations?**

Y	N
1	16

- **Delete "Document"**

Y	N
2	15

- **"Each"**

Y	N
5	12

- Make sure you identify all cyber systems. Indentify suggests uniqueness.
- "Each" identify something- each in a set. Discreetly" problems with how you document. E.g. on multiple lists vs. 1 list.
- What do we mean by BES cyber system- box or applications? What does discreet"
- **Delete "Discreetly**

Y	N
16	0

- Use vs. own (regardless of whether you own it). E.g. I.d. 3rd party tagging application. Have to do something about. "Owns not uses"

- Note that asset owners and operators make for a big difference. Possibly use: "Owns, operates or owns/operates"
- Owner knows what the equipment is but the Operator may not.
- BES cyber systems that execute or enable?
- **"Owns" vs. "uses"**

Y	N
13	4

- Its got to be ownership or else there will be big headaches. Asset means ownership.
- What about jointly owned? Agreements/contracts would address those kinds of issues.
- SDT should lock it one way or another. There will be fewer exceptions with owned than "operates."
- To enable functions. Applicability is solved earlier. This is not the best place to deal with this. Applicability to the standard. The entity will resolve, not us.
- Leaving executes and enables?
- Taking out is not appropriate- Whatever we decide. It will bring comments. At least it is in the open in the informal comment process.
- This is not a new issue. There is joint ownership now under current standards. We operate generation for other. It all comes down to money.
- **"Own" (2nd poll)**

Y	N
11	6

- Figure out what we need to do with joint ownership. Technical owners vs. lease holders.
- Discreetly identify- make sure you can't have things in two cyber systems.
- There is no way to document if you haven't identified. Is this idea redundant?
- We will need to do better on documenting guidance- for industry.
- True requirement is identification. Document is the measure.
- "Appropriate?" This doesn't read well without this word.
- But "appropriate"- doesn't identify anything.
- Can we move benefits to reliability to a guidance document? No, benefits to reliability is needed for each requirement under NERC's current approach.
- **Strike "appropriate"**

Y	N
14	3

- R1. Is the last sentence on the objective superfluous language?
- Breaking out the objective of requirement offers great value in knowing what the objective was in terms to later determining intent.
- NERC's requirement is to set forth the "benefit to reliability." You need the who what and why set out in the requirement.
- Would it be possible to pull out separately? It is confusing to read. Are we bound by format?
- Could change wording, "for the application of security requirements and controls to BES cyber systems."
- SDT- consensus- ok.

R2

- John Lim indicated he believed the sub-team would not have problems with changes suggested by NERC.
- The SDT accepted the changes.
- Should we require "categorize and annually re-categorize."
- Delete re-categorize?
- "Annual" is better used in the attachment.
- **Delete "Re categorize" SDT Consensus= Yes.**
- "and document such categorization for" OK
- Missing a date here? Add here "including the date the identification was performed"?
- Will we have to put into every requirement?
- Look in measures- lists have to be dated. Have to tie this back to the requirement.
- Remove this language from the measure and the requirement. Y 16 N 0

R3

- Do R1 and R2 once. R3 from now on keep it up to date.10 years later you missed a system on the list. Do you violate R3, R1 or both?
- If you never made the change, then you missed it the first time.
- That is why the sub-team added "that it owns or operates "
- What if it is change because of a storm, not planned. "Emergency changes"?
- Concerned about consistency as we go through. End each with the benefit piece. Look at the different wording on R1, R2 and R3. Make consistent. If benefit the same, use same language. R1- to categorize
- Just voted down "owns or operates." Should we delete here? Want to monitor for changes.
- Planned vs. unplanned change. Have to keep the list fairly static. Changes in a planned way so you know to change the cyber system.
- Planned/unplanned—"planned"- triggering issues. May need to look at this some more.
- Is an annual refresh missing where you look at categorization to make sure something didn't happen that you missed?
- "Reviewing the categorization of the BES cyber systems"
- Remember these are minimum requirements. Do we want to state annually. Or leave it up to entity (best practice). If you have a planned change, you have to revisit it. People can revisit anytime they want.
- Can you have a change not specifically planned? To take a line out they have to do some studies to figure this out. This doesn't happen spontaneously.
- **Delete "or operates" yes. All**
- Transmission owners vs. operators- is a problem. R1 has it as "owns."
- Every one else who is a transmission operator. R1 and R2 have to identify assets (probably a control center).
- Categorization- if control center controls a high impact high asset, high impact control center.
- If we already have covered applicability, is it appropriate to put into requirements?
- **Delete "planned = no, All**

- **Add" "<u>the identification and categorization</u>"** Yes All
- **Add " annual review"? "Every 12 months or as …"** Y N
  1 16
- Comes up in R1 and R2- got rid because no reliability benefit.
- The requirement to notify changes to others is not here any longer?
- That is because the BES cyber system is categorized.
- Sub-team Ok with Dave Taylor's suggested edits.
- <u>"to the portion of the BES" ? OK</u> Planned changes for my stuff only.
- "Periodic reassessment?- CIP 002 sub-team dealt with.
- Other changes: calendar OK
- Difference between requirement and controls. Control objective statement 800-53. Writing requirements. Are we authorized to write controls? Source documents are controls based,
- **Use the word <u>requirements</u> throughout documents. All Agreed.**

Measures

- Delete discreetly? Yes, All agree.

Compliance

- Note that data retention language and the audit periods (3 or 6 year cycle). Gap of compliance only keep data for the year not the last audit. Need to keep data since the last time audited.

Attachment 1

- **Scoping statement important- place it first? Yes** Y N
  13 4
- Make this the first sentence?
- Since "real time" was added NERC staff struck the purpose paragraph.
- "Operations planning horizon" ? Do we want to include this in addition to "real time"?
- Planning could affect real time as well.
- This doesn't appear in any R, or attachment 2. List of functions only.
- Reconsider operations planning horizon in all requirements?
- When define the functions could take place in real time or in the operations planning horizon.
- **Reorder the 2 paragraphs? No** Y N
  3 16
- **Delete ~~"these functions take place in real time or operations.~~ Create a single paragraph**. **Yes** Y N
  14 3
- If you delete the above you will have to deal with word "immediately"
- Day ahead? Marketing term.
- Take out planning horizon?
- If you pick wrong units, in real time you will figure out.

- What we are after here are control systems. Protect- 1 and 0s turns into action out there.
- **Delete ~~Immediately ?~~** Y 11 N 6
- Initially defined "immediate" within 15 minutes"
- Real time? 1 hour or less in the NERC glossary. Upper case or affects the operations within 15 minutes.
- Need that kind time frame. We do need to maintain it. If you aren't specific, may put security controls where you don't need them.
- JVB: time frame- affecting real time. Leave immediately there and have real time (lower case).
- Further qualification? Is it and, and/or?
- Intent is the be "and"
- **Delete "further qualifications?" Yes** All
- Is "Immediate" related to ability to act?
- Concerned there could be other cyber systems that don't have immediate affect. The ones of greatest importance, at a minimum, should be protected- this should to be clear.
- **"Can have an immediate effect"** **Yes** Y 14 N 3
- Need a definition of immediate? "Faster than a human reaction"
- e.g. Immediate access revocation- 24 hours.
- Near term.
- What about adding: "only those that have the capability to monitor or control real time operation of the BES"
  Concerned about "monitor." State estimators replacing what you are monitoring.
- "respond" vs. control.
- Is it clear that it control?
- **Support for single reworked paragraph. Yes** Y 17 N 0
- "Dynamic response"- editorial accept. OK
- "Cause a condition" vs. "cause a reaction"? Any difference?
- "Balancing load and generation." Ok
- Controlling Frequency
- "which ensure real time"?
- Cant control without real time. Don't need the clause.
- "Controlling Voltage" editorial accept. OK
- "Managing constraints" editorial accept. OK
- "Control and operation" editorial accept. OK
- Restoration of BES- editorial accept. OK
- "Necessary" should remain.
- "Situational Awareness"
- It is partly a operations planning action?
- Contingency analysis, close to real time (not a day ahead).

- Delete “anticipate and plan”?
- If you take this out and you take out RTOs.
- Solve by eliminating “~~and anticipate effects of planned and unplanned changes to conditions.”~~?
- Take “current” out of it? Immediately affects situational awareness?
- Only reason to use this clause is to scope this down. Addressing concerns that “this applies to everything.”
- “Assess the condition of the Bes necessary for real time operation.”
- Control and operation and situational awareness.
- Difference between monitoring and assessing.
- control and operations- pure SKADA status of components. Situational awareness.
- Assess the current and anticipated operating state (or condition) of the BES?
- Is there different information used to assess the current vs. evaluate what the future?
- It can be data not from a real time environment.
- Day ahead studies, state estimation. Don’t want to get to other studies being done.
- “near term”? data collecting is real time.
- Current, expected and anticipated
- **Situational awareness: activities actions and conditions to asset the current expected and anticipated state of the BES.** ***As revised*** Y N 15 0
- Inter Entity Coordination and Communication
- Active coordination. Communication is the action.
- Coordination of real time operation.
- Add, **“real time coordination”** Yes. All agree.
- Tie to attachment 2? General comment.

Attachment 2

- (“As determined by….”) Maureen Long/NERC suggested a determination.
- “Responsible entities”= functional model entities. We are using this. She has injected this back in. e.g. 1.1 generation operator doesn’t have a role in this.
- “Operations planning”- SDT decided to take out yesterday.
- 1.1- Generation facilities- (as determined by the Generation owner or the generation operator”. Might be at times the generation operator
- This parentheses might be not needed.
- Doesn’t clearly identify shared facility. “if using a shared BES cyber system”
- If he has all BES cyber systems.
- Non-shared system will not be connected with each other.
- “Shared or connected Cyber systems”
- That would be everything in the system.
- “Each BES cyber system that either singly or in combination. **Yes** Y N 13 0
- May not be as clear.

- Remove the rest of sentence (" ~~or more in Texas and Quebec interconnections~~")
- BES cyber system affecting a plant bigger than 2000 MW- everything in it is high impact.
- Each BES cyber system?
- "would" this is a conditional word. That ~~would~~ immediately affects
- That has the capability to immediately? "Has the potential to"? "Can have an immediate effect" (from yester day)
- **Each BES Cyber system that can have an immediate effect on real time operations"**
  All agree.

- This came from a NERC document. Disturbance report Categorization criteria. Done in 2009.
- ERCOT has higher contingency reserve- less than ½ of reserve. Lose 2 units bigger than 1000 MW.
- Engineering analysis language was in December 09 posting.
- Arguing the 1000 MW number
- Any way to ask Planning Committee regarding this issue.
- SM: "good enough to post" to get industry comments back. Leave something in. If you assume 2000 is appropriate for east- % of size of interconnection.
- Impact of loss of MW is the focus.
- **Remove the rest of sentence ~~("or more in Texas and Quebec interconnections")~~**

Y	N
8	8

- **Remove?**

Y	N
13	3

- **Strike 1.1 and look at 1.3 and go with contingency reserve. Defer, for now. Get feedback from the planning committee.**
- **All OK**
- We need a criteria. This is key. Used the disturbance report as basis. What our basis for this concept in 1.1?
- Few generators with 2000 MW – few are high impact.
- E.g. 3 or more transmission lines
- Move to medium vs. dropping?
- Support this. Contingency reserve. We've discussed before. Agreed to leave them in.

1.2
Sub-team ok with NERC edits/additions. SDT ok.

> Facilities, singularly or in combination (if using a shared BES Cyber System), with aggregate higher of the most current and prior to the most current rated net Reactive Power capability of 1,000 MVAR or more in Eastern and Western Interconnections and 500 MVAR or more in Texas and Quebec Interconnections. (As determined by the Generator Owner or Generation Operator, Transmission Owner or Transmission Operator)

1.3 Contingency

- This is an annual reassessment issue
- List of issues for 002-
- Including operator. Why not "as determined by the asset owner." Not clear here.
- Refers to owner of BES cyber system. Put clause- after real power capability?
- Referencing Mod 24 and 26 testing and verification standards. The concern with linking together is possible double jeopardy. Justification in mod standards for doing both. Operator doing verification and Owner doing the setting.
- This may be an across the board issue.

Generation Facilities, singularly or in combination, (if using a shared BES Cyber System), whose aggregate rated net Real Power capability, as defined in 1.1 above, exceeds the largest value, for the 12 months preceding the categorization, of the Contingency Reserve or total of reserve sharing obligations for the Reserve Sharing Group. (As determined by the Generator Owner or Generation Operator)

1.4

- John Lim questioned if the proposed edit is correct.
- "designate" "as designated by". Balancing authority not always the one making the reliability decision.
- Could be a number of entities.
- Unless this is universal, should be these be in at all.
- Propose striking parenthetical.
- Balancing authority- ERCOT e.g. balancing authority. But there are several entities in other places.
- "all reliability coordinators" ?
- "planning coordinator."?
- Who has a generation facility. They know what contracts/terms for their facility. Shouldn't be who is determining. Person with the asset knows.
- Some may be good or not. Possibly delete all.
- You can't have reliability without a review contract. Compliance auditors know if they have in terms of contracts
- Strike throughout attachment.
- Transmission facilities are named. Scoping built in with those words vs. entity type.
- **Strike all parenthetical**.

Y	N
14	0

- 2.7 "or that remotely control a BES asset with a Medium rating"
- 2.5 "including FACTS devises? All high impact or insert language there. (including flexible .)

C. CIP 002 SDT Discussion of Open Issues and Follow Up

- Dave Taylor's VSLs comment (15% high number? Came out of guideline for VSLs.
- Purpose reference to 003-009 will be adjusted after security controls
- Sub-team will go through the measures to ensure they are consistent with the requirements as revised.
- 1.1 and 1.6 in Attachment I.
- "Immediate"
- Annual or periodic
- 1.5. 2.4 Medium- 3 transmission lines right criteria? Where is the right number and what is the basis for that?
- 1.7 transmission facilities. FACTs devices added. Flexible AC Transmission Systems.
- Include "protection system " associated with transmission facilities? In IROLs? What is the reason it is included?
- Added to criteria for threshold for transmission-
- Looking now for consistency.
- In medium added a clause regarding protection systems 300 KV.
- Protection systems added to l.7 (including their associated Protection Systems) Sub-team will resolve how to reference this.
- Control center definition resolved? Yes.
- Is there a cyber component of systems that are not special systems? Yes.
- Retirement of term cyber asset? SDT will need to decide whether to retire.

D. Final CIP 002 (010) discussion

On Friday, John Lim reviewed CIP 002 Sub-team's redline version to address some of the issues raised earlier in the meeting and presented revisions on CIP 002, which were documented in the latest version of CIP 002.

Definition of BES Cyber System + definition of "immediate".
Rather than another definition, the Sub-team proposed to focus on the BES Cyber System definition and added "within 15 minutes" within the BES Cyber System. If the effect on reliability is within 15 minutes then the item is a BES Cyber System. This gives a finite time.
SDT Comments

- Does this include protective relays? Yes.

High impact rating
SDT Comments

- Is this – reserve sharing usually goes up – is it intent to move more in or more out?
- Parenthetical – I understand it but not sure anyone outside this team will understand it
- Meant to qualify or explain as a shared BES cyber system

- This doesn't make the "shared" clear – may need an explanatory box as opposed to a parenthetical
- Delete front end of the parenthetical
- Meant to clarify what it is meant by combined operation
- Using singular or in combination
- Team will work on exact language – concern noted

Transmission facilities

- This language helps but still concerned about parallel lines
- Changed to 4 to address terminal stations
- The parallel lines are a concern in our area
- Not sure we can address in the standard itself
- Other changes are on the medium impact – will need to address some of the comments and changes in the high impact discussion
- 1.14 - Consider moving transmission operator functions to the front of the statement for clarity – agreed
-
- Jackie Collett's email offers a rephrased version of earlier discussion
- May need to take out the first "or" from restatement
- Too long a sentence and confusing, so she tried to break it into two sentences and add punctuation to help clarify.
- Programmable electronic device – don't you want to say processor somewhere? No, working on programmable devices
- Worried about phrasing – if send info to cell phone does that phone become a BES asset – do we need the phrase "on data display"? It is the use of the data displayed that is the problem, not the display of the data.
- Semantics that may cause more problem to correct – need to give it more thought to see if can address without creating more problems
- Shouldn't we pull in language from Attachment #1 to establish what the BES system is?
- Cannot refer to an outside document within a requirement.
- Trying to write the scope into the requirement? Careful, need to keep it general
- May be getting too specific to say data used by an identified operator.
- Would removing "data" address the question? No we are also protecting the data
- What are we adding with the additional statement about BES condition or disturbance? Pull out of here and put into
  Attachment #1 – we are trying to say the function in two different ways and it is confusing.
- But, again we cannot refer to a separate document.
- Shouldn't try to put any of the functions in – gets too messy.
- "relied on to make real time operations decisions"
- Propose taking suggestions to the subgroup for refinement.

- Consider two short definitions – one for BES cyber system and another for cyber system
- Rest of 002 Sub-team will review on Wednesday.
- In definition of situational awareness – when is the anticipated state? What period of time? See qualifier at the top of the page

III. CIP-003-009 REQUIREMENTS (CIP 011)

The SDT first reviewed the Security Governance draft approach and the progress made for each to the Sub-Teams since Phoenix. The Sub-Teams then met on Wednesday to continue drafting work and presented the draft document on Wednesday and Thursday.

A. Security Governance Sub-Team report

- Jon Stanford presented document noting his sub-team had received statements from only two sub-teams- looked to other sub-teams to get their requirements.
- What is the mechanism to get into 003.
- R1: 3 sub bullets. Scope of applicability to organizational and third party personnel
- Security roles and responsibilities
- Identification of a single senior management official with overall responsibility for leading and managing implementation of requirements within these standards.
  - Provision for emergency situations? Address in recovery and response? Policy objectives
  - Annual review and approval of cyber security policy assigned pursuant to R2. Not in agreement.
- Manager responsible for implementing. "review and approve" – suggesting an org structure.
- Separation of duties issue.
- Delete 1.5 out.
- Clause " with authority" is not in current draft.
- 1.3 "with overall authority and responsibility."
- Topical areas removed. Not addressed in policy document? Requirements by topics- replacement for part of your security document.
- From 2 on- cover policy statements by topics. You to have a plan here, topic sections will describe what's in the plan. Took topics out- carry over from Federal thinking. They will be requirement statements.
- 1.3 annual review? IN the base statement in R.1. Require the REs to annually review.
- FERC wants the same person to know about.
- 1.3 overall authority and responsibility.
- Consistency. In CIP 002- eliminated annual review. Initial and upon changes vs.
- Annual review in policy statements and cover it globally.
- Program review if global

- JS: some requirements for annual review of a plan.
- SM: Double jeopardy- how write language of policy in 3 vs. procedures and plans in other standards. Don't link too tightly together.
- Annual review- different from CIP 002 annual review issue. What would be the triggering event? At policy level. Annual review catches what has happened in year.
- Feds- bi-annual review of high level policy document. At least every 2 years.
- Annual review is practiced in the industry. Good to put in as a requirement. Don't need to say who does. Senior manager should approve?
- Tie to responsible entity
- Some have single policy, some have more than one policy. Separate policy for NERC CIP.
- Presupposes they approve.
- Interpretation questions. Single senior manager. Per responsible entity. A company could have different officials. Each functional model entity.
- Double jeopardy issue we can't solve
- By functional model- have many registered entity. Let the organization decide. Can be the same or different.
- CIP Cyber security policy focus here. Consistent with version 3. Not broader security policy.
- Senior manger was to insure accountability. $1 million a day. Why special requirement. FERC directive.

R2

- 4 sub numbers.
- Shall develop a system security plan for each BES Cyber System that: 4 bullets.
- What is the need for this? Comes from a federal space. We may not want a system security plan? (describes operating environment for what you are protecting)
- List of BES cyber system out of 002. Where is the best place to document. Some requirements provide for plans.
- All documentation required. If it is spread around, then take this out.
- Security plan not only in federal model. Becoming a standard way to define system security.
- Maybe as guidance- accumulate documentation and place where makes sense.
- Make auditing easier if they have 1 place to go to for each system. Easier to see how came about. If you provide this.
- Notice requirement for a document for each BES cyber system regardless of level. As written for each and every one. Auditor needs only finds a missing document to be in violation.
- Isn't a new challenge for large multi-nationals. "Real time" operations in CIP 002- number of different REs involved. Compartmentalization. Entergy- single VP- fossil nuclear, distribution, etc. fiduciary presidents of 5 operating companies in 4 states. If divide up may not have security.
- Program plan- describes things you have to address. IN areas such as access control systems
- If came back to command and control fabric- systems that do that. Organization "shall". Have a program plan for how to attack each of the technical area.

- Security plan for each BES cyber system.
- CIP 006 physical security plan that needs to get added.
- Keep this a much higher level.
- Why look at BES system first and then at BES cyber system.
- This could create nightmare scenario.
- Security plan that addresses the following for h/m/l. Not at each cyber system level.
- Too onerous. Have security requirements for low impact systems. Security plan doesn't add much to what you are already doing. Have to document environment to demonstrate compliance. Think of
- For high impact assets need this level of documentation because of their important. Specific plan. At low level, generic plan how we address these as a whole. Not as onerous.
- Program plan approach?
- Other requirements may lend themselves to this.
- Coalesce all the plan requirements into a program plan by topic. High assets- security plan requirements.
- Program plan a good one.
- Incidence response and restoration plan. Just mentioned. Cover exclusion for emergencies.
- Details of what is in the plans in others requirements.
- "The security for each BES cyber system will be addressed in a security plan.
- Responsible entities came from markets. Shakes down to 3 organizations. Operating unit.
- Model for policy statements- in R3.
- Each responsible entity shall:…..
- Program plan-- take each of the topical areas "BES cyber system connections" DHS Control system connections.
- Authorize and document external connections. Only those authorized are in place.
- Revise R2 to include topics.
- R4 down- talks about plans- info protection plans.
- Codify details of procedures.
- Rework R2 and put a program plan approach.

R3

- How is R3 a policy? Embedded in controls document. Pull out of here?
- Won't need this if we take program plan approach.
- **R3 is redundant**. All Agree. JS will remove.
- 3 Rs.- in 003 (manager, program plan)
- E.g. configuration management plan- vulnerability assessment etc. Will these be set out as topics?
- Keep simple, not require multiple plans, but set out the topical areas.
- Probably won't need topical areas going forward.
- Program plan approach simplifies. Collapse these down.
- "Policy"- what do we mean?

- "shall language"- requirements framework- everything is a shall. If you are getting into procedures, attributes. If you are talking about topics.
- E.g. Personnel screening process. Shall have this. Procedure on how implement.
- Have to be careful- shall includes- have to have a policy. These are the areas you have to address in the policy statement about the CIP standards.
- Recovery plans and incidence response plans- not policy? Require you have one and have to do it. Develop and implement the plan.
- The plan must contain the following- e.g. recovery plans must contain….
- E.g. CIP 008 and CIP 003 statement- possible double jeopardy?
- How to deal with CIP 003, if you don't have that requirement as a low? Low impacts that don't require a response plan.
- 1 approach – policy statements you will do access control, you will.
- 2nd approach- you have to have a plan for all these things.
- Current CIP require plans where you may not need plans. Create compliance activities that have been necessary for enhancing security.
- All in a single table- do everything in a table. Policy should address. E.g. 4.3 include applicable controls specific in Table 1 Information Protection Controls.
- CIP standards are topically light and DHS are topically heavy.
- Agreed on program plan approach. Don't know where policy will go. Then come back with a proposal.
- Easy to write a double jeopardy requirement. Just to create policy statements. Policy statement you have to have recovery plan. CIP 008 and 009- plan contents. Measure for the policy- policy statement. If measure in CIP 003- you have plans to support the policy. Draw a line between requirements for policies and writing plans.
- Sending over the plan? Annual review and updates in CIP 003. CIP 006 here is what plan contain.
- This is a global question. Handle annual review in 003 or in the subsections?
- Requirement- policy statement that addresses recovery plans. Go to CIP 8 & 9 about content of plans.
- In requirement- state what the policy must address. Guidance document to be developed what the thought was behind the requirement.

R4

- R4 a problem? Looks ok.
- R4- e.g. where you are putting in requirements for the contents of plan. Here just say you have to have a plan.
- If this creates a double jeopardy problem would have to roll up into R1.
- Address the topic of information protection.
- Read it as a family of one. Why not make it one.
- Tie up topical areas in R1. Policy statement to be made in topical areas will be made in the sections.
- Does this raise double jeopardy issues?

- Puts all high level requirements in one place- shows accountability.
- Asking whether we need policy statements in CIP? Every requirement in standards is a policy?
- In practice, that is how they are written today. Current 003- policies should address all requirements.
- Doing it by topic. Not as granular as current 003.
- Placed some of these info mgt requirements here in the last week- they tie the policies to the program elements. Put things together that belong together.
- Why not put under a single standard?
- Put all tables in a single standards
- Take outliers and make them standards themselves.
- Existing format- CIP 003 policy for this, implemented in CIP 005 .
- If we change into one standard, we will hurt ourselves with the outside world.
- Move to their own standard. CIP 007 single requirement about access control.
- Standard- talks about access control (physical or otherwise)
- Does NERC have a definition. CIP 006 physical security plan. CIP 004 cyber security control training program. Do we need to get one?
- Use the same word across all standards.
- What do want to call this? "Program" is what you are doing.
- Collect all the topics together. Figure out how to put together as a team. Plans, Programs,
- 002 about scope. 2nd is about governance- management requirements. Got to have a policy and a program to address different subject areas. Outliers- are common to others, e.g. access controls. Policy can be simple what is important are the plans, woven together under management oversight.
- 003 umbrella standard- 4-9 addressing in more detail. Jumping off point for more detailed to follow.
- This standard is skeletal- areas management.
- Compartmentalized- to some degree will be necessary.
- Plans and programs- different disciplines use the same words- physical guys call things plan. What we mean is program and not a plan.
- If it doesn't lend itself to a plan.

B. Quick Update on Sub-Team Progress since Phoenix Meeting

The CIP 003-009 Sub-teams provided progress reports on work since the Phoenix meeting and then met in small groups until mid afternoon to draft or refine their requirements.

1. Change management.

- Areas- CIP 003 didn't fit into oox standard.

- Coordination- low/medium/high impact and connectivity- environmental differences? Didn't have many.

2. Access control and Auditing

- Sharon Edwards noted the excellent contributions of Jeff Hoffman and Frank Kim
- Got input from NERC
- Open issues- password measurements.
- Review what NERC offered.

3. Recovery and response.

- Scott noted good progress made and acknowledged Tom Stevenson's help and has reviewed Maureen's suggestions.

4. Operations

- Jay Cribb report that the Requirements are in good shape.
- Work needed on objectives and measures
- Coordination- ESP access points. Electronic Access Points- defined term – happy with

5. Personnel and Physical Security

- Doug Johnson reported that they have reviewed Maureen and/Dave's comments
- CIP 004. Get some policy statements over to Jon Stanford- addressing physical security and training and physical risk
- Do we still have an electronic security perimeter?
- What we have been doing- we have a word doc with a list of requirements. Get that into a real document.

C. CIP 003-009 Sub-Team Requirement Review

1. Governance

Jon Stanford presented the changes made to CIP 003 offering the following points:

- 003 can become 010
- Edited R1- adding the 9 subject areas (1.4- 1.12)
- R2- Each responsible entity shall implement the requirements specified in Table 1 (Subject Area XXX here)
- R3: Each responsible entity will implement the requirements specified in Table 2 (subject area xxx) in order to (benefit to the BES here)
- Can link VSLs to requirements

SDT Discussion

- NERC staff recommended retiring existing CIP standards and start afresh with CIP 10. Some cross e.g. vulnerability assessment is in 3 areas currently.

- Allows to quickly look through and make sure not requiring same thing in 4 requirements.
- We would need to explain- here's the map from the old and the new ones.
- Another benefit- requirement language will be simplified. As standards evolve- you'll modify the table not the policy making it more adaptable for future.
- Don't have to have a requirement that says "develop a plan"- avoiding circular logic.
- There is 1 requirement for each subject area? Will have own VRF? Everything in that Table will have the same VRF. Table will in essence- be the sub requirements.
- If we want to differentiate VRFs, we can develop multiple requirements.
- Implementation plan that will need to go along with this. If 1 standard. New implementation for a full standard.
- This will help out with the implementation plan.
- Version 4 and dates
- CIP 8 and 9. How would that be handled?
- CIP 8 with 4 Requirements and 4 tables would become 1 requirement and 1 table. Or use a group heading..
- We will need a new number strategy for interpretations.
- Need the SDT to determine what are the topics. Starting with 9 proposed by the Governance sub-team.
- Rolling each into a requirement. Reporting potential violation. Physical security violations (minor and major). Not sure this is the right way to go.
- There is precedent for lots of standards.
- Helps with granularity. We need to think about all implications.
- List of stuff that needs to be done will be the same. The granularity of the standards will be different.
- Need different frames of references- think about this overnight.
- Its important that the SDT makes sure we have the buckets right. Make sure they are chunked the right way. How it is organized will make a lot of differences.
- SDT should flesh out proposal among the Team. We need to agree on chunking. Get together and decide uniformly and collectively.
- This is a hard subject to get one's head around. Anything changes in format will be initially received as not necessarily simpler. Awareness and staff capacity is an issue in the industry. Practically consider starting what we have.
- Should there be a motion to stay with current CIP framework?
- WECC auditors have indicated that this would be easier with one caveat that tables would need to be numbered. Need a way to track that to the table.
- This does not represent a radical change. In fact, the H/M/L categorization is the radical change. Tables right now don't work. Need to find a way to present appropriately. This is about presentation of requirements.
- About 140 requirements in a single standard. Will violations of any requirement be a violation of standard? This raises repeat violations. Measures more complex and VSLs VRFs.

- Do we have the time to do it? Most of the other teams have requirements written. Significant re-writing will need to be done. Content of both the tables and requirements.
- This will be seen as a radical change in the industry.
- Could improve reporting. Violation of categories. Better reporting overall. E.g. personnel risk assessment. Create a better taxonomy.
- This is the appropriate time to propose the change and get it in front of the industry.
- Changes to software. It will get updated.
- Not lots of additional work. You take requirements. Put together in 1 document. Not a step back in reworking a lot of things. Most requirements are already in a table format.
- This could go faster for us and present a better governance model. Not making changes for no reason.
- What is there to debate if we stick with the current?
- This model is a vast improvement to what we have now. Might be well received by the industry. This team shouldn't concern itself about the vendors. Rather debate the merits of the ideas.
- This approach could help us in terms of consistency checking. Consistency is important. Advantages. Lots of organizational and process changes in the industry. Vendor software is the least of it. If not restating things in multiple places.
- Initially I like it. We have forever been defending one family of standards and we have viewed as 1 standard. We keep as one standard anyway.
- Messy now. Access control and monitoring asset. 5 line requirement. Makes a mess today to figure out what kind of asset is that.
- Many trade organizations are together. NERC CIP, Smart Grid standards coming out. Tracking on 800-53 model. Several doing efforts internally to map all requirements to such a model.
- Granularity for compliance- removing.
- Explained the proposed formats.- 9 topical areas. Policy
- One of the issues- compliance implications of doing that. Now between 8 and 150 requirements. Fewer # and granularity. Single VRF factor. Single V Severity levels . What would they do in terms of an investigation. How report to regions. Penalty calculation.
- Now with 41 requirements moving down to smaller number or having 150 requirements in single standard.
- Putting all standards into 1 document and consist of requirements and table.
- Consider all existing standards 3 -9 into one standard. Requirements have table associated with it.
- As auditors- take requirements and put into table format. Still looking at R and compliance with R. Having worked with military docs. Once you have anything that large and point back in terms of compliance. First time you updated. Move anything else up. From version to version.
- Keeping up to date or compliance tool- hassle in terms of bookkeeping and paperwork accurate.

- R language would be fairly vanilla- table could change. Have policy and procedures with the details.
- 2 action items. Categories need to be finalized and agreed to. Coalesce to action quicker.
- Tom Hoffsetter offered comments

Wednesday evening the Chair asked Howard Gugel to prepare a sample "proof of concept" for the access control requirements to inform a decision regarding format.

D. Review of the Sub-Team Products

Thursday afternoon the SDT reviewed each of the sub-team's draft requirements as revised and refined in the sub-team meetings on Wednesday, offering guidance on various issues raised by the draft requirements.

III. CIP FORMAT REVIEW

A. Tables in the Standard(s)

Howard Gugel, NERC, reviewed the changes regarding format, tables- (R3 referring to table 1). Editing tables. Propose for title to Table R __ helping to tie back.

SDT Comments

- Multiple Rs referring to the same table?
- Keep each table specific with each requirement.
- Bring back question of multiple references to the same table.
- CIP 6- one table and the column as the Rs. Different from the others.
- Need to be consistent for the format for all requirements. Use same format for other tables.
- Consider the guidance documents.
- Rows in table play role of bullet items under each requirement. Separate table links back to each requirement. Resolves issue of multiple rows references back to multiple requirements.
- Grouping the Tables at the end of the standard. Disjointed in a standard. Lot more readable and manageable. Sub requirements, as table entries.
- Similar to attachments in CIP 002. Idea of tables at end, keep requirements concise. Will pose to Maureen to get her opinion. Consistency better at the end.
- Look at Rs and make sure wording is consistent with other requirements.
- Looking at each R how you would measure it. Proof of that- light on this.
- Look at objective statements- read and make sense it is the purpose of the standards.

B. Objective Statements

SDT Comments

- Putting the objective within the requirement? Fraught with danger down the road.
- Enhancing reliability purpose clear.
- Reason it is there, who it applies to why needs to be done.
- Putting in requirement language- gets in the way. Defer that language until requirement language drafted.
- Get requirements first then measures.
- Defer the objectives as part of the requirement. Corollary document.
- If doesn't have a basis in reliability, shouldn't be a requirement.
- Format- R words. Designate.
- The objectives makes it harder to read.
- However it is important to have objective in there.
- Need to be specific about the benefits.
- For now, just bracket the objective.
- Part of the deliverable- measures, VSLs and requirements formats at the end of the session.
- Benefits for reliability? NERC could throw their proposal on each of them.
- Important to deal with measures- know when the requirement been met with. Tangible proof of requirement.

C. CIP Proof of Concept for Format- Access Control

1. Access Control and Auditing- Review for Format

Sharon Edwards presented the work to date on access control including 004 R4, 005 R2, 008 R5 and dispersed throughout the standard.

R1. Account Specifications (007 R 5) **Table**

- Beginning of table- policy should include the following: 20 points. Technical high level controls- H. M. at low- need to understand what they have. #15 "immediate revocation" of access. FERC expectations and SDT's belief of a reasonable starting point. The Sub-team had hard time with this.

Electronic Access Controls

- Sharon noted that this may be redundant.
- Box- "remote access"- Could develop a definition to the standard at hand.

Table R2- Electronic Access Controls

SDT Comments

- Need to decide which formatting for H/M/L.
- Outlier- information protection- document management.
- Measures as previously written- "make available documentation….."
- Haven't tackled VSLs and clean up work. Need sub-team time today.

- Split tables up into more tables? Is violation of one piece, violation of the whole requirement?
- Chunked up more? Good question for further discussion of the sub-team
- Tables provide an improvement and clarity- Keep concept of table. Share concern about multiple violation. Groupings of similar rows and make a separate requirement.
- E.g. Password- under own requirement. Reduces impact re multiple violations.
- Lot of value of tables but reduce the impact in terms of compliance.
- Break into more logical groups and individual requirements.
- Table not to consolidate all requirements. Table facilitates the breakdown of requirement points.
- Table looks good. Clarification. Separate document for audit and monitoring?
- Looked and most of audits related to things NERC would be doing. Didn't develop another table for auditing requirements.
- Row 13- Ports and Services- overlap with Change Management and Operations Security? Probably needs coordination.
- Doesn't specify the content of use restrictions? Is this an issue.
- Wireless approach- didn't want a comprehensive set of wireless standards. Other standards already done a good job. Trying to be less proscriptive. Down the road with encryption. We are not resourced to do.
- What does a blank in the table mean? Clarify if not required or something else.
- Communications aspect of this? Things that are not connected vs. routably connected. Did you intend to stay away from this?
- We did talk about this in the Sub-Team. Spent a lot of time discussing FERC directive to remove access. FERC didn't suggest anything to treat differently. Didn't go down road- may be others. Made decision.
- If talking about remote access, not remote access for user sessions outside of the USPN.
- Format: Required vs. analogue values in the rows. Larger number of individual similar requirements as long as each is a discreet, well worded.
- Breaking out. Barrier. Not having VSL correlated with requirements. Break up or chunk the topic areas – access control.
- When doing measures, have a table form? Matching those in requirement?
- Sub-Team used the generic measures.
- Let's make sure that the SDT knows the topics. E.g. "Security management controls"?
- Repeated wording. E.g. 11 "is required"
- We need a section where you address FERC directives. They had one directive (immediate) Make sure that we cover that for each of the sub-team. We don't need this posting.
- Authentication of un-manned devices. We will see more and more. Will this be covered someplace else? Should this be "human" access control. Do we need to say that?

D. CIP Format Review

1. Overview of Format Questions

On Thursday morning, Howard Gugel presented to the SDT a proof of concept for the access control requirements. He asked the SDT to look at format not merits of requirements in order to get a picture of how the requirements would be presented. He noted the table would be embedded in text and at the end of each requirement. NERC standards review staff agreed with this format approach. This would be the same regardless of which approach is chosen.

- **Option 1.** Keep 003-009 and work from there.
- **Option 2**: retire existing CIP standards and organized by the topics in sequence from 010 on. Access Control e.g. CIP 017.
- **Option 3:** One standards document with 2 sections 010 (002) and 011 (003-009). All controls together. R1 security policies addressing all topics
  - R2 implement per table
  - R3- table for access control
  - R4 implement 2nd table (account specifications).

Initial SDT Member Comments on Format

- Will 002 be on its own? Yes speaking of 003-009 together.
- Where are we capturing connectivity? 005.
- Connectivity is more important than big iron.
- 1st 5 LMH.
- Left column- allows item tracking
- Title Access Controls.
- It will not hard to make change if industry doesn't like this format,
- Language of the table can address connectivity.
- Industry confusion currently in terms of audits at the requirement level. Radical format change may not be well advised.
- Missing opportunity- keep simpler to scope out key things, like was discussed in Austin.
- Tables concept came out of the Phoenix meeting.
- Will FERC have a problem with the tables? There may be no process for reporting on that currently. Process will need to be addressed in this document.
- Common PCI and HIPPA common auditing format for standards.
- Read tables- allows flexibility of the columns. Reporting issue not an issue. Row number tracking will help.
- Table structure agreed to a couple meetings back. We are using them. Whether we keep groupings separate or have a single standard for this is the question. Culture of compliance- repeated violation of standards might be held against the industry with the single format.
- Will it be possible to write a VSL for this table format?

- Separate tables for requirements? E.g. account info and another with remote access issue. Past VSL at requirement level and where with sub requirements. This could end up with a lot of "ors"
- Break out the VSLs with the sub requirements in the table?
- Everything happens at the requirements.
- "Foolish consistency is the hobgoblin of small minds."
- When file with FERC it becomes law.
- Same issue with the VSLs- regardless of options.
- Can split the tables into more areas- can get as granular as the SDT wants.
- Put Rs on left column. Lose the R4 and number Rs. Use if /then construction.
- Now would be the time to propose this. Timing for this.
- Clarification on status quo. Decide on the buckets? We don't do buckets. Stay with 003-009.
- Do some reorganization what is in each standard and possible move- but keep in. Fix for Order 706.
- 003-009 numbering. Moving some Rs around. Tweaking re 706.
- The Team needs to make sure this works. Sees value in topical groupings but has concern with industry confusion. When CIP version 2 was put out the numbering changed and industry members asked why.
- Have a comment form question to get feedback. Makes sense from various standpoints. Ask how much confusion this cause confusion. In the comment form.
- Is there precedent in other reliability standards- if you are generator operator, if you have X, then.
- Limited. Lots based on functional model. Rs directed to different functional entities.
- What ever we do there are going to be changes in the industry. Better we do on our guidance, the better the industry will know what's going on. Need a strong foot forward on guidance.
- Option one- access control. Are they outliers. Easy to place those in a standard.
- Public Comment: Owner operator. Option 3 will be confusing. Is it the whole standard you must follow? CIP have 3-9. Too many changes together for industry to handle. Do option 1.
- Not proposing 4 options. Need to understand difference between 1 and 2 & 3. 2 and 3 carry new organizations. Current standards are supposed to be considered together. They are 1 standard. Change 1 must change all. They are buried and possibly scattered around in the current. New organization with different topical naming.
- Lot of thinking into organization of current standards. Big change is a new organization scheme
- Use tables with all of these options.
- Version 1, 2, 3 confusion- application. Version 4. Renumber standards. Option 2 less confusing.
- Radical change in the standard is required. Some equivalency 3-9 but the approach we are taking and the different formats. Would cause more confusion to use the same numbers. Start for new set 10- onward. Not to be confused with 3-9. Option 2 doesn't follow. It is a

different set of controls organized differently. Likes smaller groupings regarding compliance.

- Tom Hoffstetter noted that he doesn't speak for NERC but that organization in tables is good and he likes the break-out in terms of topics. Required columns will make it a lot clearer for both entity and auditor.
- If we go to option 3- collapse into 1 standards. 140 controls in one standard. Violation more than1 get a penalty.
- Whole different paradigm require a new approach as to how penalties assess. Approach different in many ways. Wouldn't try to make current structure fit. Have to depart from traditional approach to penalties. Have to describe them differently and assess in a different format. Across the board.
- Nothing to argue with what TH said. These standards will be balloted and posted and implemented under the current process.
- Option 3 recognizes how tightly knit these are together.
- This may not matter in the end. Push in his company.
- Can NERC help with this issue that RK brought up? What is the audit standpoint. Can they do this. Might help to present options 2 and 3 at the Technical Workshop. Show how NERC and auditors of regional areas would handle. How models would be handled in audit and penalties.
- Option 3- organization within? Still the same? Structured as per 1 or 2?
- Constrained by current compliance structure. Could we propose a new approach? Put out standards with a proposed structure?
- Confined now to VSR VSL structure.

2. Initial Preference Ranking of Options and Voting for the Preferred Format Option

The Team following the discussion of the pros/cons of the options, voted first on each of the three options indicating its acceptability. Following that each Team member voted to support the option they found most acceptable or preferable based on the discussion and their perspective.

Format Option 1: keep existing CIP 003 to 009 in its current form maintaining its existing logical construct (may involve minor movement of existing requirements between standards)

Yes	*No*	*Indifferent/could go either way*
8	**7**	**3**

Format Option 2: Retire 003 to 009, create new CIP 010-16 grouping according to small group assignments.

Yes	*No*	*Indifferent/could go either way*
12	**2**	**6**

Format Option 3: Collapse CIP 003-009 into a single standard that contains all requirements created/edits by small groups and grouped according to small group assignments.

Yes	*No*	*Indifferent/could go either way*
12	**7**	**2**

The team then voted for one of the two highest ranked options under consideration:

- Option 2: Retire 003 to 009, create new CIP 010-16 grouping according to small group assignments. ***Yes*=6**
- Option 3 Collapse CIP 003-009 into a single standard that contains all requirements created/edits by small groups and grouped according to small group assignments. ***Yes*=10**
- *Abstained from voting for Option #2 or #3:* 4

Comments on the Options Ranking and Next Steps for the Sub-Teams

- Need to take into account the industry's reactions.
- Don't see any real difference between option 2 and 3.
- Not a single requirement vs. standard.
- It is different in terms of what is presented. Violation of any requirements may present problems.
- This is just an organization issue.
- What are the expectations for Sub-teams in terms of drafting VSLs?
- Allowed to have content- for each row of your table a VSL statement in that format.
- Finish up writing requirements. We can pull back together into multiple standards or into one standards following a decision.
- Would be helpful to go through one of the sub-team's reports before breaking. Substance requirements, measures and VSLs.
- Missing several definitions. Should we use boxes? Indicate it is guidance. If not, it will be exported to glossary, or in requirement.
- Note if put in guidance then not part of standard. If it goes out without guidance document. Comments won't be complete.
- As a reality check, take access control and go through it and reframe expectations. Going to need work after going out for informal comment. Interim work product posting. Work as hard. Focus on requirements.
- Some sub-teams are using different definitions for external connectivity. Factor into what is put in the rows on table. Each needs to do the walk through.
- Five remaining areas that need SDT guidance for sub-teams.
  - Square box definitions- specific to standards (vegetation management standard precedent
  - Control centers definition
  - Different types of communications
  - How should the sub-team address drafting measures or consider putting out document for industry review without measures

  - Address VSLs or consider putting out document for industry review without measures
- SDT should clarify outliers- definitions. Whose will be used? When will see all the definitions in the various document?
- Governance section, based on SDT input pulling policy statements up.
- Suggest that a SAR for a drafting team be considered. Address FERC 706 items that may be outside the scope of drafting team, e.g. NIST risk management framework.
- 9 Categories of proposals to organize. Put the level of controls in right hand columns or separate rows.
- Option 1. Allows different time frames. Separate line items for medium. Time frames in columns. Bulleted lists time frames.

3. Reviewing and Ranking Option 2 (2nd Round)

At the end of the day the Team took up the format issue again. The Vice Chair made a proposal that the Team use Option 2 (which would renumber the requirements using the topics to organize them. The Team discussed this option:

- Consider renumbering 002 as 010 – confusing to have 002 then renumber at 010
- Posted previously as 002, proposed keeping then renumbering new.
- Yes, different titles for the same thing that exist with a few split out.
- Some match what we have now, some are new – where we can group into the existing CIP we could do so and renumber only the new ones.
- Is media protection now media disposal? Where would you move information protection?
- How many teams work on multiple standards at the same time? Yes, others teams do address more than one but not ten of them
- The titles may seem the same but many of the sub-parts have been moved around except for 002 which is still focused on the same topic area – we would need to educate the industry on what is in each standard.
- Rename the last item 021 as Boundary protection rather than data communications?
- Will we map old standards into the new ones? If so, why not retain some of the old numbers
- Did not gain consensus on this earlier – this seems ad hoc.
- We probably need to agree on something today in order to to put this into a format.
- Propose altering proposal to start with 010 for old 002 – new numbers for all of them – less confusing
- Access control needs to be separated into physical and electronic.
- Under personnel and training – would that include training for all the other standards?
- Idea is to combine training and awareness and risk assessment.
- Change name of the last one and make electronic access protection or role into new 013 under system security?
- Heartache at pulling physical access control out as separate item.
- May still need further renaming or organization as we move forward.

- We have to write the standards so we are not assuming IT security and physical security will be handled by the same people
- Physical security and access control – IT controls access to server but not the badging for physical security –
- Need to go with this not as a concept but as framework – it is a format

The facilitators polled the team on their support for the option #2 (multiple standards) and 7 of 16 members were in support of utilizing this as the format.

An additional member joined and the Team then tested support for Option 3 (putting all into single standard) and 9 of 17 supported using this format. Neither format approach received sufficient support to make an SDT decision.

4. Numbering the Requirements

The Team them reviewed and tested support for each of the following propositions:

- **Change from existing CIP numbering system?** Yes- 13 favor changing (of 17 = 76%)

SDT Comments

- Adopting the headings would be the same under multiple numbers or as one
- If we keep CIP 002 as 002 for continuity then the rest are renumbered or just one,
- would be more confusing
- change to Option 2 if we revote but concerned this is under duress
- Think we need just one standard

5. Adopting Category Headings for Requirements

- **Adopt the proposed headings for the requirements as the categories whether as one or multiple standards** – Yes-13 (of 17 = 76%)

After further Team discussion it was determined that there was no longer a quorum and the Chair suggested postponing further discussion until Friday morning.

6. Final Review of Format Options

On Friday morning the SDT took up the final review of format options for the informal posting document(s) in order to make a decision.

The facilitator suggested the SDT use an acceptability ranking of the two possible format options that had been discussed and debated yesterday followed by clarification of concerns to see if they could be met and a requisite number of members could agree on the format to use for the informal posting.

He reviewed the scale to be used as: 4= fine as is, 3= support but have questions, 2= need to address concerns before I can support, or 1= cannot support. The SDT then ranked each option and those providing a 2 or 1 offered what their concern was.

Option #2 – Requirements in Multiple Standards

- Use the Topical areas discussed on Thursday and utilize multiple standards (example CIP 010 -020). CIP 002 also gets re-numbered.

4-3 3=7 2-6 1-0 (Avg. 2.81)

Option #2 Concerns

- All the standards have a single purpose and are meant to be viewed as one. Should be one for clarity.
- Efficiency of one (better implementation) - Don't like fragmentation between multiple standards.
- Much cleaner to have just one standard
- Current standards say to consider as one but in fact they are not treated that way thus making compliance difficult.
- There is a greater chance for double jeopardy. Easier to manage with Option 3 in a single standard format. Fragmentation leads to fragmented implementation rather than unified management.
- We do talk about the CIP standards as one but in practice they are treated differently.
- I like the grouping or headings but multiple standards looks like we are asking them to do more - also additional documentation
- If we post additional standards, the reaction of industry will be that we are asking them to do more. Having only one standard will reduce required documentation. Eventually multiple standards would be on different version levels, thus adding to confusion.

Option #3 – Requirements all in One Standard

Use the Topical areas discussed on Thursday, but one new standard is posted containing sections for.

4=6 3=5 2=3 1=2 (Avg. 2.93)

Option #3 Concerns

- Compliance implications - violating one standard even if different requirements- significant increased risk for multiple violations of one standard.
- Need to hear technical argument to support 3
- Compliance issue- non-compliance on low items makes you vulnerable to citations for repeat finding of non-compliance
- Compliance my main concern- tie our hands about splitting later- once merged cannot deal with future revisions separately
- Just trying to format for posting

- Concerned about complexity- more than value of unified
- Voted a 1 because of the number of requirements and sub-requirements. There are about 120 major requirements plus sub requirements. The 140 plus requirements may means that any violation of any of these requirements you are in violation of one standard. Compliance reporting and compliance sanction issue on the issue of multiple violation of the standard.
- When RSAW's are prepared, the SME should only view information pertinent to his area of expertise.
- Agree with concern about repeat violations of the same standard.
- Can the compliance situation could be fixed if the structure of the way NERC viewed the standards for sanctions, etc. were changed? However, that will not change.
- Is it likely that NERC would change the way they viewed compliance to support Option 3?
- Concern with the sheer complexity of the one standard. Also see disadvantages of the lack of a unified approach, but there have also been advantages in the divide and conquer approach.

SDT Options Discussion following the Ranking

- Fragmentation of the standards will contribute to lack of a unified management and implementation.
- Sometimes the only change in a standard is the change in the standard number. This makes no sense. If you look at the categories we approved yesterday, there will be tighter integration between the CIP standards. If we have separate standards, we need to make sure each can stand alone.
- Prefers the unified standard and believes that we can help the complexity by making them one. The big concern is the regulatory impact mentioned by others.
- The Current standards do not lend themselves to good organized implementation. The new adopted topic areas are the most important thing to consider. Can both options be presented to the industry for feedback?
- The facilitator asked NERC staff is we need one or the other for the posting?
- Scott Mix noted that raw work papers will not be sufficient for the posting. Presentation in two formats will likely confuse the industry. Perhaps the posting could be presented in one format, but we explain the other format and ask the industry to comment on whether they like the change or not.
- Scott Mix showed the Team the NERC generated report does show total violations by standard.
- Howard Gugel submitted the enforcement question to Joel DeJesus at NERC concerning compliance concerns. Is there a compounding effect? A: If there are multiple impacts of multiple violations of the same standard, there may be some compounding effect. If R3, R12, and R22 were violated, they would be separate violations with no compounding effect.

- The concern is the "culture of compliance" at NERC and FERC. If the same standard is violated, it will have the consequence of doubting the culture of compliance.
- If we get one single standard that has magnitudes of violations, it will send the wrong message and numbers of violations will be noticed.
- In terms in the ability to observe, Scott Mix suggested he did not see the difference.
- All the reports to the member committees are by standard number and he believes there will be a spike if all CIP is one standard.
- Legislators are aware of the collections of standards that the industry must deal with. For example FISMA is a collection they are familiar with.
- We need a decision. We spent too much time discussing this. We have agreed on the categories. Let's get something out there. We are wasting too much time.
- We could debate this all day, but we need to move forward.
- If we step away from CIP and started talking about vegetation management, he believes breaking the standard into multiple would not make sense.
- Lawmakers and congress will understand and support that while there are multiple topics, there is still one framework for improving cyber security implementation.
- Do we need a transition before moving dramatically to either new set?
- These categories make it hard to divide responsibility.
- Think new categories provide better organization and will improve implementation.
- Can we put out both as two separate documents?
- That may be too confusing to address option with questions in comment form
- Need to be accountable.
- We need to put a question to the NERC enforcement side. Can we go with this and limit compounding violations?
- Concerned about potential impact on Congress if there is a spike in non-compliance because multiple violations of one standard.
- Congress is most concerned about fragmentation and used to looking at one standard for an industry.
- The facilitator asked if any concerns addressed that would move their vote from a 3 or 4?
- Some members expressed concerns about suspending rules- changing the game. Needs to be a yes/no choice
- Concerned adding in "either" result in super majority for both options - then what?
- Is there an alternative embedded in the decision rules for this post for informal comment? Can the SDT use a majority (50%+) for purpose of posting using single standard or multiple standards and documenting the SDT differences in comment form for either choice.

The 17 SDT members present then voted for their preference for posting for informal comment between the two options with the following result:

Option #2 (multiple standards) **Yes = 6 (35%)**

Option #3 (single standard) **Yes = 11 (65%)**

The SDT agreed that while this decision to post for informal comment has a majority support (65%) but not the super majority (75%) of the members called for in the decision rules, the Team is asking for industry comment and input on the formats through comment form before finalizing a format to present in the formal comment draft in July, 2010. The Team discussed that this approach is consistent with the spirit of the following consensus rule provision: "In instances where the Team finds that even 75% acceptance or support is not achievable, the Team's report will include documentation of any differences as well as the options that were considered for which there was greater than 50% support from the Team."

IV. NEXT STEPS AND ASSIGNMENTS

On Friday the Chair reviewed the schedule, assignments and next steps for the SDT to produce a final version for posting on May 3, 2010. Joe Bucciero will lead with assistance from Howard Gugel the drafting of comment form with information provided by each of the team leads and will also add a question from discussion of the format to document discussion

The SDT will need to begin creating an implementation plan for posting in July for formal comment with a small group of SDT members in order to provide some frame for discussion at the May meeting and to answer any questions at the May workshop in Dallas. Scott Mix will be looking for individuals to work with – this will occur after May 3.

We need something in cover letter for May 3 posting that speaks to the SDT's philosophy on implementing the plan – industry needs to understand what we are doing. Need a couple paragraphs explaining our approach or intent Jackie Collett, John Lim and Doug Johnson agreed to work with Scott Mix on developing a draft implementation plan.

The Chair reviewed the schedule from April 19, Monday to posting on May 3, Monday. It was agreed the sub-teams need to complete their drafting and get these to Howard to put into "standard" for review by NERC staff. The plan will be to assimilate the NERC comments with team leads, then late in last week of April have a ready-talk and email vote for approval to post on May 3. Have conference call on April 26 for team leads and 29th for ready-talk review with full team Each Sub-team lead will seek to get work done and to Howard Gugel by Monday morning then review with Howard and team leads on Tuesday afternoon. The following schedule was reviewed and approved by the SDT:

- 19th by 5:00 – requirements, measures, vsl's and glossary drafts to Howard
- 20th Sub-team leads with Howard at 3:00 – 6:00 EST

- 21st Howard will get team drafts to NERC staff for review
- 27th full day (10-5) meeting with NERC staff with Sub-team leads and anyone else who wants to join (NERC comments back by 26th if possible to full team – concern is legal and compliance) – updated version send out on 28th to full team for review
- 29th full team meeting (1 to 4) for review and vote to post

The Chair and Vice Chair and the SDT thanked Jay Cribb for his excellent hosting and great facilities.
The meeting adjourned at 12:00 p.m.

Appendix # 1— Meeting Agenda
Project 2008-06 Cyber Security Order 706 SDT
Draft 20th Meeting Agenda
April 13, 2010, Tuesday- 1 PM to 5:30 PM EST
April 14, 2010 Wednesday- 8 AM to 6:15 PM EST
April 15, 2010 Thursday- 8 AM to 5 PM EST
April 16, 2010 Friday- 8 AM to 12 PM EST
Georgia Power
241 Ralph McGill Blvd
Atlanta, GA 30308
NOTE:
1. Agenda Times May be Adjusted as Needed during the Meeting
2. Drafting Team Meetings May Not Have Access to Telephones and Ready Talk

Proposed Meeting Objectives/Outcomes

- Review the revised CSO 706 SDT 2010 Work plan and Schedule
- Receive updates on other related cyber security initiatives
- Receive a NERC update on implementing the CIP Communication Plan and the May 2010 Technical Workshop
- Review, refine and adopt the Draft Final CIP-002-4 for industry informal comment
- Review, refine and adopt the Sub-Team Security Control Requirements draft for industry informal comment
- Develop related CIP 002 and Security Controls Requirements Guidance Documents
- Agree on next steps and assignments

Draft Agenda

Tuesday **April 13, 2009**
1:00 p.m. Welcome and Opening Remarks- *John Lim, Chair & Phil Huff, Vice Chair*

	Roll Call; NERC Antitrust Compliance Guidelines Facilitator review and SDT acceptance of March 9-12, 2010 Phoenix SDT meeting summary
1:10	Review of Meeting Objectives, Agenda and Meeting Guidelines- *Bob Jones*
1:15	Review and Discussion of CSO 706 SDT Workplan and Schedule - March-December, 2010- *Stu Langton*
1:45	Updates on other related cyber security initiatives- *NERC Staff and SDT Members*
1:55	Update on CIP Communication Plan and May 2010 Technical Workshop - *Carl Dombek*
2:15	Overview of Single Text- CIP-002-4 & Security Controls Requirements
2:45	*Break*
3:00	Review of Revised CIP-002-4 Draft Final and SDT Industry Response Document- *CIP-002-4 Drafting Team, John Lim et al.*
3:30	Full Team Consensus Testing on Refinements of draft final CIP 002-4
5:25	Review of Proposal for Wednesday Agenda
5:30	*Recess* ▪ *Possible Security Controls Requirements Sub Team Meetings- Evening* ▪ *If needed, CIP-002 Drafting Team to meet to finalize draft and present for adoption Wednesday morning.*

Wednesday	**April 14, 2010**
8:00	Welcome and Agenda Review, Roll Call and Antitrust Guidelines- *John Lim, Phil Huff, Joe Bucierro*
8:10	Final Review of CIP-002-4 as revised
9:00	Security Governance Requirements- Overview and Consensus Testing
10:30	Break
10:45	Personnel and Physical Security Requirements and Guidance- Overview and Consensus Testing
12:15	Working Lunch
1:00	Operations Security Requirements and Guidance - Overview and Consensus Testing
2:30	Break
2:45	Recovery and Response Requirements- Overview and Consensus Testing
3:45	Access Control and Auditing- Requirements- Overview and Consensus Testing
5:00	Change Management, System Lifecycle and Information Management- Requirements- Overview and Consensus Testing
6:15	*Recess* ▪ *Possible Security Controls Requirements Sub Team Meetings- Evening*

Thursday	**April 15, 2010**
8:00	Welcome and Agenda Review, Roll Call and Antitrust Guidelines- *John Lim, Phil Huff, Joe Bucierro*
8:10	Security Controls Sub-Teams Refinement Sessions
10:00	Break
10:15	Security Controls Sub-Teams Refinement Sessions
12:00	*Working Lunch*

1:00	Full Team Review and Consensus Testing on Final Draft
3:00	Break
3:15	Full Team Consensus Testing on Refinements-*Continued*
4:15	Motion to Adopt in Concept Draft CIP 002 and Security Controls Requirements for Informal Comment Posting Review Any Drafting Assignments and Friday Agenda
5:00	*Recess* ▪ *As needed ad-hoc drafting groups- Evening*

Friday	**April 16, 2010**
8:00	Welcome and Agenda Review, Roll Call and Antitrust Guidelines- *John Lim, Phil Huff, Joe Bucierro*
8:10	Sub-Team Development of Guidance Documents
10:15	*Break*
10:30	SDT Review and Suggested Refinement of CIP Guidance Documents
11:15	Review of May 2010 Technical Workshop Planning and Preparation
11:45	Review of Dallas Agenda and Agree on Next Steps and Meeting Evaluation
12:00	*Adjourn & Lunch*

Appendix # 2 Attendees List
March 9-12, 2010, Phoenix, Arizona

Attending in Person — SDT Members and Staff

1. Rob Antonishen	Ontario Power Generation
2. Jim Brenton	ERCOT (T/W/Th)
3. Jay S. Cribb	Southern Company Services
4. Sharon Edwards	Duke Energy
5. Jeff Hoffman	U.S. Bureau of Reclamation, Denver
6. Gerald S. Freese	America Electric Pwr. (T/W/Th)
7. Phillip Huff, Vice Chair	Arkansas Electric Coop Corporation
8. Doug Johnson	Exelon Corporation – Commonwealth Edison
9. Frank Kim	Hydro One Networks Inc. (T/W/Th)
10. Rich Kinas	Orlando Utilities Commission (Th/F)
12. John Lim, Chair	Consolidated Edison Co. NY
13. David Norton	Entergy (T/W/Th)
14. David S. Revill	Georgia Transmission Corporation
15. Scott Rosenberger	Luminant Energy (T/W/Th)
16. Jonathan Stanford	Bonneville Power Administration
17.Tom Stevenson	Constellation
18.Keith Stouffer	National Institute of Standards & Technology (T/W/Th)
19. John Van Boxtel	WECC
20. John D. Varnell	Technology Director, Tenaska Power Services Co.
21. William Winters	Arizona Public Service, Inc.
Scott Mix	NERC
Howard Gugel	NERC
Joe Bucciero	NERC/Bucciero Consulting, LLC
Robert Jones	FSU/FCRC Consensus Center
Hal Beardal	FSU/FCRC Consensus Center
Stuart Langton	FSU/FCRC Consensus Center
Tom Hoffstetter	NERC (Thurs a.m. by phone)

SDT Members Attending via ReadyTalk and Phone

22. Jackie Collett	Manitoba Hydro
23. Patricio Leon	Southern California Edison (T/W/Th)
24. Kevin Sherlin	Sacramento Municipal Utility District (Th)

SDT Members Not Participating

Joe Doetzl	Kansas City Pwr. & Light Co

Others Attending in Person

Jim Fletcher	AEP
Brian Newell	AEP
Bryn Wilson	OGE
Clyde Poole	TDITX
Rod Hardiman	Southern Company
Elizabeth Moses	Georgia Transmission
Jason Marshall	Midwest ISO

Others Attending via WebEx and Phone

Andres	Lopez	andres.lopez@usace.army.com
Justin	Kelly	FERC
John	Fridye	jfridye@rrienergy.com
Steve	Newman	srnewman@midamerican.com
Maggy	Powell	margaret.powell@constellation.com
Bill	Keagle	william.a.keagle.jr@constellation.com
Steve	Newman	srnewman@midamerican.com
Jerome	Farquharson	jfarquharson@burnsmcd.com

Appendix # 3 — NERC Antitrust Compliance Guidelines

I. General

It is NERC's policy and practice to obey the antitrust laws and to avoid all conduct that unreasonably restrains competition. This policy requires the avoidance of any conduct that
violates, or that might appear to violate, the antitrust laws. Among other things, the antitrust laws forbid any agreement between or among competitors regarding prices, availability of service, product design, terms of sale, division of markets, allocation of customers or any other activity that unreasonably restrains competition.

It is the responsibility of every NERC participant and employee who may in any way affect
NERC's compliance with the antitrust laws to carry out this commitment.

Antitrust laws are complex and subject to court interpretation that can vary over time and from one court to another. The purpose of these guidelines is to alert NERC participants and employees to potential antitrust problems and to set forth policies to be followed with respect to activities that may involve antitrust considerations. In some instances, the NERC policy contained in these guidelines is stricter than the applicable antitrust laws. Any NERC participant or employee who is uncertain about the legal ramifications of a particular course of conduct or who has doubts or concerns about whether NERC's antitrust compliance policy is implicated in any situation should consult NERC's General Counsel immediately.

II. Prohibited Activities

Participants in NERC activities (including those of its committees and Sub-groups) should refrain from the following when acting in their capacity as participants in NERC activities (e.g., at NERC meetings, conference calls and in informal discussions):

- Discussions involving pricing information, especially margin (profit) and internal cost
- information and participants' expectations as to their future prices or internal costs.
- Discussions of a participant's marketing strategies.
- Discussions regarding how customers and geographical areas are to be divided among competitors.
- Discussions concerning the exclusion of competitors from markets.

- Discussions concerning boycotting or group refusals to deal with competitors, vendors or suppliers.

III. Activities That Are Permitted

From time to time decisions or actions of NERC (including those of its committees and Sub-groups) may have a negative impact on particular entities and thus in that sense adversely
impact competition. Decisions and actions by NERC (including its committees and Sub-groups) should only be undertaken for the purpose of promoting and maintaining the reliability and adequacy of the bulk power system. If you do not have a legitimate purpose consistent with this objective for discussing a matter, please refrain from discussing the matter during NERC meetings and in other NERC-related communications.

You should also ensure that NERC procedures, including those set forth in NERC's Certificate of Incorporation and Bylaws are followed in conducting NERC business. Other NERC procedures that may be applicable to a particular NERC activity include the following:

- Reliability Standards Process Manual
- Organization and Procedures Manual for the NERC Standing Committees
- System Operator Certification Program

In addition, all discussions in NERC meetings and other NERC-related communications should be within the scope of the mandate for or assignment to the particular NERC committee or Sub-group, as well as within the scope of the published agenda for the meeting.

No decisions should be made nor any actions taken in NERC activities for the purpose of giving an industry participant or group of participants a competitive advantage over other participants. In particular, decisions with respect to setting, revising, or assessing compliance with NERC reliability standards should not be influenced by anti-competitive motivations.

Subject to the foregoing restrictions, participants in NERC activities may discuss:

- Reliability matters relating to the bulk power system, including operation and planning matters such as establishing or revising reliability standards, special operating procedures, operating transfer capabilities, and plans for new facilities.
- Matters relating to the impact of reliability standards for the bulk power system on

- electricity markets, and the impact of electricity market operations on the reliability of the bulk power system.
- Proposed filings or other communications with state or federal regulatory authorities or other governmental entities.
- Matters relating to the internal governance, management and operation of NERC, such as nominations for vacant committee positions, budgeting and assessments, and
- employment matters; and procedural matters such as planning and scheduling meetings.

Any other matters that do not clearly fall within these guidelines should be reviewed with NERC's General Counsel before being discussed.

APPENDIX # 4
CSO 706 SDT MEETING SCHEDULE
APRIL –DECEMBER 2010

Schedule Convergence: Full CIP V4 Package		
Date	**Week of**	**CIP Task**
SDT Meeting-Atlanta, (4/13-16)	4/12/2010	**Present Controls draft for full team review and comment. Sub team drafting. Finalize draft for Informal Comment, Full Package**
	4/19/2010	**NERC Prepares Full Package for Industry Comment**
	4/26/2010	**SDT Reviews and Approved Full Package for 30-day Industry Comment Period**
5/3/2010	5/3/2010	***Informal Comment Posting for full package starts Completes on 6/2/2010***
SDT Meeting-Dallas, (5/11-14)	5/10/2010	**Prepare for Industry Workshop**
5/19 & 5/20/2010	5/17/2010	**1.5-day Industry Technical Workshop (Dallas, TX)**
	5/24/2010	**SDT Considers Comments from Workshop**
6/4/2010	*5/31/2010*	***2nd Informal comment period ends***
6/2/2010		***Comment Period Ends***
6/3-6/4/2010		***SDT Summarizes Comments Received***
SDT Meeting, Sacramento (6/8-11)	6/7/2010	**SDT Meeting: Comment review, response process, re-drafting, as needed**
	6/14/2010	Sub team meetings
	6/21/2010	Sub team meetings
6/29/2010	6/28/2010	Sub team meetings. SDT interim online meeting.
	7/5/2010	Subteams Package modifications into Standard documents
SDT Meeting, Pittsburgh, (7/13-16)	7/12/2010	**Finalize & Approve Documents for posting for 45 day formal comment period**

Schedule Convergence: Full CIP V4 Package		
Date	**Week of**	**CIP Task**
	7/19/2010	***NERC Prepares Materials/SDT Approves Revisions/NERC Seeks SC Approval for Ballot***
7/26/2010	7/26/2010	***45 Day formal comment period starts (completes 9/8/10) /Ballot Pool formation (completes 8/25/10)***
	8/2/2010	**Industry Comments on Standards**
SDT Meeting, TBD, (8/10-13)	8/9/2010	**SDT Meeting: Prepare for Industry Webinar**
8/18/10	*8/16/2010*	***Hold Industry Webinar***
8/25/2010	8/23/2010	***30 Ballot Preview/Initial Comment Preview ends/Ballot Pool formed***
8/30/2010	*8/30/2010*	***Initial Ballot Starts***
SDT Meeting Winnipeg, (9/7-10)	9/6/2010	**Respond to comments received. Drafting revisions. Review Ballot Results and Additional Comments**
	9/8/2010	**Initial Ballot Ends**
	9/13/2010	Sub team meetings
9/24/10	9/20/2010	Sub team meetings; Full SDT on-line meeting to adopt revised draft of documents
	9/27/2010	NERC Staff Review of Documents and SDT Approval for Re-ballot
10/4 to 10/13/10	10/4/2010	Re-Ballot Period Begins
SDT Meeting TBD, (10/12-15)	10/11/2010	**Prepare responses to 2nd ballot comments**
10/19/2010	*10/18/2010*	***Sub-teams meet to adjust requirements***
10/29/2010	10/25/2010	***Prepare & Finalize revisions to standards and responses to comments on standards***
	11/1/2010	NERC Staff Review of Documents and SDT Approval for Re-ballot
11/8 to 11/17/2010	11/8/2010	3rd Ballot Period Begins

Schedule Convergence: Full CIP V4 Package		
Date	**Week of**	**CIP Task**
SDT Meeting TBD, (11/16-19)	11/15/2010	**Prepare responses to 3rd Ballot comments**
	11/22/2010	*NERC & SDT finalize responses to ballot package*
	11/29/2010	*Seek SC & BOT Approval for Filing*
	12/6/2010	*Seek SC & BOT Approval for Filing*
SDT Meeting TBD, (12/13-17)	12/13/2010	**SDT Meeting to review Filing and Celebrate Project Completion**
	12/24/2010	*Submit for Regulatory Approval*

Appendix #5

CSO 706 SDT DRAFTING SUB-TEAMS

Sub-Team	NERC Standards and DHS Control Families	Team Members
Security Governance	CIP-003 – R1, R2, R3; CIP-005 R4, CIP-007 R8 DHS 2.1 Security Policy, DHS 2.2 Organizational Security, DHS 2.7 Strategic Planning, DHS 2.17 Monitoring and Reviewing Control System Security Policy, DHS 2.18 Risk Management and Assessment, DHS 2.19 Security Program Management	Jon Stanford (Lead), Jerry Freese, Dave Norton
CIP 002-4	Draft revisions to CIP-002-4, and Summary of Responses to Industry comments	John Lim, Dave Revill, Rich Kinas, Jim Brenton, Jackie Collett, Bill Winters, Dave Norton *Rod Hardiman (Observer)*
Personnel and Physical Security	CIP-004 – R1, R2, R3, CIP-006 R1 through R6 DHS 2.3 Personnel Security, DHS 2.11 Security Awareness and Training DHS 2.4 Physical and Environmental Security,	Doug Johnson (Lead), Rob Antonishen, Patrick Leon, Kevin Sherlin
Operations Security	CIP-005 R1, R3 CIP-007 R2, R3, R4, R6 DHS 2.8 System and Communication Protection DHS 2.14 System and Information Integrity	Jay Cribb (Lead), Jim Brenton, Jackie Collette, John Varnell
Recovery and Response	CIP-008 R1 & R2 CIP-009 R1 through R5 Incidence Response and Contingency Planning	Scott Rosenberger (Lead), Joe Doetzl, *Observer Participants: Jason Marshall*
Access Control and Auditing	CIP-003 R5; CIP-005 R2; CIP-007 R5; CIP 004 R4 DHS 2.15 Access Control DHS 2.16 Audit and Accountability	Sharon Edwards (Lead), Jeff Hoffman, Frank Kim *Observer Participants: Sam Merrell*
Change Management, System Lifecycle and Information Management	CIP-003 R6; CIP-007 R1, R7 CIP-003 R4; CIP-005 R5.1.1, R5.1.3 DHS 2.5 System and Services Acquisition, DHS 2.6 Configuration Management and System Lifecycle, DHS 2.10 System Development and Mainten. DHS 2.9 Information and Document Mgt. DHS 2.13 Media Protection	Keith Stouffer, Phil Huff (Lead) *Observer Participants: John Fridye*

Security Controls Sub-Team Principles and Drafting Guidance

CSO 706 SDT SECURITY CONTROLS SUB-TEAM DRAFTING PRINCIPLES

(ADOPTED BY CSO 706 SDT, JANUARY, 2010)

1. Applicability [NERC ROP] Each reliability standard shall clearly identify the functional classes of entities responsible for complying with the reliability standard, with any specific additions or exceptions noted.	**9.Practicality** [NERC ROP] – Each reliability standard shall establish requirements that can be practically implemented by the assigned responsible entities within the specified effective date and thereafter.
2.Reliabiliy Objective [NERC ROP] Each reliability standard shall have a clear statement of purpose that shall describe how the standard contributes to the reliability of the bulk power system.	**10. Consistent Terminology** [NERC ROP] To the extent possible, reliability standards shall use a set of standard terms and definitions that are approved through the NERC reliability standards development process.
3.Performance Requirement or Outcome (NERC ROP) Each reliability standard shall state one or more performance requirements, which if achieved by the applicable entities, will provide for a reliable bulk power system, consistent with good utility practices and the public interest.	**11. Commensurate Controls for BES Impact Categories.** Security controls shall be commensurate with the identified level of BES impact categories.
4. Measurability (ROP) Each performance requirement shall be stated so as to be objectively measurable by a third party with knowledge or expertise in the area addressed by that requirement.	**12. Change Documentation.** Changes from prior versions of CIP Standards have clear rationale. These include the following types of changes: a. Above and beyond the current standards; b. Removal of requirements; and c. Major formatting changes.
5.Technical Basis in Engineering and Operations [NERC ROP] Each reliability standard shall be based upon sound engineering and operating judgment, analysis, or experience, as determined by expert practitioners in that particular field.	**13. Reduce Administrative Overhead**. Administrative documentation shall be kept to the minimum that is necessary
6. Completeness (NERC ROP) Reliability standards shall be complete and self-contained. The standards shall not depend on external information to determine the required level of performance.	**14. Priority.** Implementation plans for the Standards are prioritized according to level of BES impact.
7. Consequences for Non-Compliance [NERC ROP] In combination with guidelines for penalties and sanctions, as well as other ERO and regional entity compliance documents, the consequences of violating a standard are clearly presented to the entities responsible for complying with the standards.	**15. Eliminate or Minimize TFEs.** Security controls shall eliminate or at least minimize the need for TFEs. Allow for compensating controls to mitigate the need for a TFE.
8. Clear Language [NERC ROP] – Each reliability standard shall be stated using clear and unambiguous language. Responsible entities, using reasonable judgment and in keeping with good utility practices, are able to arrive at a consistent interpretation of the required performance.	

SECURITY CONTROLS SUB-TEAM
PROCESS AND DRAFTING GUIDANCE AND DELIVERABLES

Guidance from the January, 2010 Tucker Meeting and the February 2010 Austin Meeting

For the purpose of maintaining consistency across the teams and capturing interim decisions and change documentation, each team should utilize the following development process:

1. **DHS Catalogue of Controls:** Begin by identifying applicable controls that are enumerated in the *DHS Catalog of Control System Security Recommendations* for High Impact Cyber Systems.
2. **Cross Reference CIP Version 3 Requirements/sub-Requirements:** For each security control identified in step 1, cross reference the CIP version 3 Requirement/sub-Requirement or validate previous mapping work.
3. **Specific not Prescriptive:** As a general rule, be specific but not prescriptive in writing the requirements.
4. **"What" not "How":** In general, seek to draft a "what" requirements, not "how" requirements.
5. **Develop the requirement language** for each security control identified in step 1.
   a. When mapping to existing CIP requirements, use language from CIP, making improvements where needed.
   b. When no associated requirement from CIP exists, develop the new requirement using language from the *DHS Catalog*.
6. **Document significant changes to CIP Standards:** Document significant changes made to previous versions of the CIP Standards. Conceptual or broad changes can be captured by a single statement.
7. **Incorporate existing CIP requirements not mapped to the *DHS Catalog*.** If a requirement is no longer necessary because the intent was captured elsewhere, then include this in the change documentation.
8. **Address specific directives from FERC Order 706** that may be applicable to the requirement.
9. **Analysis and Determination of Requirements for Medium and Low Impact:** In the analysis and determination of applicability of requirements to Medium and Low Impact Cyber Systems, consider the cost in relation to the security benefits (i.e., a minimal cost requirement that significantly mitigates risk would apply to *ALL* Cyber Systems. Similarly, a significant cost requirement that minimally reduces risk or provides little additional security may apply only to *HIGH* impact Cyber Systems).
10. **Specify Applicability to Environments:** Specify applicability of a requirement to Generation, Transmission, and/or Control Center environments.
11. **Apply Requirements to BES Cyber System:** Requirements should apply to either:
    (a) The BES Cyber System as a whole, or
    (b) Components of the BES Cyber System. However, when a requirement only applies to specific types of components, Sub-Teams should describe those types of components to determine where component classes exist.

(c) Requirements specific to boundary protection or ESP can be written to the interface of the BES Cyber System.

12: **Level of Requirements:** Sub-Teams should generally write the requirements at a high enough level to avoid applicability of specific technology. Where there are applicable CIP requirements, start with the CIP words and tweak if needed to include some DHS language/concept. However, the "level" of the requirements text should be raised, if needed.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Agenda
Cyber Security Order 706 SDT — Project 2008-06

May 11, 2010 | 1:00 PM to 5:00 PM CDT
May 12, 2010 | 8:00 AM to 5:00 PM CDT
May 13, 2010 | 8:00 AM to 12 PM CDT
Dallas TX

NOTE:
1. Agenda Times May be Adjusted as Needed during the Meeting
2. Drafting Team Meetings May Not Have Access to Telephones and Ready Talk

Proposed Meeting Objectives/Outcomes:

- Review the CSO 706 SDT 2010 Work plan and Schedule;
- Review and adopt the CSO 706 SDT 2010 Consensus Procedures as refined;
- Receive updates on other related cyber security initiatives;
- Receive a NERC overview of the Technical Workshop;
- Review and Refine "Parking Lot" Issues from the April, 2010 CIP Documents for Informal Posting;
- Sub-Teams will: detail how FERC directives have been addressed; develop a "change documentation" draft; develop Technical Workshop Presentations; and identify possible guidance areas and bullet lists of guidance content;
- To review a proposal for drafting a CIP Guidance Document for posting in July, 2010;
- To review how the SDT will develop the CIP Measures, VSLs and VRFs for posting in July, 2010;
- To review the May 27, 2010 meeting with NERC/SDT and FERC; and
- Agree on next steps and assignments

Draft Agenda

Tuesday **May 11, 2009**

1:00 p.m.	Welcome and Opening Remarks— *John Lim, Chair & Phil Huff, Vice Chair* Roll Call; NERC Antitrust Compliance Guidelines— *Joe Bucciero* Facilitator review and SDT acceptance of April 13-16, 2010 Atlanta SDT meeting summary
1:10	Review of Meeting Objectives, Agenda and Meeting Guidelines— *Bob Jones*
1:15	Review of April, 2010 Development of the Informal Documents for Posting- What Worked, What Could be Improved

1:30	Discussion of CSO 706 SDT Workplan, Schedule and Sub-team Expectations: May-December, 2010— *Stu Langton*
1:45	Review of Draft SDT Consensus Procedures
2:00	Updates on other related cyber security initiatives— *NERC Staff and SDT Members*
2:10	Technical Workshop Overview- Planning and Preparation- *Gerry Adamski?*
2:30	Review and Refine of "Parking Lot" Issues Draft from the April, 2010 Informal Posting Documents
3:00	*Break*
3:15	Review and Refine of "Parking Lot" Issues Draft from the April, 2010 Informal Posting Documents
4:45	Review of Expectations for Sub-Team Meetings on Wednesday
5:00	*Recess* ▪ *Possible Sub Team Meetings- Evening*

Wednesday **May 12, 2010**

8:00	Welcome and Agenda Review, Roll Call and Antitrust Guidelines- *John Lim, Phil Huff, Joe Bucciero*
8:10	Security Controls Sub-Team Meetings Orientation and Expectations: • Detail how FERC directives have been addressed; • Develop a "change documentation" draft; • Develop Technical Workshop Presentations; • Identify possible guidance areas and bullet lists of guidance content; and • Begin to identify possible measures, VSLs and VRFs for Formal Comment posting in July.
8:30	Security Controls Sub-Team Meetings
10:30	Break
10:45	Security Controls Sub-Team Meetings
12:30	*Working Lunch*
1:15	Sub-Team Report CIP- 010- FERC directives, Change Documentation and Technical Workshop Presentations, Guidance Bullets
2:00	Sub-Team Reports CIP- 011 FERC directives, Change Documentation and Technical Workshop Presentations, Guidance Bullets
3:00	Break
3:15	Sub-Team Reports CIP- 011 FERC directives, Change Documentation and Technical Workshop Presentations, Guidance Bullets-*continued*
4:55	Review of Proposal for Thursday Agenda
5:00	*Recess* ▪ *Possible Sub Team Meetings- Evening*

Thursday **May 13, 2010**

8:00	Welcome and Agenda Review, Roll Call and Antitrust Guidelines- *John Lim, Phil Huff, Joe Bucciero*

8:10	Sub-Team Reports CIP- 011 FERC directives, Change Documentation and Technical Workshop Presentations, Guidance Bullets-*continued*
10:00	*Break*
10:15	Review Proposal for a Guidance Document Drafting Team
10:30	Review How Measures, VSLs and VRFs will be Produced.
10:45	Review and Adopt SDT Consensus Procedures
11:00	Review May 27, 2010 NERC/SDT Meeting with FERC
11:15	Review of May 2010 Technical Workshop Planning and Preparation including Tuesday evening SDT Technical Workshop "Walk Through."
11:45	Review of Sacramento Agenda and Agree on Next Steps and Meeting Evaluation
12:00	*Adjourn & Lunch*

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Cyber Security Order 706 Standard Drafting Team (Project 2008-06)

1. Chairman	**John Lim**, CISSP Department Manager, IT Infrastructure Planning	Consolidated Edison Co. of New York New York, New York
2. Vice-Chairman	**Philip Huff** Manager, IT Security and Compliance	Arkansas Electric Cooperative Corporation Little Rock, Arkansas
Members		
3.	**Robert Antonishen** Protection and Control Manager, Hydro Engineering Division	Ontario Power Generation Inc. Niagara-on the-Lake, Ontario
4.	**Jim Brenton**, CISSP-ISSAP Director, CIP Standards Development	Electric Reliability Council of Texas, Inc. Taylor, Texas
5.	**Jackie Collett** Cyber Security Operations Engineer	Manitoba Hydro Winnipeg, Manitoba
6.	**Jay S. Cribb** Information Security Analyst, Principal	Southern Company Services, Inc. Atlanta, Georgia
7.	**Joe Doetzl** Manager, Information Security	Kansas City Power & Light Co. Kansas City, Missouri
8.	**Sharon Edwards** Project Manager	Duke Energy Cincinnati, Ohio
9.	**Gerald S. Freese** Director, Enterprise Information Security	American Electric Power Columbus, Ohio
10.	**Jeffrey Hoffman** Chief Architect IT Policy & Security Division	U.S. Bureau of Reclamation Denver Federal Center Denver, Colorado
11.	**Doug Johnson** Operations Support Group Transmission Operations & Planning	Exelon - Commonwealth Edison Lombard, Illinois
12.	**Patricio Leon-Alvarado** Engineer, E&TS Compliance and Quality	Southern California Edison Pomona, California
13.	**Frank Kim** Director, Power System Information Tech.	Hydro One Networks, Inc. Barrie, Ontario
14.	**Richard Kinas** Manager of Standards Compliance	Orlando Utilities Commission Orlando, Florida
15.	**David L. Norton** Policy Consultant - CIP	Entergy Corporation New Orleans, Louisiana
16.	**David S Revill** Group Lead, Electronic Maintenance	Georgia Transmission Corporation Tucker, Georgia
17.	**Scott Rosenberger** Director, Security and Compliance	Luminant Dallas, Texas
18.	**Kevin Sherlin** Manager, Business Technology Operations	Sacramento Municipal Utility District Sacramento, California
19.	**Jon Stanford** Chief Information Security Officer	Bonneville Power Administration Portland, Oregon
20.	**Thomas Stevenson** Gen Supv. Engineering Projects Generation Services Dept	Constellation Energy Baltimore, MD
21.	**Keith Stouffer** Program Manager, Industrial Control System Security	National Institute of Standards & Technology Gaithersburg, Maryland
22.	**John Van Boxtel** CIP Compliance Engineer	Western Electricity Coordinating Council Vancouver, WA 98662
23.	**John D. Varnell** Director, Asset Operations Analysis	Tenaska Power Services Co. Arlington, Texas

24.	**William Winters** IS Senior Systems Consultant	Arizona Public Service Co. Phoenix, Arizona
Consultant to NERC	**Joseph Bucciero** President and Executive Consultant	Bucciero Consulting, LLC 3011 Samantha Way Gilbertsville, Pennsylvania 19525
Facilitator Consultant	**Hal Beardall**	FCRC Consensus Center Florida State University
Facilitator Consultant	**Robert M. Jones**	FCRC Consensus Center Florida State University
Facilitator Consultant	**Stuart Langton, PhD**	FCRC Consensus Center Florida State University
NERC Staff	**Gerard Adamski** Vice President and Director of Standards	North American Electric Reliability Corporation Princeton, New Jersey
NERC Staff	**Michael Assante** Vice President & CSO	North American Electric Reliability Corporation Princeton, New Jersey
NERC Staff	**Howard L. Gugel** Standards Development Coordinator	North American Electric Reliability Corporation Princeton, New Jersey
NERC Staff	**Roger Lampila** Regional Compliance Auditor	North American Electric Reliability Corporation Princeton, New Jersey
NERC Staff	**Scott R Mix** Manager Infrastructure Security	North American Electric Reliability Corporation Princeton, New Jersey
NERC Staff	**David Taylor** Manager of Standards Development	North American Electric Reliability Corporation Princeton, New Jersey
NERC Staff	**Todd Thompson** Compliance Investigator	North American Electric Reliability Corporation Princeton, New Jersey

CSO 706 SDT SCHEDULE: FULL CIP V4 PACKAGE		
Week Of	*Key Dates*	*CIP Task*
4/12/2010	**SDT Meeting Atlanta, GA (SouthernCo) (4/13-16)**	**Present Controls draft for full SDT review and comment. Sub team drafting. Finalize draft for Informal Comment, Full Package**
4/19/2010	4/19-4/23/2010 4/23/2010	**SDT Sub-Teams and Leads Meet to Finalize Documents** **NERC Receives and Prepares Full Package for Industry Comment**
4/26/2010	**4/26/2010** **4/27/2010** **4/28/2010** **4/29/2010**	**SDT Sub-Teams Develop Package** **SDT Reviews with NERC Staff Proposals** **SDT Scoping Meeting on Documents** **SDT Reviews and Approves Full Package for 30-day Industry Comment Period**
5/3/2010	**5/4/2010**	**Informal Comment Posting for full package starts** **Completes on 6/3/2010**
5/10/2010	**SDT Meeting Dallas, TX (Luminant) (5/11-13)**	**Review Parking Lot Issues, Prepare for Industry Workshop and Begin Development of Guidance Documents**
5/17/2010	5/19 & 5/20/2010	**1.5-day Industry Technical Workshop (Dallas, TX)**
5/24/2010	5/24 to 5/28/2010 5/27/2010	**SDT Considers Comments from Workshop** **Meeting with FERC to Review Standards and Posting**
5/31/2010	6/3/2010 6/4/2010	**Informal comment period ends** **SDT Reviews Comments Received** Sub team meetings to Review Comments Received
6/7/2010	6/7/2010 **SDT Meeting, Sacramento, CA (SMUD) (6/8-11)**	Sub team meetings to Review Comments Received **SDT Meeting: Industry Comment review, response process, re-drafting, as needed**
6/14/2010		Sub team meetings
6/21/2010		Sub team meetings
6/28/2010	6/29/2010	Sub team meetings. SDT interim online meeting.
7/5/2010		Sub teams Package modifications into Standard documents

CSO 706 SDT SCHEDULE: FULL CIP V4 PACKAGE		
Week Of	*Key Dates*	*CIP Task*
7/12/2010	**SDT Meeting, Pittsburgh, PA (CERT) (7/13-16)**	**Finalize & Approve Documents for posting for 45 day formal comment period**
7/19/2010		**NERC Prepares Materials/SDT Approves Revisions/NERC Seeks SC Approval for Ballot**
7/26/2010	7/26/2010	**45 Day formal comment period begins (closes on 9/8/2010)**
8/2/2010		**Formal comment period for CIP standards**
8/9/2010	**SDT Meeting, Chicago, IL (ComEd) (8/10-13)**	**SDT Meeting: Prepare for Industry Webinar**
8/16/2010	8/16/2010 8/18/2010	**Ballot Pool Formation Begins (completes 8/30/2010)** **Hold Industry Webinar (tentative)**
8/23/2010	8/25/2010	**Comment Preview Period Ends** **Ballot Pool formed**
8/30/2010	8/30/2010	**Initial Ballot Begins**
9/6/2010	**SDT Meeting Winnipeg, Canada (Manitoba Hydro) (9/7-10)**	**Respond to comments received. Drafting revisions. Review Ballot Results and Additional Comments**
9/8/2010		**Initial Ballot Ends**
9/13/2010		Sub team meetings
9/20/2010	9/24/2010	Sub team meetings; Full SDT on-line meeting to adopt revised draft of documents
9/27/2010		NERC Staff Review of Documents and SDT Approval for Re-ballot
10/4/2010	10/4 to 10/13/2010	Re-Ballot Period
10/11/2010	**SDT Meeting, Toronto, Canada (OPG) (10/12-15)**	**Prepare responses to 2nd ballot comments**
10/18/2010		**Sub-teams meet to adjust requirements**

CSO 706 SDT SCHEDULE: FULL CIP V4 PACKAGE		
Week Of	*Key Dates*	*CIP Task*
10/25/2010	10/29/2010	**Prepare and Finalize revisions to standards and responses to comments on standards**
11/1/2010		NERC Staff Review of Documents and SDT Approval for Re-ballot
11/8/2010	11/8 to 11/17/2010	3rd Ballot Period (if needed)
11/15/2010	**SDT Meeting, Baltimore, MD (Constellation Energy) (11/16-19)**	**Prepare responses to 3rd Ballot comments**
11/22/2010		*NERC and SDT finalize responses to ballot package*
11/29/2010		*Seek SC and BOT Approval for Filing*
12/6/2010		*Seek SC and BOT Approval for Filing*
12/13/2010	**SDT Meeting Tampa, FL (FRCC) (12/13-17)**	**SDT Meeting to review Filing Project Completion**
12/24/2010		***Submit for Regulatory Approval***

CYBER SECURITY FOR ORDER 706 STANDARD DRAFTING TEAM
Proposed Refinements to CSO 706 SDT Consensus Guidelines *(May, 2010)*

(To be Reviewed at the May 11-13, 2010 CSO 706 SDT Meeting in Dallas, TX)

The Cyber Security for Order 706 Standard Drafting Team (Team) will seek consensus on its recommendations for any revisions to the CIP standards.

Consensus Defined. Consensus is a participatory process whereby, on matters of substance, the Team strives for agreements which all of the members can accept, support, live with or agree not to oppose. In instances where, after vigorously exploring possible ways to enhance the members' support for posting CIP standards documents for industry comment or balloting, and the Team finds that 100% acceptance or support of the members present is not achievable, decisions to adopt standards documents for balloting will require at least 75% favorable vote of all members present and voting. This super majority decision rule underscores the importance of actively developing a Team consensus on substantive issues, which the industry will need to approve, by a 2/3's vote.

Postings for Industry Comment. For decisions on CIP standards documents to be posted for industry comment where the Team finds that 75% acceptance or support is not achievable but an option or options under consideration had greater than 50% support from the Team, the Team's accompanying Comment form will seek industry input to help the Team resolve any differences and select an option going forward.

Quorum Defined. The Team will make decisions only when a quorum is present. A quorum shall be constituted by at least 2/3 of the appointed members being present in person or by telephone.

Electronic Mail Voting. In instances when a quorum is not present (in the room and/or on the phone), the Chair may call for an option or proposal to be circulated by electronic mail for a vote by all SDT members. The notice of an electronic mail vote with a deadline will be conveyed by electronic mail to all SDT members. Results of an electronic mail vote will be sent to all SDT members and those on the "plus" list and reviewed at the next face-to-face SDT meeting.

Consensus Building Techniques and Robert's Rules of Order. The Team will develop its recommendations using consensus-building techniques with the leadership of the Chair and Vice Chair and the assistance of the facilitators. Techniques such as brainstorming, ranking and prioritizing approaches will be utilized. The Team's consensus process will be conducted as a facilitated consensus-building process. Only Team members may participate in consensus ranking or votes on proposals and recommendations. Observers/members of the public are welcome to speak when recognized by the Chair, Vice Chair or Facilitator.

The Team will utilize Robert's Rules of Order *(as per the NERC Reliability Standards Development Procedure)*, as modified by the Team's adopted procedural guidelines, to make and approve motions. However, the 75% super-majority voting requirement will supersede the normal voting requirements used in Robert's Rules of Order for decision-making on substantive motions and amendments to motions. The Team will develop substantive written materials and options using their adopted

facilitated consensus-building procedures, and will use Robert's Rules of Order only for formal motions once the Chair determines that a facilitated discussion is completed.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

SDT Consensus Guidelines
Adopted Unanimously, November 13, 2008

Cyber Security for Order 706 Standard Drafting Team

The Cyber Security for Order 706 Standard Drafting Team (Team) will seek consensus on its recommendations for any revisions to the CIP standards.

General consensus is a participatory process whereby, on matters of substance, the members strive for agreements which all of the members can accept, support, live with or agree not to oppose. In instances where, after vigorously exploring possible ways to enhance the members' support for the final package of recommended revisions, and the Team finds that 100% acceptance or support of the members present is not achievable, final consensus recommendations will require at least 75% favorable vote of all members present and voting. This super majority decision rule underscores the importance of actively developing consensus throughout the process on substantive issues with the participation of all members. In instances where the Team finds that even 75% acceptance or support is not achievable, the Team's report will include documentation of any differences as well as the options that were considered for which there was greater than 50% support from the Team.

The Team will develop its recommendations using consensus-building techniques with the leadership of the Chair and Vice Chair and the assistance of the facilitators. Techniques such as brainstorming, ranking and prioritizing approaches will be utilized. The Team's consensus process will be conducted as a facilitated consensus-building process. Team members, NERC staff and facilitators will be the only participants seated at the table. Only Team members may participate in consensus ranking or vote on proposals and recommendations. Observers/members of the public are welcome to speak when recognized by the Facilitator and all written comments submitted on the comment forms will be included in the Team and facilitators' summary reports.

The Team will make decisions only when a quorum is present. A quorum shall be constituted by at least 51% of the appointed members being present (simple majority). The Team will utilize Robert's Rules of Order *(as per the NERC Reliability Standards Development Procedure),* as modified by the Team's adopted procedural guidelines, to make and approve motions; however, the 75% supermajority voting requirement will supersede the normal voting requirements used in Robert's Rules of Order for decision making on substantive motions and amendments to motions. In addition, the Team will utilize their adopted meeting guidelines for conduct during meetings. The Team will make substantive recommendations using their adopted facilitated consensus-building procedures, and will use Robert's Rules of Order only for formal motions once a facilitated discussion is completed.

The presiding chair and/or Facilitator of the SDT, in general, should use parliamentary procedures set forth in Robert's Rules of Order, as modified by the Team's adopted procedural guidelines.

To enhance the possibility of constructive discussions as members educate themselves on the issues and engage in consensus-building, members agree to refrain from public statements that may prejudge the outcome of the Team's consensus process. In discussing the Team process with the media, members

agree to be careful to present only their own views and not the views or statements of other participants and/or may direct such inquiries to the Team Chair and Vice Chair. In addition, in order to provide balance to the Team process, members agree to represent and consult with their stakeholder interest group.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Notes
Cyber Security Order 706 SDT — Project 2008-06

April 13, 2010 | 1:00 PM to 5:00 PM EDT
April 14, 2010 | 8:00 AM to 5:00 PM EDT
April 15, 2010 | 8:00 AM to 5:00 PM EDT
April 16, 2010 | 8:00 AM to 1:00 PM EDT

Unanimously Adopted, May 13, 2010

Robert Jones, Stuart Langton, and Hal Beardall
Facilitation and Meeting Design
FCRC Consensus Center, Florida State University

Joe Bucciero, Bucciero Consulting, LLC

http://www.nerc.com/filez/standards/Project_2008-06_Cyber_Security.html

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

CSO706 SDT April 13-16, 2010 Meeting Summary Contents

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

CSO706 SDT APRIL 13-16, 2010 MEETING
EXECUTIVE SUMMARY

On Tuesday afternoon, the Chair, John Lim welcomed the members to the SDT's 21st meeting. Joe Bucciero conducted a roll call of members and participants in the room and on the conference call. The host Jay Cribb, a SDT member, welcomed everyone to the facilities and covered logistics. Bob Jones, facilitator, reviewed the proposed meeting agenda. On Friday morning the SDT approved without objection the meeting summary for the March 9-12, 2010 SDT session in Phoenix, Arizona. Mr. Bucciero reviewed the need to comply with NERC's Antitrust Guidelines.

Stu Langton presented a proposed CSO 706 SDT schedule which was circulated within a day of the meeting and made adjustments in the process to allow for NERC reviews and formatting of materials.

John Lim provided an overview of the revisions of CIP-002 Draft Final and SDT Industry Response Document since the Phoenix meeting. The SDT discussed the following topics:

- "Immediately affect real time operations."
- Interconnections.
- Attachment 2, Item 1.6- 3 or more transmission lines.
- VSLs
- Miscellaneous topics including functions, compliance issues,

The Chair noted that since the Phoenix meeting, much work has been done by the CIP 002 Sub-team responding to the input and suggestions received. The Team sent to NERC staff a preliminary draft for their input. However subsequent to submitting the drafts to NERC, the Sub-teams produced further refinements to their drafts. The Team agreed to review the NERC comments and consider them in relation to the current draft of CIP-010. Howard Gugel led the SDT discussion of the NERC staff comments on the earlier draft of CIP-002 as well as various proposed edits, such as using the term "requirements" throughout the documents, utilizing owner/operator vs. user, defining "immediate" and "situational awareness." The SDT reviewed all of CIP 002 requirements and Attachments #1 and #2 and took a number of polls on whether to accept the proposed NERC edits.

On Friday, John Lim reviewed CIP 002 Sub-team's redline version to address some of the issues raised earlier in the meeting and reviewed the proposed language on: Definition of BES Cyber System and the definition of "immediate"; High impact rating; and Transmission facilities.

On Wednesday, the SDT reviewed the work of the CIP 003-009 Sub-teams since the Phoenix meeting (including Change Management; Access Control and Auditing; Recovery and Response; Operations; and Personnel and Physical Security). The SDT

focused first on reviewing and refining the Security Governance requirements including the proposed 9 category areas.

Wednesday evening the Chair asked Howard Gugel to prepare a sample "proof of concept" for the access control requirements to inform a decision regarding format of the standards.

Thursday afternoon the SDT reviewed each of the sub-team's draft requirements as revised and refined in the sub-team meetings on Wednesday, offering guidance on various issues raised by the draft requirements.

The SDT reviewed and confirmed previous decisions to use tables in the new CIP standards and to formulate objective statements for each requirement. Sharon Edwards presented the work to date on access control including CIP-004 R4, CIP-005 R2, CIP-008 R5 and dispersed throughout the standard as a way to highlighting the presentation of different formats. Following this the SDT reviewed three format options:

- **Option 1.** Keep CIP-003 to-009 and work from there.
- **Option 2**: retire existing CIP standards and organize the new standards by the topics in sequence from CIP-010 on. (e,g,.,Access Control could be CIP-017).
- **Option 3:** One big standard document with 2 sections CIP-010 (formerly CIP-002) and CIP-011 (formerly CIP-003 to -009). All controls requirements would be together in one CIP standard, with CIP-011:
  - R1 (security policies) addressing all topics.
  - R2 implement per table
  - R3- table for access control
  - R4 implement 2nd table (account specifications)
  - etc.

The Team following the discussion of the pros/cons of the options, voted first on each of the three options indicating its acceptability. Following that each Team member voted to support the option they found most acceptable or preferable based on the discussion and their perspective.

Format Option 1: keep existing CIP 003 to 009 in its current form maintaining its existing logical construct (may involve minor movement of existing requirements between standards)

Yes	*No*	*Indifferent/could go either way*
8	**7**	**3**

Format Option 2: Retire 003 to 009, create new CIP 011-17 grouping according to small group assignments.

Yes	*No*	*Indifferent/could go either way*
12	**2**	**6**

Format Option 3: Collapse CIP 003-009 into a single standard that contains all requirements created/edits by the sub-teams and grouped according to sub-team assignments.

Yes	*No*	*Indifferent/could go either way*
12	**7**	**2**

The team then voted for one of the two highest ranked options under consideration:

- Option 2: Retire 003 to 009, create new CIP 011-17 grouping according to small group assignments.
  ***Yes*=6**
- Option 3 Collapse CIP 003-009 into a single standard that contains all requirements created/edits by sub-teams and grouped according to sub-team assignments.
  ***Yes*=10**
- *Abstained from voting for Option #2 or #3:* 4

At the end of Thursday, the Team took up the format issue again. The Vice Chair made a proposal that the Team use Option 2 (which would renumber the requirements using the topics to organize them).

The facilitators polled the team on their support for the **Option #2 (multiple standards) and 7 of 16 members** were in support of utilizing this as the format. An additional member joined and the Team then tested support for **Option 3 (putting all into single standard) and 9 of 17 supported using this format.** Neither format approach received sufficient support to make an SDT decision.

The Team then reviewed and tested support for each of the following propositions:

1. Change from existing CIP numbering system? Yes- 13 favor changing (of 17 = 76%)
2. Adopt the proposed headings for the requirements as the categories whether as one or multiple standards? Yes-13 (of 17 = 76%)

On Friday morning the SDT took up the final review of format options for the informal posting document(s) in order to make a decision.

The facilitator suggested the SDT use an acceptability ranking of the two possible format options that had been discussed and debated yesterday followed by clarification of concerns to see if they could be met and a requisite number of members could agree on the format to use for the informal posting.

- **Option #2 – Requirements in Multiple Standards.** Use the Topical areas discussed on Thursday and utilize multiple standards (example CIP 010 -020). CIP 002 also gets re-numbered.
  4**=3,** 3**=7,** 2**=6,** 1-**0** *(Avg. 2.81)*

- **Option #3 – Requirements all in One Standard.** Use the Topical areas discussed on Thursday, but one new standard is posted containing sections for all topics. 4=**6,** 3=**5,** 2=**3,** 1=**2** *(Avg. 2.93)*

The 17 SDT members present then voted for their preference for posting for informal comment between the two options with the following result:

- **Option #2** *(multiple standards)* **Yes= 6 (35%)**
- **Option #3** *(single standard)* **Yes= 11 (65%)**

The SDT agreed that while this decision to post for informal comment has a majority support (65%) but not the super majority (75%) of the members called for in the decision rules, the Team is asking for industry comment and input on the formats through the comment form before finalizing a format to present in the formal comment draft in July, 2010. The Team discussed that this approach is consistent with the spirit of the following consensus rule provision: "In instances where the Team finds that even 75% acceptance or support is not achievable, the Team's report will include documentation of any differences as well as the options that were considered for which there was greater than 50% support from the Team."

On Friday the Chair reviewed the schedule, assignments and next steps for the SDT to produce a final version for posting on May 3, 2010. Joe Bucciero will lead, with assistance from Howard Gugel, preparation of the draft of comment form with information provided by each of the Sub-team leads. A question will also be added based on the discussion on the format of the CIP Standards. The SDT will need to begin creating an implementation plan for posting in July for formal comment. A small group of SDT members needs to be formed to provide some framework for discussion at the May meeting (in Dallas) and to answer any questions at the May SDT Workshop in Dallas. Scott Mix will be looking for individuals to work with him to prepare the Implementation Plan, and this will occur after May 3. The SDT agreed that the cover letter for the informal May 3 posting of the draft CIP Standards should speak to the SDT's philosophy on implementing the plan. Jackie Collett, John Lim and Doug Johnson agreed to work with Scott Mix on developing a draft implementation plan.

The Chair reviewed and the SDT agreed on the schedule of activities from Monday, April 19, to posting of the draft CIP Standards on Monday, May 3. The Chair and Vice Chair and the SDT thanked Jay Cribb for his excellent hosting and Southern Company for the great facilities.

The meeting adjourned at 12:00 p.m.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

CYBER SECURITY ORDER 706 SDT- PROJECT 2008-06
21ST MEETING SUMMARY

April 13-16, 2010
Atlanta, Georgia

I. AGENDA REVIEW AND WORKPLAN

A. Agenda Review

On Tuesday afternoon, the Chair, John Lim welcomed the members to the SDT's 21st meeting. Joe Bucciero conducted a roll call of members and participants in the room and on the conference call *(See Appendix #2*). The host Jay Cribb, a SDT member, welcomed everyone to the facilities and covered logistics. The Chair reviewed the following meeting objectives:

- Review the revised CSO 706 SDT 2010 Work plan and Schedule
- Receive updates on other related cyber security initiatives
- Receive a NERC update on implementing the CIP Communication Plan and the May 2010 Technical Workshop
- Review, refine and adopt the Draft Final CIP-002-4 for industry informal comment
- Review, refine and adopt the Sub-Team Security Control Requirements draft for industry informal comment
- Develop related CIP 002 and Security Controls Requirements Guidance Documents
- Agree on next steps and assignments

Bob Jones, facilitator, reviewed the proposed meeting agenda *(See appendix #1*). On Friday morning the SDT approved without objection the meeting summary for the March 9-12, 2010 SDT session in Phoenix, Arizona.

Mr. Bucciero reviewed the need to comply with NERC's Antitrust Guidelines *(See Appendix #3).* He urged the team and other participants in the process to carefully review the guidelines as they would cover all participants and observers. He urged all to avoid behaviors or appearance that would be anti-competitive nature and also reminded the group of the sensitive nature of the information under discussion.

B. Workplan Schedule Review

Stu Langton presented a proposed CSO 706 SDT schedule which was circulated within a day of the meeting and made adjustments in the process to allow for NERC reviews and formatting of materials. Joe Bucciero suggested the SDT might want to review this overnight and take up first thing on Wednesday morning.

II. CIP 002 REQUIREMENTS

A. Overview of CIP-002 Requirements

John Lim provided an overview of the revisions of CIP-010 Draft Final and SDT Industry Response Document since the Phoenix meeting, noting the following:

- R1 changes: "Uniquely" changed to the adverb "discretely,"
- Member comments and suggestions included: take the adjective out. Consider "discretely" "distinctly" May not need this word. The call is document all; this may be "lawyer bait."
- R2- "appropriately: added.
- Attachment 2. Used terms defined in the glossary. Didn't change thresholds. 1.2- struck generation. Threshold too high. 1.6- before had separate criteria for protective systems. And protected at 350 or higher without any qualifications. Covered all substations at 350 KV. Not intended. Merged with 1.11 with 1.6.
- Medium: thresholds lower than before. Protection systems with 3 or more lines. Rest fall into the medium.
- Member comments: 2.5- no fax systems- everyone is high? This is an oversight.
- Low Impact: added to be consistent with high and medium.

SDT Comments on Overview

"Immediately affect real time operations."

- Short range planning impact issue? Other situational awareness but not in the "immediately affect real time operations" language? Does it include next day planning?
- John Lim noted that they didn't have a consensus in the group on this.
- "Immediately"- what does this mean? Week, day, now? Are they needed.
- Maybe we should distinguish from planning and real time operation.
- Since you refer to operations planning in part 1. In part 2 need to apply to operations planning.
- Look at beginning of Attachment #1 language.
- Attachment 2- 1.1- "facilities – why combine generation facilities?
- BES cyber system is subject which covers shared cyber system.

Interconnections.

- Texas- lower requirement for ERCOT? Why a separate requirement for ERCOT? Different size in terms of megawatt capability and mode.
- Why have spinning reserve requirements higher in ERCOT?
- This focuses on the Texas and Quebec interconnections.

- Did SDT December posting allowed for regional variation? Not by regional variations but by interconnection variations. Numbers come from category 3 events.
- Definition of control center? Lower threshold will bring in more things. E.g. 1.7 medium- primary and backup control centers? Are these defined? How are they distinguished from control centers? Shouldn't assume everyone understands these terms.
- Work is being done on a NERC back up facilities standard. Went through initial ballot but didn't get support on that proposal.

1.6- 3 or more transmission lines.

- 1.6- what was technical basis behind 3 lines?
- 1.6- 3 or more transmission lines? Individual connectors? What about DC circuit with 2 lines on the tower? One transmission line or referred to as conductors or phases.
- In the context of transmission planning studies, 2 or more would be ridiculous. 3 or more is a good place to draw a line.
- We have redundant subsystems. 3 line threshold may be too low some companies.
- 5 transmission lines would be hard to justify for a national standard. 300 kv above and higher.
- Multiple entities have asked for the technical basis for this. Need to respond if we leave it at 3.
- "Or that remotely control a BES asset with a high impact rating" Asset= facility? Hardware?

VSLs

- VSLs measure R1 in terms of how many you miss. Assumes auditors know the right total. How will this be computed. This is defined by the entity. These are squishy number to begin with.
- Auditors won't use this. This is not looked at part of the audit itself. Use only when there is an alleged violation. After a potential violation an investigation is conducted to confirm a violation and the circumstances associated with a violation. Then someone comes to do analysis what the count should have been.
- Every requirement must have a VSL or FERC won't accept.
- We can make this a number vs. a %. 1, 2 or 3. Have not been identified more than 3 high.
- Previous VSLs had numbers. Some entities have suggested 5 could be a small number.
- Don't see the difference between 1 and %. Issue is entity is identifying the cyber system. Investigator and entity work together to define- a number or % calculated.
- Are we spending too much time on VSLs? Difficult to correlate the auditing fine and the VSLs. What value is added by debating VSLs *ad naseum*.
- What about using "misidentified"
- Get rid of % but develop better definition of the BES cyber system

Miscellaneous

- Is the whole functions area a mush?

- BES cyber system identification is up to the entity. Entities will appropriately draw the line in different ways.
- This is where we need NERC compliance to weigh in to provide advice to the SDT.
- Concrete recommendation: Eliminate line 1 on chart since it is untenable since you can't calculate a %.
- This is not an audit tool to determine if you have met the requirement.
- Requirement is to identify all BES cyber systems.
- First step is to find if you find a BES cyber system that wasn't identified. The investigator will develop the list.
- Add "Additional"?
- From #2, on it presupposes you have a list.

B. NERC Suggested Edits for CIP 002-4 *(Including Maureen Long and Dave Taylor)*

The Chair noted that since the Phoenix meeting, much work has been done by the 002 Sub-team responding to the input . The Team sent to NERC staff a preliminary draft for their input. However subsequent to that the Sub-teams produced further refinements to their drafts. The Team agreed to review the NERC comments in relation to the current draft 002. Howard Gugel led the SDT discussion of the NERC staff comments on an earlier draft of the SDT.

SDT Comments and Polls

Definitions section.

- Functions sentence should remain.
- List doesn't have a proper introduction in Dave's edits.
- Computer systems themselves are control centers, not the dispatch arena etc.? Not supporting
- In the field- this is a control center.
- Is there a something out there- is a computer or a programmable controller.
- This is the first time the SDT is using "computer systems"- will be confusion on this.
- Remote data collection equipment as well.
- A control system vs. control center? Leery to tying back to computers.
- Does fix some physical security if only around computer systems.
- Tied back to EOP 8. Do you need to define control center?
- Go back to original wording. Not trying to define BES cyber system.
- "associated"
- Propose striking second sentence.
- EOP 8- strong linkages with other standards raise double jeopardy issues.
- **Retaining the SDT language:**

Y	N
15	0

- **Add "Functions that support"**

Y	N
15	0

- "typically" in the second sentence)-
- For a definition, we should remove the second sentence.
- "At a minimum"? No.
- Are we removing reference to real time operations?

- Retain the 2nd sentence and remove "typically"?
- Delete: "listed below" in first sentence.
- All agreed. 002 Sub-team will follow up with these changes.
- Purpose addition. OK
- "including the date the identification was performed"? OK no objections all agreed.

R-1

- The 1st thing NERC suggested was to make 1 and 2 a single requirement that has 2 parts.
- If you don't put criteria on correctly but come up with violation. If you have list and criteria. Violation for either part? Or if stick with separately changes for R1 and R2. This might eliminate struggles with VSL statement earlier.
- R1- from "all " to "each"? "One or more" If we use R1. Why not make R3 subset of R1?
- NERC had advised against doing sub-requirements?
- Sub points not sub requirements. All one requirement. This is very confusing.
- Leaning towards keeping current structure.
- This format is being used in other standards. Filed with FERC. May be obligated to use. Either way may be acceptable.
- Benefit to sub numbering format. Keeps together things by. Sub numbers help clarify the numbers intent.
- In favor: of **Sub numbers option**

Y	N
7	9

- NERC's suggestions on R1. Requirement is to "identify" and "all" vs. "each". Identify and document each.
- **Should we accept the NERC R-1 recommendations?**

Y	N
1	16

- **Delete "Document"**

Y	N
2	15

- **"Each"**

Y	N
5	12

- Make sure you identify all cyber systems. Indentify suggests uniqueness.
- "Each" identify something- each in a set. Discreetly" problems with how you document. E.g. on multiple lists vs. 1 list.
- What do we mean by BES cyber system- box or applications? What does discreet"
- **Delete "Discreetly**

Y	N
16	0

- Use vs. own (regardless of whether you own it). E.g. I.d. 3rd party tagging application. Have to do something about. "Owns not uses"

- Note that asset owners and operators make for a big difference. Possibly use: "Owns, operates or owns/operates"
- Owner knows what the equipment is but the Operator may not.
- BES cyber systems that execute or enable?
- **"Owns" vs. "uses"**

Y	N
13	4

- Its got to be ownership or else there will be big headaches. Asset means ownership.
- What about jointly owned? Agreements/contracts would address those kinds of issues.
- SDT should lock it one way or another. There will be fewer exceptions with owned than "operates."
- To enable functions. Applicability is solved earlier. This is not the best place to deal with this. Applicability to the standard. The entity will resolve, not us.
- Leaving executes and enables?
- Taking out is not appropriate- Whatever we decide. It will bring comments. At least it is in the open in the informal comment process.
- This is not a new issue. There is joint ownership now under current standards. We operate generation for other. It all comes down to money.
- **"Own" (2nd poll)**

Y	N
11	6

- Figure out what we need to do with joint ownership. Technical owners vs. lease holders.
- Discreetly identify- make sure you can't have things in two cyber systems.
- There is no way to document if you haven't identified. Is this idea redundant?
- We will need to do better on documenting guidance- for industry.
- True requirement is identification. Document is the measure.
- "Appropriate?" This doesn't read well without this word.
- But "appropriate"- doesn't identify anything.
- Can we move benefits to reliability to a guidance document? No, benefits to reliability is needed for each requirement under NERC's current approach.
- **Strike "appropriate"**

Y	N
14	3

- R1. Is the last sentence on the objective superfluous language?
- Breaking out the objective of requirement offers great value in knowing what the objective was in terms to later determining intent.
- NERC's requirement is to set forth the "benefit to reliability." You need the who what and why set out in the requirement.
- Would it be possible to pull out separately? It is confusing to read. Are we bound by format?
- Could change wording, "for the application of security requirements and controls to BES cyber systems."
- SDT- consensus- ok.

R2

- John Lim indicated he believed the sub-team would not have problems with changes suggested by NERC.
- The SDT accepted the changes.
- Should we require "categorize and annually re-categorize."
- Delete re-categorize?
- "Annual" is better used in the attachment.
- **Delete "Re categorize" SDT Consensus= Yes.**
- "and document such categorization for" OK
- Missing a date here? Add here "including the date the identification was performed"?
- Will we have to put into every requirement?
- Look in measures- lists have to be dated. Have to tie this back to the requirement.
- Remove this language from the measure and the requirement. Y 16 N 0

R3

- Do R1 and R2 once. R3 from now on keep it up to date.10 years later you missed a system on the list. Do you violate R3, R1 or both?
- If you never made the change, then you missed it the first time.
- That is why the sub-team added "that it owns or operates "
- What if it is change because of a storm, not planned. "Emergency changes"?
- Concerned about consistency as we go through. End each with the benefit piece. Look at the different wording on R1, R2 and R3. Make consistent. If benefit the same, use same language. R1- to categorize
- Just voted down "owns or operates." Should we delete here? Want to monitor for changes.
- Planned vs. unplanned change. Have to keep the list fairly static. Changes in a planned way so you know to change the cyber system.
- Planned/unplanned—"planned"- triggering issues. May need to look at this some more.
- Is an annual refresh missing where you look at categorization to make sure something didn't happen that you missed?
- "Reviewing the categorization of the BES cyber systems"
- Remember these are minimum requirements. Do we want to state annually. Or leave it up to entity (best practice). If you have a planned change, you have to revisit it. People can revisit anytime they want.
- Can you have a change not specifically planned? To take a line out they have to do some studies to figure this out. This doesn't happen spontaneously.
- **Delete "or operates" yes. All**
- Transmission owners vs. operators- is a problem. R1 has it as "owns."
- Every one else who is a transmission operator. R1 and R2 have to identify assets (probably a control center).
- Categorization- if control center controls a high impact high asset, high impact control center.
- If we already have covered applicability, is it appropriate to put into requirements?
- **Delete "planned = no, All**

- **Add" "<u>the identification and categorization</u>"** Yes All
- **Add " annual review"? "Every 12 months or as …"** Y N
  1 16
- Comes up in R1 and R2- got rid because no reliability benefit.
- The requirement to notify changes to others is not here any longer?
- That is because the BES cyber system is categorized.
- Sub-team Ok with Dave Taylor's suggested edits.
- <u>"to the portion of the BES" ? OK</u> Planned changes for my stuff only.
- "Periodic reassessment?- CIP 002 sub-team dealt with.
- Other changes: calendar OK
- Difference between requirement and controls. Control objective statement 800-53. Writing requirements. Are we authorized to write controls? Source documents are controls based,
- **Use the word <u>requirements</u> throughout documents. All Agreed.**

Measures

- Delete discreetly? Yes, All agree.

Compliance

- Note that data retention language and the audit periods (3 or 6 year cycle). Gap of compliance only keep data for the year not the last audit. Need to keep data since the last time audited.

Attachment 1

- **Scoping statement important- place it first? Yes** Y N
  13 4
- Make this the first sentence?
- Since "real time" was added NERC staff struck the purpose paragraph.
- "Operations planning horizon" ? Do we want to include this in addition to "real time"?
- Planning could affect real time as well.
- This doesn't appear in any R, or attachment 2. List of functions only.
- Reconsider operations planning horizon in all requirements?
- When define the functions could take place in real time or in the operations planning horizon.
- **Reorder the 2 paragraphs? No** Y N
  3 16
- **Delete ~~"these functions take place in real time or operations.~~ Create a single paragraph**. **Yes** Y N
  14 3
- If you delete the above you will have to deal with word "immediately"
- Day ahead? Marketing term.
- Take out planning horizon?
- If you pick wrong units, in real time you will figure out.

- What we are after here are control systems. Protect- 1 and 0s turns into action out there.
- **Delete ~~Immediately ?~~** Y 11 N 6
- Initially defined "immediate" within 15 minutes"
- Real time? 1 hour or less in the NERC glossary. Upper case or affects the operations within 15 minutes.
- Need that kind time frame. We do need to maintain it. If you aren't specific, may put security controls where you don't need them.
- JVB: time frame- affecting real time. Leave immediately there and have real time (lower case).
- Further qualification? Is it and, and/or?
- Intent is the be "and"
- **Delete "further qualifications?" Yes** All
- Is "Immediate" related to ability to act?
- Concerned there could be other cyber systems that don't have immediate affect. The ones of greatest importance, at a minimum, should be protected- this should to be clear.
- **"Can have an immediate effect"** **Yes** Y 14 N 3
- Need a definition of immediate? "Faster than a human reaction"
- e.g. Immediate access revocation- 24 hours.
- Near term.
- What about adding: "only those that have the capability to monitor or control real time operation of the BES"
  Concerned about "monitor." State estimators replacing what you are monitoring.
- "respond" vs. control.
- Is it clear that it control?
- **Support for single reworked paragraph. Yes** Y 17 N 0
- "Dynamic response"- editorial accept. OK
- "Cause a condition" vs. "cause a reaction"? Any difference?
- "Balancing load and generation." Ok
- Controlling Frequency
- "which ensure real time"?
- Cant control without real time. Don't need the clause.
- "Controlling Voltage" editorial accept. OK
- "Managing constraints" editorial accept. OK
- "Control and operation" editorial accept. OK
- Restoration of BES- editorial accept. OK
- "Necessary" should remain.
- "Situational Awareness"
- It is partly a operations planning action?
- Contingency analysis, close to real time (not a day ahead).

- Delete “anticipate and plan”?
- If you take this out and you take out RTOs.
- Solve by eliminating “~~and anticipate effects of planned and unplanned changes to conditions.”~~?
- Take “current” out of it? Immediately affects situational awareness?
- Only reason to use this clause is to scope this down. Addressing concerns that “this applies to everything.”
- “Assess the condition of the Bes necessary for real time operation.”
- Control and operation and situational awareness.
- Difference between monitoring and assessing.
- control and operations- pure SKADA status of components. Situational awareness.
- Assess the current and anticipated operating state (or condition) of the BES?
- Is there different information used to assess the current vs. evaluate what the future?
- It can be data not from a real time environment.
- Day ahead studies, state estimation. Don’t want to get to other studies being done.
- “near term”? data collecting is real time.
- Current, expected and anticipated
- **Situational awareness: activities actions and conditions to asset the current expected and anticipated state of the BES.** ***As revised*** Y N 15 0
- Inter Entity Coordination and Communication
- Active coordination. Communication is the action.
- Coordination of real time operation.
- Add, **“real time coordination”** Yes. All agree.
- Tie to attachment 2? General comment.

Attachment 2

- (“As determined by….”) Maureen Long/NERC suggested a determination.
- “Responsible entities”= functional model entities. We are using this. She has injected this back in. e.g. 1.1 generation operator doesn’t have a role in this.
- “Operations planning”- SDT decided to take out yesterday.
- 1.1- Generation facilities- (as determined by the Generation owner or the generation operator”. Might be at times the generation operator
- This parentheses might be not needed.
- Doesn’t clearly identify shared facility. “if using a shared BES cyber system”
- If he has all BES cyber systems.
- Non-shared system will not be connected with each other.
- “Shared or connected Cyber systems”
- That would be everything in the system.
- “Each BES cyber system that either singly or in combination. **Yes** Y N 13 0
- May not be as clear.

- Remove the rest of sentence (" ~~or more in Texas and Quebec interconnections~~")
- BES cyber system affecting a plant bigger than 2000 MW- everything in it is high impact.
- Each BES cyber system?
- "would" this is a conditional word. That ~~would~~ immediately affects
- That has the capability to immediately? "Has the potential to"? "Can have an immediate effect" (from yester day)
- **Each BES Cyber system that can have an immediate effect on real time operations"**
  All agree.

- This came from a NERC document. Disturbance report Categorization criteria. Done in 2009.
- ERCOT has higher contingency reserve- less than ½ of reserve. Lose 2 units bigger than 1000 MW.
- Engineering analysis language was in December 09 posting.
- Arguing the 1000 MW number
- Any way to ask Planning Committee regarding this issue.
- SM: "good enough to post" to get industry comments back. Leave something in. If you assume 2000 is appropriate for east- % of size of interconnection.
- Impact of loss of MW is the focus.
- **Remove the rest of sentence ~~("or more in Texas and Quebec interconnections")~~**

Y	N
8	8

- **Remove?**

Y	N
13	3

- **Strike 1.1 and look at 1.3 and go with contingency reserve. Defer, for now. Get feedback from the planning committee.**
- **All OK**
- We need a criteria. This is key. Used the disturbance report as basis. What our basis for this concept in 1.1?
- Few generators with 2000 MW – few are high impact.
- E.g. 3 or more transmission lines
- Move to medium vs. dropping?
- Support this. Contingency reserve. We've discussed before. Agreed to leave them in.

1.2
Sub-team ok with NERC edits/additions. SDT ok.

> Facilities, singularly or in combination (if using a shared BES Cyber System), with aggregate higher of the most current and prior to the most current rated net Reactive Power capability of 1,000 MVAR or more in Eastern and Western Interconnections and 500 MVAR or more in Texas and Quebec Interconnections. (As determined by the Generator Owner or Generation Operator, Transmission Owner or Transmission Operator)

1.3 Contingency

- This is an annual reassessment issue
- List of issues for 002-
- Including operator. Why not "as determined by the asset owner." Not clear here.
- Refers to owner of BES cyber system. Put clause- after real power capability?
- Referencing Mod 24 and 26 testing and verification standards. The concern with linking together is possible double jeopardy. Justification in mod standards for doing both. Operator doing verification and Owner doing the setting.
- This may be an across the board issue.

Generation Facilities, singularly or in combination, (if using a shared BES Cyber System), whose aggregate rated net Real Power capability, as defined in 1.1 above, exceeds the largest value, for the 12 months preceding the categorization, of the Contingency Reserve or total of reserve sharing obligations for the Reserve Sharing Group. (As determined by the Generator Owner or Generation Operator)

1.4

- John Lim questioned if the proposed edit is correct.
- "designate" "as designated by". Balancing authority not always the one making the reliability decision.
- Could be a number of entities.
- Unless this is universal, should be these be in at all.
- Propose striking parenthetical.
- Balancing authority- ERCOT e.g. balancing authority. But there are several entities in other places.
- "all reliability coordinators" ?
- "planning coordinator."?
- Who has a generation facility. They know what contracts/terms for their facility. Shouldn't be who is determining. Person with the asset knows.
- Some may be good or not. Possibly delete all.
- You can't have reliability without a review contract. Compliance auditors know if they have in terms of contracts
- Strike throughout attachment.
- Transmission facilities are named. Scoping built in with those words vs. entity type.
- **Strike all parenthetical**.

Y	N
14	0

- 2.7 "or that remotely control a BES asset with a Medium rating"
- 2.5 "including FACTS devises? All high impact or insert language there. (including flexible .)

C. CIP 002 SDT Discussion of Open Issues and Follow Up

- Dave Taylor's VSLs comment (15% high number? Came out of guideline for VSLs.
- Purpose reference to 003-009 will be adjusted after security controls
- Sub-team will go through the measures to ensure they are consistent with the requirements as revised.
- 1.1 and 1.6 in Attachment I.
- "Immediate"
- Annual or periodic
- 1.5. 2.4 Medium- 3 transmission lines right criteria? Where is the right number and what is the basis for that?
- 1.7 transmission facilities. FACTs devices added. Flexible AC Transmission Systems.
- Include "protection system " associated with transmission facilities? In IROLs? What is the reason it is included?
- Added to criteria for threshold for transmission-
- Looking now for consistency.
- In medium added a clause regarding protection systems 300 KV.
- Protection systems added to l.7 (including their associated Protection Systems) Sub-team will resolve how to reference this.
- Control center definition resolved? Yes.
- Is there a cyber component of systems that are not special systems? Yes.
- Retirement of term cyber asset? SDT will need to decide whether to retire.

D. Final CIP 002 (010) discussion

On Friday, John Lim reviewed CIP 002 Sub-team's redline version to address some of the issues raised earlier in the meeting and presented revisions on CIP 002, which were documented in the latest version of CIP 002.

Definition of BES Cyber System + definition of "immediate".
Rather than another definition, the Sub-team proposed to focus on the BES Cyber System definition and added "within 15 minutes" within the BES Cyber System. If the effect on reliability is within 15 minutes then the item is a BES Cyber System. This gives a finite time.
SDT Comments

- Does this include protective relays? Yes.

High impact rating
SDT Comments

- Is this – reserve sharing usually goes up – is it intent to move more in or more out?
- Parenthetical – I understand it but not sure anyone outside this team will understand it
- Meant to qualify or explain as a shared BES cyber system

- This doesn't make the "shared" clear – may need an explanatory box as opposed to a parenthetical
- Delete front end of the parenthetical
- Meant to clarify what it is meant by combined operation
- Using singular or in combination
- Team will work on exact language – concern noted

Transmission facilities

- This language helps but still concerned about parallel lines
- Changed to 4 to address terminal stations
- The parallel lines are a concern in our area
- Not sure we can address in the standard itself
- Other changes are on the medium impact – will need to address some of the comments and changes in the high impact discussion
- 1.14 - Consider moving transmission operator functions to the front of the statement for clarity – agreed
-
- Jackie Collett's email offers a rephrased version of earlier discussion
- May need to take out the first "or" from restatement
- Too long a sentence and confusing, so she tried to break it into two sentences and add punctuation to help clarify.
- Programmable electronic device – don't you want to say processor somewhere? No, working on programmable devices
- Worried about phrasing – if send info to cell phone does that phone become a BES asset – do we need the phrase "on data display"? It is the use of the data displayed that is the problem, not the display of the data.
- Semantics that may cause more problem to correct – need to give it more thought to see if can address without creating more problems
- Shouldn't we pull in language from Attachment #1 to establish what the BES system is?
- Cannot refer to an outside document within a requirement.
- Trying to write the scope into the requirement? Careful, need to keep it general
- May be getting too specific to say data used by an identified operator.
- Would removing "data" address the question? No we are also protecting the data
- What are we adding with the additional statement about BES condition or disturbance? Pull out of here and put into
  Attachment #1 – we are trying to say the function in two different ways and it is confusing.
- But, again we cannot refer to a separate document.
- Shouldn't try to put any of the functions in – gets too messy.
- "relied on to make real time operations decisions"
- Propose taking suggestions to the subgroup for refinement.

- Consider two short definitions – one for BES cyber system and another for cyber system
- Rest of 002 Sub-team will review on Wednesday.
- In definition of situational awareness – when is the anticipated state? What period of time? See qualifier at the top of the page

III. CIP-003-009 REQUIREMENTS (CIP 011)

The SDT first reviewed the Security Governance draft approach and the progress made for each to the Sub-Teams since Phoenix. The Sub-Teams then met on Wednesday to continue drafting work and presented the draft document on Wednesday and Thursday.

A. Security Governance Sub-Team report

- Jon Stanford presented document noting his sub-team had received statements from only two sub-teams- looked to other sub-teams to get their requirements.
- What is the mechanism to get into 003.
- R1: 3 sub bullets. Scope of applicability to organizational and third party personnel
- Security roles and responsibilities
- Identification of a single senior management official with overall responsibility for leading and managing implementation of requirements within these standards.
  - Provision for emergency situations? Address in recovery and response? Policy objectives
  - Annual review and approval of cyber security policy assigned pursuant to R2. Not in agreement.
- Manager responsible for implementing. "review and approve" – suggesting an org structure.
- Separation of duties issue.
- Delete 1.5 out.
- Clause " with authority" is not in current draft.
- 1.3 "with overall authority and responsibility."
- Topical areas removed. Not addressed in policy document? Requirements by topics- replacement for part of your security document.
- From 2 on- cover policy statements by topics. You to have a plan here, topic sections will describe what's in the plan. Took topics out- carry over from Federal thinking. They will be requirement statements.
- 1.3 annual review? IN the base statement in R.1. Require the REs to annually review.
- FERC wants the same person to know about.
- 1.3 overall authority and responsibility.
- Consistency. In CIP 002- eliminated annual review. Initial and upon changes vs.
- Annual review in policy statements and cover it globally.
- Program review if global

- JS: some requirements for annual review of a plan.
- SM: Double jeopardy- how write language of policy in 3 vs. procedures and plans in other standards. Don't link too tightly together.
- Annual review- different from CIP 002 annual review issue. What would be the triggering event? At policy level. Annual review catches what has happened in year.
- Feds- bi-annual review of high level policy document. At least every 2 years.
- Annual review is practiced in the industry. Good to put in as a requirement. Don't need to say who does. Senior manager should approve?
- Tie to responsible entity
- Some have single policy, some have more than one policy. Separate policy for NERC CIP.
- Presupposes they approve.
- Interpretation questions. Single senior manager. Per responsible entity. A company could have different officials. Each functional model entity.
- Double jeopardy issue we can't solve
- By functional model- have many registered entity. Let the organization decide. Can be the same or different.
- CIP Cyber security policy focus here. Consistent with version 3. Not broader security policy.
- Senior manger was to insure accountability. $1 million a day. Why special requirement. FERC directive.

R2

- 4 sub numbers.
- Shall develop a system security plan for each BES Cyber System that: 4 bullets.
- What is the need for this? Comes from a federal space. We may not want a system security plan? (describes operating environment for what you are protecting)
- List of BES cyber system out of 002. Where is the best place to document. Some requirements provide for plans.
- All documentation required. If it is spread around, then take this out.
- Security plan not only in federal model. Becoming a standard way to define system security.
- Maybe as guidance- accumulate documentation and place where makes sense.
- Make auditing easier if they have 1 place to go to for each system. Easier to see how came about. If you provide this.
- Notice requirement for a document for each BES cyber system regardless of level. As written for each and every one. Auditor needs only finds a missing document to be in violation.
- Isn't a new challenge for large multi-nationals. "Real time" operations in CIP 002- number of different REs involved. Compartmentalization. Entergy- single VP- fossil nuclear, distribution, etc. fiduciary presidents of 5 operating companies in 4 states. If divide up may not have security.
- Program plan- describes things you have to address. IN areas such as access control systems
- If came back to command and control fabric- systems that do that. Organization "shall". Have a program plan for how to attack each of the technical area.

- Security plan for each BES cyber system.
- CIP 006 physical security plan that needs to get added.
- Keep this a much higher level.
- Why look at BES system first and then at BES cyber system.
- This could create nightmare scenario.
- Security plan that addresses the following for h/m/l. Not at each cyber system level.
- Too onerous. Have security requirements for low impact systems. Security plan doesn't add much to what you are already doing. Have to document environment to demonstrate compliance. Think of
- For high impact assets need this level of documentation because of their important. Specific plan. At low level, generic plan how we address these as a whole. Not as onerous.
- Program plan approach?
- Other requirements may lend themselves to this.
- Coalesce all the plan requirements into a program plan by topic. High assets- security plan requirements.
- Program plan a good one.
- Incidence response and restoration plan. Just mentioned. Cover exclusion for emergencies.
- Details of what is in the plans in others requirements.
- "The security for each BES cyber system will be addressed in a security plan.
- Responsible entities came from markets. Shakes down to 3 organizations. Operating unit.
- Model for policy statements- in R3.
- Each responsible entity shall:…..
- Program plan-- take each of the topical areas "BES cyber system connections" DHS Control system connections.
- Authorize and document external connections. Only those authorized are in place.
- Revise R2 to include topics.
- R4 down- talks about plans- info protection plans.
- Codify details of procedures.
- Rework R2 and put a program plan approach.

R3

- How is R3 a policy? Embedded in controls document. Pull out of here?
- Won't need this if we take program plan approach.
- **R3 is redundant**. All Agree. JS will remove.
- 3 Rs.- in 003 (manager, program plan)
- E.g. configuration management plan- vulnerability assessment etc. Will these be set out as topics?
- Keep simple, not require multiple plans, but set out the topical areas.
- Probably won't need topical areas going forward.
- Program plan approach simplifies. Collapse these down.
- "Policy"- what do we mean?

- "shall language"- requirements framework- everything is a shall. If you are getting into procedures, attributes. If you are talking about topics.
- E.g. Personnel screening process. Shall have this. Procedure on how implement.
- Have to be careful- shall includes- have to have a policy. These are the areas you have to address in the policy statement about the CIP standards.
- Recovery plans and incidence response plans- not policy? Require you have one and have to do it. Develop and implement the plan.
- The plan must contain the following- e.g. recovery plans must contain….
- E.g. CIP 008 and CIP 003 statement- possible double jeopardy?
- How to deal with CIP 003, if you don't have that requirement as a low? Low impacts that don't require a response plan.
- 1 approach – policy statements you will do access control, you will.
- 2nd approach- you have to have a plan for all these things.
- Current CIP require plans where you may not need plans. Create compliance activities that have been necessary for enhancing security.
- All in a single table- do everything in a table. Policy should address. E.g. 4.3 include applicable controls specific in Table 1 Information Protection Controls.
- CIP standards are topically light and DHS are topically heavy.
- Agreed on program plan approach. Don't know where policy will go. Then come back with a proposal.
- Easy to write a double jeopardy requirement. Just to create policy statements. Policy statement you have to have recovery plan. CIP 008 and 009- plan contents. Measure for the policy- policy statement. If measure in CIP 003- you have plans to support the policy. Draw a line between requirements for policies and writing plans.
- Sending over the plan? Annual review and updates in CIP 003. CIP 006 here is what plan contain.
- This is a global question. Handle annual review in 003 or in the subsections?
- Requirement- policy statement that addresses recovery plans. Go to CIP 8 & 9 about content of plans.
- In requirement- state what the policy must address. Guidance document to be developed what the thought was behind the requirement.

R4

- R4 a problem? Looks ok.
- R4- e.g. where you are putting in requirements for the contents of plan. Here just say you have to have a plan.
- If this creates a double jeopardy problem would have to roll up into R1.
- Address the topic of information protection.
- Read it as a family of one. Why not make it one.
- Tie up topical areas in R1. Policy statement to be made in topical areas will be made in the sections.
- Does this raise double jeopardy issues?

- Puts all high level requirements in one place- shows accountability.
- Asking whether we need policy statements in CIP? Every requirement in standards is a policy?
- In practice, that is how they are written today. Current 003- policies should address all requirements.
- Doing it by topic. Not as granular as current 003.
- Placed some of these info mgt requirements here in the last week- they tie the policies to the program elements. Put things together that belong together.
- Why not put under a single standard?
- Put all tables in a single standards
- Take outliers and make them standards themselves.
- Existing format- CIP 003 policy for this, implemented in CIP 005 .
- If we change into one standard, we will hurt ourselves with the outside world.
- Move to their own standard. CIP 007 single requirement about access control.
- Standard- talks about access control (physical or otherwise)
- Does NERC have a definition. CIP 006 physical security plan. CIP 004 cyber security control training program. Do we need to get one?
- Use the same word across all standards.
- What do want to call this? "Program" is what you are doing.
- Collect all the topics together. Figure out how to put together as a team. Plans, Programs,
- 002 about scope. 2nd is about governance- management requirements. Got to have a policy and a program to address different subject areas. Outliers- are common to others, e.g. access controls. Policy can be simple what is important are the plans, woven together under management oversight.
- 003 umbrella standard- 4-9 addressing in more detail. Jumping off point for more detailed to follow.
- This standard is skeletal- areas management.
- Compartmentalized- to some degree will be necessary.
- Plans and programs- different disciplines use the same words- physical guys call things plan. What we mean is program and not a plan.
- If it doesn't lend itself to a plan.

B. Quick Update on Sub-Team Progress since Phoenix Meeting

The CIP 003-009 Sub-teams provided progress reports on work since the Phoenix meeting and then met in small groups until mid afternoon to draft or refine their requirements.

1. Change management.

- Areas- CIP 003 didn't fit into oox standard.

- Coordination- low/medium/high impact and connectivity- environmental differences? Didn't have many.

2. Access control and Auditing

- Sharon Edwards noted the excellent contributions of Jeff Hoffman and Frank Kim
- Got input from NERC
- Open issues- password measurements.
- Review what NERC offered.

3. Recovery and response.

- Scott noted good progress made and acknowledged Tom Stevenson's help and has reviewed Maureen's suggestions.

4. Operations

- Jay Cribb report that the Requirements are in good shape.
- Work needed on objectives and measures
- Coordination- ESP access points. Electronic Access Points- defined term – happy with

5. Personnel and Physical Security

- Doug Johnson reported that they have reviewed Maureen and/Dave's comments
- CIP 004. Get some policy statements over to Jon Stanford- addressing physical security and training and physical risk
- Do we still have an electronic security perimeter?
- What we have been doing- we have a word doc with a list of requirements. Get that into a real document.

C. CIP 003-009 Sub-Team Requirement Review

1. Governance

Jon Stanford presented the changes made to CIP 003 offering the following points:

- 003 can become 010
- Edited R1- adding the 9 subject areas (1.4- 1.12)
- R2- Each responsible entity shall implement the requirements specified in Table 1 (Subject Area XXX here)
- R3: Each responsible entity will implement the requirements specified in Table 2 (subject area xxx) in order to (benefit to the BES here)
- Can link VSLs to requirements

SDT Discussion

- NERC staff recommended retiring existing CIP standards and start afresh with CIP 10. Some cross e.g. vulnerability assessment is in 3 areas currently.

- Allows to quickly look through and make sure not requiring same thing in 4 requirements.
- We would need to explain- here's the map from the old and the new ones.
- Another benefit- requirement language will be simplified. As standards evolve- you'll modify the table not the policy making it more adaptable for future.
- Don't have to have a requirement that says "develop a plan"- avoiding circular logic.
- There is 1 requirement for each subject area? Will have own VRF? Everything in that Table will have the same VRF. Table will in essence- be the sub requirements.
- If we want to differentiate VRFs, we can develop multiple requirements.
- Implementation plan that will need to go along with this. If 1 standard. New implementation for a full standard.
- This will help out with the implementation plan.
- Version 4 and dates
- CIP 8 and 9. How would that be handled?
- CIP 8 with 4 Requirements and 4 tables would become 1 requirement and 1 table. Or use a group heading..
- We will need a new number strategy for interpretations.
- Need the SDT to determine what are the topics. Starting with 9 proposed by the Governance sub-team.
- Rolling each into a requirement. Reporting potential violation. Physical security violations (minor and major). Not sure this is the right way to go.
- There is precedent for lots of standards.
- Helps with granularity. We need to think about all implications.
- List of stuff that needs to be done will be the same. The granularity of the standards will be different.
- Need different frames of references- think about this overnight.
- Its important that the SDT makes sure we have the buckets right. Make sure they are chunked the right way. How it is organized will make a lot of differences.
- SDT should flesh out proposal among the Team. We need to agree on chunking. Get together and decide uniformly and collectively.
- This is a hard subject to get one's head around. Anything changes in format will be initially received as not necessarily simpler. Awareness and staff capacity is an issue in the industry. Practically consider starting what we have.
- Should there be a motion to stay with current CIP framework?
- WECC auditors have indicated that this would be easier with one caveat that tables would need to be numbered. Need a way to track that to the table.
- This does not represent a radical change. In fact, the H/M/L categorization is the radical change. Tables right now don't work. Need to find a way to present appropriately. This is about presentation of requirements.
- About 140 requirements in a single standard. Will violations of any requirement be a violation of standard? This raises repeat violations. Measures more complex and VSLs VRFs.

- Do we have the time to do it? Most of the other teams have requirements written. Significant re-writing will need to be done. Content of both the tables and requirements.
- This will be seen as a radical change in the industry.
- Could improve reporting. Violation of categories. Better reporting overall. E.g. personnel risk assessment. Create a better taxonomy.
- This is the appropriate time to propose the change and get it in front of the industry.
- Changes to software. It will get updated.
- Not lots of additional work. You take requirements. Put together in 1 document. Not a step back in reworking a lot of things. Most requirements are already in a table format.
- This could go faster for us and present a better governance model. Not making changes for no reason.
- What is there to debate if we stick with the current?
- This model is a vast improvement to what we have now. Might be well received by the industry. This team shouldn't concern itself about the vendors. Rather debate the merits of the ideas.
- This approach could help us in terms of consistency checking. Consistency is important. Advantages. Lots of organizational and process changes in the industry. Vendor software is the least of it. If not restating things in multiple places.
- Initially I like it. We have forever been defending one family of standards and we have viewed as 1 standard. We keep as one standard anyway.
- Messy now. Access control and monitoring asset. 5 line requirement. Makes a mess today to figure out what kind of asset is that.
- Many trade organizations are together. NERC CIP, Smart Grid standards coming out. Tracking on 800-53 model. Several doing efforts internally to map all requirements to such a model.
- Granularity for compliance- removing.
- Explained the proposed formats.- 9 topical areas. Policy
- One of the issues- compliance implications of doing that. Now between 8 and 150 requirements. Fewer # and granularity. Single VRF factor. Single V Severity levels . What would they do in terms of an investigation. How report to regions. Penalty calculation.
- Now with 41 requirements moving down to smaller number or having 150 requirements in single standard.
- Putting all standards into 1 document and consist of requirements and table.
- Consider all existing standards 3 -9 into one standard. Requirements have table associated with it.
- As auditors- take requirements and put into table format. Still looking at R and compliance with R. Having worked with military docs. Once you have anything that large and point back in terms of compliance. First time you updated. Move anything else up. From version to version.
- Keeping up to date or compliance tool- hassle in terms of bookkeeping and paperwork accurate.

- R language would be fairly vanilla- table could change. Have policy and procedures with the details.
- 2 action items. Categories need to be finalized and agreed to. Coalesce to action quicker.
- Tom Hoffsetter offered comments

Wednesday evening the Chair asked Howard Gugel to prepare a sample "proof of concept" for the access control requirements to inform a decision regarding format.

D. Review of the Sub-Team Products

Thursday afternoon the SDT reviewed each of the sub-team's draft requirements as revised and refined in the sub-team meetings on Wednesday, offering guidance on various issues raised by the draft requirements.

III. CIP FORMAT REVIEW

A. Tables in the Standard(s)

Howard Gugel, NERC, reviewed the changes regarding format, tables- (R3 referring to table 1). Editing tables. Propose for title to Table R __ helping to tie back.

SDT Comments

- Multiple Rs referring to the same table?
- Keep each table specific with each requirement.
- Bring back question of multiple references to the same table.
- CIP 6- one table and the column as the Rs. Different from the others.
- Need to be consistent for the format for all requirements. Use same format for other tables.
- Consider the guidance documents.
- Rows in table play role of bullet items under each requirement. Separate table links back to each requirement. Resolves issue of multiple rows references back to multiple requirements.
- Grouping the Tables at the end of the standard. Disjointed in a standard. Lot more readable and manageable. Sub requirements, as table entries.
- Similar to attachments in CIP 002. Idea of tables at end, keep requirements concise. Will pose to Maureen to get her opinion. Consistency better at the end.
- Look at Rs and make sure wording is consistent with other requirements.
- Looking at each R how you would measure it. Proof of that- light on this.
- Look at objective statements- read and make sense it is the purpose of the standards.

B. Objective Statements

SDT Comments

- Putting the objective within the requirement? Fraught with danger down the road.
- Enhancing reliability purpose clear.
- Reason it is there, who it applies to why needs to be done.
- Putting in requirement language- gets in the way. Defer that language until requirement language drafted.
- Get requirements first then measures.
- Defer the objectives as part of the requirement. Corollary document.
- If doesn't have a basis in reliability, shouldn't be a requirement.
- Format- R words. Designate.
- The objectives makes it harder to read.
- However it is important to have objective in there.
- Need to be specific about the benefits.
- For now, just bracket the objective.
- Part of the deliverable- measures, VSLs and requirements formats at the end of the session.
- Benefits for reliability? NERC could throw their proposal on each of them.
- Important to deal with measures- know when the requirement been met with. Tangible proof of requirement.

C. CIP Proof of Concept for Format- Access Control

1. Access Control and Auditing- Review for Format

Sharon Edwards presented the work to date on access control including 004 R4, 005 R2, 008 R5 and dispersed throughout the standard.

R1. Account Specifications (007 R 5) **Table**

- Beginning of table- policy should include the following: 20 points. Technical high level controls- H. M. at low- need to understand what they have. #15 "immediate revocation" of access. FERC expectations and SDT's belief of a reasonable starting point. The Sub-team had hard time with this.

Electronic Access Controls

- Sharon noted that this may be redundant.
- Box- "remote access"- Could develop a definition to the standard at hand.

Table R2- Electronic Access Controls

SDT Comments

- Need to decide which formatting for H/M/L.
- Outlier- information protection- document management.
- Measures as previously written- "make available documentation….."
- Haven't tackled VSLs and clean up work. Need sub-team time today.

- Split tables up into more tables? Is violation of one piece, violation of the whole requirement?
- Chunked up more? Good question for further discussion of the sub-team
- Tables provide an improvement and clarity- Keep concept of table. Share concern about multiple violation. Groupings of similar rows and make a separate requirement.
- E.g. Password- under own requirement. Reduces impact re multiple violations.
- Lot of value of tables but reduce the impact in terms of compliance.
- Break into more logical groups and individual requirements.
- Table not to consolidate all requirements. Table facilitates the breakdown of requirement points.
- Table looks good. Clarification. Separate document for audit and monitoring?
- Looked and most of audits related to things NERC would be doing. Didn't develop another table for auditing requirements.
- Row 13- Ports and Services- overlap with Change Management and Operations Security? Probably needs coordination.
- Doesn't specify the content of use restrictions? Is this an issue.
- Wireless approach- didn't want a comprehensive set of wireless standards. Other standards already done a good job. Trying to be less proscriptive. Down the road with encryption. We are not resourced to do.
- What does a blank in the table mean? Clarify if not required or something else.
- Communications aspect of this? Things that are not connected vs. routably connected. Did you intend to stay away from this?
- We did talk about this in the Sub-Team. Spent a lot of time discussing FERC directive to remove access. FERC didn't suggest anything to treat differently. Didn't go down road- may be others. Made decision.
- If talking about remote access, not remote access for user sessions outside of the USPN.
- Format: Required vs. analogue values in the rows. Larger number of individual similar requirements as long as each is a discreet, well worded.
- Breaking out. Barrier. Not having VSL correlated with requirements. Break up or chunk the topic areas – access control.
- When doing measures, have a table form? Matching those in requirement?
- Sub-Team used the generic measures.
- Let's make sure that the SDT knows the topics. E.g. "Security management controls"?
- Repeated wording. E.g. 11 "is required"
- We need a section where you address FERC directives. They had one directive (immediate) Make sure that we cover that for each of the sub-team. We don't need this posting.
- Authentication of un-manned devices. We will see more and more. Will this be covered someplace else? Should this be "human" access control. Do we need to say that?

D. CIP Format Review

1. Overview of Format Questions

On Thursday morning, Howard Gugel presented to the SDT a proof of concept for the access control requirements. He asked the SDT to look at format not merits of requirements in order to get a picture of how the requirements would be presented. He noted the table would be embedded in text and at the end of each requirement. NERC standards review staff agreed with this format approach. This would be the same regardless of which approach is chosen.

- **Option 1.** Keep 003-009 and work from there.
- **Option 2**: retire existing CIP standards and organized by the topics in sequence from 010 on. Access Control e.g. CIP 017.
- **Option 3:** One standards document with 2 sections 010 (002) and 011 (003-009). All controls together. R1 security policies addressing all topics
  - R2 implement per table
  - R3- table for access control
  - R4 implement 2nd table (account specifications).

Initial SDT Member Comments on Format

- Will 002 be on its own? Yes speaking of 003-009 together.
- Where are we capturing connectivity? 005.
- Connectivity is more important than big iron.
- 1st 5 LMH.
- Left column- allows item tracking
- Title Access Controls.
- It will not hard to make change if industry doesn't like this format,
- Language of the table can address connectivity.
- Industry confusion currently in terms of audits at the requirement level. Radical format change may not be well advised.
- Missing opportunity- keep simpler to scope out key things, like was discussed in Austin.
- Tables concept came out of the Phoenix meeting.
- Will FERC have a problem with the tables? There may be no process for reporting on that currently. Process will need to be addressed in this document.
- Common PCI and HIPPA common auditing format for standards.
- Read tables- allows flexibility of the columns. Reporting issue not an issue. Row number tracking will help.
- Table structure agreed to a couple meetings back. We are using them. Whether we keep groupings separate or have a single standard for this is the question. Culture of compliance- repeated violation of standards might be held against the industry with the single format.
- Will it be possible to write a VSL for this table format?

- Separate tables for requirements? E.g. account info and another with remote access issue. Past VSL at requirement level and where with sub requirements. This could end up with a lot of "ors"
- Break out the VSLs with the sub requirements in the table?
- Everything happens at the requirements.
- "Foolish consistency is the hobgoblin of small minds."
- When file with FERC it becomes law.
- Same issue with the VSLs- regardless of options.
- Can split the tables into more areas- can get as granular as the SDT wants.
- Put Rs on left column. Lose the R4 and number Rs. Use if /then construction.
- Now would be the time to propose this. Timing for this.
- Clarification on status quo. Decide on the buckets? We don't do buckets. Stay with 003-009.
- Do some reorganization what is in each standard and possible move- but keep in. Fix for Order 706.
- 003-009 numbering. Moving some Rs around. Tweaking re 706.
- The Team needs to make sure this works. Sees value in topical groupings but has concern with industry confusion. When CIP version 2 was put out the numbering changed and industry members asked why.
- Have a comment form question to get feedback. Makes sense from various standpoints. Ask how much confusion this cause confusion. In the comment form.
- Is there precedent in other reliability standards- if you are generator operator, if you have X, then.
- Limited. Lots based on functional model. Rs directed to different functional entities.
- What ever we do there are going to be changes in the industry. Better we do on our guidance, the better the industry will know what's going on. Need a strong foot forward on guidance.
- Option one- access control. Are they outliers. Easy to place those in a standard.
- Public Comment: Owner operator. Option 3 will be confusing. Is it the whole standard you must follow? CIP have 3-9. Too many changes together for industry to handle. Do option 1.
- Not proposing 4 options. Need to understand difference between 1 and 2 & 3. 2 and 3 carry new organizations. Current standards are supposed to be considered together. They are 1 standard. Change 1 must change all. They are buried and possibly scattered around in the current. New organization with different topical naming.
- Lot of thinking into organization of current standards. Big change is a new organization scheme
- Use tables with all of these options.
- Version 1, 2, 3 confusion- application. Version 4. Renumber standards. Option 2 less confusing.
- Radical change in the standard is required. Some equivalency 3-9 but the approach we are taking and the different formats. Would cause more confusion to use the same numbers. Start for new set 10- onward. Not to be confused with 3-9. Option 2 doesn't follow. It is a

different set of controls organized differently. Likes smaller groupings regarding compliance.

- Tom Hoffstetter noted that he doesn't speak for NERC but that organization in tables is good and he likes the break-out in terms of topics. Required columns will make it a lot clearer for both entity and auditor.
- If we go to option 3- collapse into 1 standards. 140 controls in one standard. Violation more than1 get a penalty.
- Whole different paradigm require a new approach as to how penalties assess. Approach different in many ways. Wouldn't try to make current structure fit. Have to depart from traditional approach to penalties. Have to describe them differently and assess in a different format. Across the board.
- Nothing to argue with what TH said. These standards will be balloted and posted and implemented under the current process.
- Option 3 recognizes how tightly knit these are together.
- This may not matter in the end. Push in his company.
- Can NERC help with this issue that RK brought up? What is the audit standpoint. Can they do this. Might help to present options 2 and 3 at the Technical Workshop. Show how NERC and auditors of regional areas would handle. How models would be handled in audit and penalties.
- Option 3- organization within? Still the same? Structured as per 1 or 2?
- Constrained by current compliance structure. Could we propose a new approach? Put out standards with a proposed structure?
- Confined now to VSR VSL structure.

2. Initial Preference Ranking of Options and Voting for the Preferred Format Option

The Team following the discussion of the pros/cons of the options, voted first on each of the three options indicating its acceptability. Following that each Team member voted to support the option they found most acceptable or preferable based on the discussion and their perspective.

Format Option 1: keep existing CIP 003 to 009 in its current form maintaining its existing logical construct (may involve minor movement of existing requirements between standards)

Yes	*No*	*Indifferent/could go either way*
8	**7**	**3**

Format Option 2: Retire 003 to 009, create new CIP 010-16 grouping according to small group assignments.

Yes	*No*	*Indifferent/could go either way*
12	**2**	**6**

Format Option 3: Collapse CIP 003-009 into a single standard that contains all requirements created/edits by small groups and grouped according to small group assignments.

Yes	*No*	*Indifferent/could go either way*
12	**7**	**2**

The team then voted for one of the two highest ranked options under consideration:

- Option 2: Retire 003 to 009, create new CIP 010-16 grouping according to small group assignments. ***Yes*=6**
- Option 3 Collapse CIP 003-009 into a single standard that contains all requirements created/edits by small groups and grouped according to small group assignments. ***Yes*=10**
- *Abstained from voting for Option #2 or #3:* 4

Comments on the Options Ranking and Next Steps for the Sub-Teams

- Need to take into account the industry's reactions.
- Don't see any real difference between option 2 and 3.
- Not a single requirement vs. standard.
- It is different in terms of what is presented. Violation of any requirements may present problems.
- This is just an organization issue.
- What are the expectations for Sub-teams in terms of drafting VSLs?
- Allowed to have content- for each row of your table a VSL statement in that format.
- Finish up writing requirements. We can pull back together into multiple standards or into one standards following a decision.
- Would be helpful to go through one of the sub-team's reports before breaking. Substance requirements, measures and VSLs.
- Missing several definitions. Should we use boxes? Indicate it is guidance. If not, it will be exported to glossary, or in requirement.
- Note if put in guidance then not part of standard. If it goes out without guidance document. Comments won't be complete.
- As a reality check, take access control and go through it and reframe expectations. Going to need work after going out for informal comment. Interim work product posting. Work as hard. Focus on requirements.
- Some sub-teams are using different definitions for external connectivity. Factor into what is put in the rows on table. Each needs to do the walk through.
- Five remaining areas that need SDT guidance for sub-teams.
  - Square box definitions- specific to standards (vegetation management standard precedent
  - Control centers definition
  - Different types of communications
  - How should the sub-team address drafting measures or consider putting out document for industry review without measures

  - Address VSLs or consider putting out document for industry review without measures
- SDT should clarify outliers- definitions. Whose will be used? When will see all the definitions in the various document?
- Governance section, based on SDT input pulling policy statements up.
- Suggest that a SAR for a drafting team be considered. Address FERC 706 items that may be outside the scope of drafting team, e.g. NIST risk management framework.
- 9 Categories of proposals to organize. Put the level of controls in right hand columns or separate rows.
- Option 1. Allows different time frames. Separate line items for medium. Time frames in columns. Bulleted lists time frames.

3. Reviewing and Ranking Option 2 (2nd Round)

At the end of the day the Team took up the format issue again. The Vice Chair made a proposal that the Team use Option 2 (which would renumber the requirements using the topics to organize them. The Team discussed this option:

- Consider renumbering 002 as 010 – confusing to have 002 then renumber at 010
- Posted previously as 002, proposed keeping then renumbering new.
- Yes, different titles for the same thing that exist with a few split out.
- Some match what we have now, some are new – where we can group into the existing CIP we could do so and renumber only the new ones.
- Is media protection now media disposal? Where would you move information protection?
- How many teams work on multiple standards at the same time? Yes, others teams do address more than one but not ten of them
- The titles may seem the same but many of the sub-parts have been moved around except for 002 which is still focused on the same topic area – we would need to educate the industry on what is in each standard.
- Rename the last item 021 as Boundary protection rather than data communications?
- Will we map old standards into the new ones? If so, why not retain some of the old numbers
- Did not gain consensus on this earlier – this seems ad hoc.
- We probably need to agree on something today in order to to put this into a format.
- Propose altering proposal to start with 010 for old 002 – new numbers for all of them – less confusing
- Access control needs to be separated into physical and electronic.
- Under personnel and training – would that include training for all the other standards?
- Idea is to combine training and awareness and risk assessment.
- Change name of the last one and make electronic access protection or role into new 013 under system security?
- Heartache at pulling physical access control out as separate item.
- May still need further renaming or organization as we move forward.

- We have to write the standards so we are not assuming IT security and physical security will be handled by the same people
- Physical security and access control – IT controls access to server but not the badging for physical security –
- Need to go with this not as a concept but as framework – it is a format

The facilitators polled the team on their support for the option #2 (multiple standards) and 7 of 16 members were in support of utilizing this as the format.

An additional member joined and the Team then tested support for Option 3 (putting all into single standard) and 9 of 17 supported using this format. Neither format approach received sufficient support to make an SDT decision.

4. Numbering the Requirements

The Team them reviewed and tested support for each of the following propositions:

- **Change from existing CIP numbering system?** Yes- 13 favor changing (of 17 = 76%)

SDT Comments

- Adopting the headings would be the same under multiple numbers or as one
- If we keep CIP 002 as 002 for continuity then the rest are renumbered or just one,
- would be more confusing
- change to Option 2 if we revote but concerned this is under duress
- Think we need just one standard

5. Adopting Category Headings for Requirements

- **Adopt the proposed headings for the requirements as the categories whether as one or multiple standards** – Yes-13 (of 17 = 76%)

After further Team discussion it was determined that there was no longer a quorum and the Chair suggested postponing further discussion until Friday morning.

6. Final Review of Format Options

On Friday morning the SDT took up the final review of format options for the informal posting document(s) in order to make a decision.

The facilitator suggested the SDT use an acceptability ranking of the two possible format options that had been discussed and debated yesterday followed by clarification of concerns to see if they could be met and a requisite number of members could agree on the format to use for the informal posting.

He reviewed the scale to be used as: 4= fine as is, 3= support but have questions, 2= need to address concerns before I can support, or 1= cannot support. The SDT then ranked each option and those providing a 2 or 1 offered what their concern was.

Option #2 – Requirements in Multiple Standards

- Use the Topical areas discussed on Thursday and utilize multiple standards (example CIP 010 -020). CIP 002 also gets re-numbered.

4-3 3=7 2-6 1-0 (Avg. 2.81)

Option #2 Concerns

- All the standards have a single purpose and are meant to be viewed as one. Should be one for clarity.
- Efficiency of one (better implementation) - Don't like fragmentation between multiple standards.
- Much cleaner to have just one standard
- Current standards say to consider as one but in fact they are not treated that way thus making compliance difficult.
- There is a greater chance for double jeopardy. Easier to manage with Option 3 in a single standard format. Fragmentation leads to fragmented implementation rather than unified management.
- We do talk about the CIP standards as one but in practice they are treated differently.
- I like the grouping or headings but multiple standards looks like we are asking them to do more - also additional documentation
- If we post additional standards, the reaction of industry will be that we are asking them to do more. Having only one standard will reduce required documentation. Eventually multiple standards would be on different version levels, thus adding to confusion.

Option #3 – Requirements all in One Standard

Use the Topical areas discussed on Thursday, but one new standard is posted containing sections for.

4=6 3=5 2=3 1=2 (Avg. 2.93)

Option #3 Concerns

- Compliance implications - violating one standard even if different requirements- significant increased risk for multiple violations of one standard.
- Need to hear technical argument to support 3
- Compliance issue- non-compliance on low items makes you vulnerable to citations for repeat finding of non-compliance
- Compliance my main concern- tie our hands about splitting later- once merged cannot deal with future revisions separately
- Just trying to format for posting

- Concerned about complexity- more than value of unified
- Voted a 1 because of the number of requirements and sub-requirements. There are about 120 major requirements plus sub requirements. The 140 plus requirements may means that any violation of any of these requirements you are in violation of one standard. Compliance reporting and compliance sanction issue on the issue of multiple violation of the standard.
- When RSAW's are prepared, the SME should only view information pertinent to his area of expertise.
- Agree with concern about repeat violations of the same standard.
- Can the compliance situation could be fixed if the structure of the way NERC viewed the standards for sanctions, etc. were changed? However, that will not change.
- Is it likely that NERC would change the way they viewed compliance to support Option 3?
- Concern with the sheer complexity of the one standard. Also see disadvantages of the lack of a unified approach, but there have also been advantages in the divide and conquer approach.

SDT Options Discussion following the Ranking

- Fragmentation of the standards will contribute to lack of a unified management and implementation.
- Sometimes the only change in a standard is the change in the standard number. This makes no sense. If you look at the categories we approved yesterday, there will be tighter integration between the CIP standards. If we have separate standards, we need to make sure each can stand alone.
- Prefers the unified standard and believes that we can help the complexity by making them one. The big concern is the regulatory impact mentioned by others.
- The Current standards do not lend themselves to good organized implementation. The new adopted topic areas are the most important thing to consider. Can both options be presented to the industry for feedback?
- The facilitator asked NERC staff is we need one or the other for the posting?
- Scott Mix noted that raw work papers will not be sufficient for the posting. Presentation in two formats will likely confuse the industry. Perhaps the posting could be presented in one format, but we explain the other format and ask the industry to comment on whether they like the change or not.
- Scott Mix showed the Team the NERC generated report does show total violations by standard.
- Howard Gugel submitted the enforcement question to Joel DeJesus at NERC concerning compliance concerns. Is there a compounding effect? A: If there are multiple impacts of multiple violations of the same standard, there may be some compounding effect. If R3, R12, and R22 were violated, they would be separate violations with no compounding effect.

- The concern is the "culture of compliance" at NERC and FERC. If the same standard is violated, it will have the consequence of doubting the culture of compliance.
- If we get one single standard that has magnitudes of violations, it will send the wrong message and numbers of violations will be noticed.
- In terms in the ability to observe, Scott Mix suggested he did not see the difference.
- All the reports to the member committees are by standard number and he believes there will be a spike if all CIP is one standard.
- Legislators are aware of the collections of standards that the industry must deal with. For example FISMA is a collection they are familiar with.
- We need a decision. We spent too much time discussing this. We have agreed on the categories. Let's get something out there. We are wasting too much time.
- We could debate this all day, but we need to move forward.
- If we step away from CIP and started talking about vegetation management, he believes breaking the standard into multiple would not make sense.
- Lawmakers and congress will understand and support that while there are multiple topics, there is still one framework for improving cyber security implementation.
- Do we need a transition before moving dramatically to either new set?
- These categories make it hard to divide responsibility.
- Think new categories provide better organization and will improve implementation.
- Can we put out both as two separate documents?
- That may be too confusing to address option with questions in comment form
- Need to be accountable.
- We need to put a question to the NERC enforcement side. Can we go with this and limit compounding violations?
- Concerned about potential impact on Congress if there is a spike in non-compliance because multiple violations of one standard.
- Congress is most concerned about fragmentation and used to looking at one standard for an industry.
- The facilitator asked if any concerns addressed that would move their vote from a 3 or 4?
- Some members expressed concerns about suspending rules- changing the game. Needs to be a yes/no choice
- Concerned adding in "either" result in super majority for both options - then what?
- Is there an alternative embedded in the decision rules for this post for informal comment? Can the SDT use a majority (50%+) for purpose of posting using single standard or multiple standards and documenting the SDT differences in comment form for either choice.

The 17 SDT members present then voted for their preference for posting for informal comment between the two options with the following result:

Option #2 (multiple standards) **Yes = 6 (35%)**

Option #3 (single standard) **Yes = 11 (65%)**

The SDT agreed that while this decision to post for informal comment has a majority support (65%) but not the super majority (75%) of the members called for in the decision rules, the Team is asking for industry comment and input on the formats through comment form before finalizing a format to present in the formal comment draft in July, 2010. The Team discussed that this approach is consistent with the spirit of the following consensus rule provision: "In instances where the Team finds that even 75% acceptance or support is not achievable, the Team's report will include documentation of any differences as well as the options that were considered for which there was greater than 50% support from the Team."

IV. NEXT STEPS AND ASSIGNMENTS

On Friday the Chair reviewed the schedule, assignments and next steps for the SDT to produce a final version for posting on May 3, 2010. Joe Bucciero will lead with assistance from Howard Gugel the drafting of comment form with information provided by each of the team leads and will also add a question from discussion of the format to document discussion

The SDT will need to begin creating an implementation plan for posting in July for formal comment with a small group of SDT members in order to provide some frame for discussion at the May meeting and to answer any questions at the May workshop in Dallas. Scott Mix will be looking for individuals to work with – this will occur after May 3.

We need something in cover letter for May 3 posting that speaks to the SDT's philosophy on implementing the plan – industry needs to understand what we are doing. Need a couple paragraphs explaining our approach or intent Jackie Collett, John Lim and Doug Johnson agreed to work with Scott Mix on developing a draft implementation plan.

The Chair reviewed the schedule from April 19, Monday to posting on May 3, Monday. It was agreed the sub-teams need to complete their drafting and get these to Howard to put into "standard" for review by NERC staff. The plan will be to assimilate the NERC comments with team leads, then late in last week of April have a ready-talk and email vote for approval to post on May 3. Have conference call on April 26 for team leads and 29th for ready-talk review with full team Each Sub-team lead will seek to get work done and to Howard Gugel by Monday morning then review with Howard and team leads on Tuesday afternoon. The following schedule was reviewed and approved by the SDT:

- 19th by 5:00 – requirements, measures, vsl's and glossary drafts to Howard
- 20th Sub-team leads with Howard at 3:00 – 6:00 EST

- 21st Howard will get team drafts to NERC staff for review
- 27th full day (10-5) meeting with NERC staff with Sub-team leads and anyone else who wants to join (NERC comments back by 26th if possible to full team – concern is legal and compliance) – updated version send out on 28th to full team for review
- 29th full team meeting (1 to 4) for review and vote to post

The Chair and Vice Chair and the SDT thanked Jay Cribb for his excellent hosting and great facilities.
The meeting adjourned at 12:00 p.m.

Appendix # 1— Meeting Agenda
Project 2008-06 Cyber Security Order 706 SDT
Draft 20th Meeting Agenda
April 13, 2010, Tuesday- 1 PM to 5:30 PM EST
April 14, 2010 Wednesday- 8 AM to 6:15 PM EST
April 15, 2010 Thursday- 8 AM to 5 PM EST
April 16, 2010 Friday- 8 AM to 12 PM EST
Georgia Power
241 Ralph McGill Blvd
Atlanta, GA 30308
NOTE:
1. Agenda Times May be Adjusted as Needed during the Meeting
2. Drafting Team Meetings May Not Have Access to Telephones and Ready Talk

Proposed Meeting Objectives/Outcomes

- Review the revised CSO 706 SDT 2010 Work plan and Schedule
- Receive updates on other related cyber security initiatives
- Receive a NERC update on implementing the CIP Communication Plan and the May 2010 Technical Workshop
- Review, refine and adopt the Draft Final CIP-002-4 for industry informal comment
- Review, refine and adopt the Sub-Team Security Control Requirements draft for industry informal comment
- Develop related CIP 002 and Security Controls Requirements Guidance Documents
- Agree on next steps and assignments

Draft Agenda

Tuesday **April 13, 2009**
1:00 p.m. Welcome and Opening Remarks- *John Lim, Chair & Phil Huff, Vice Chair*

	Roll Call; NERC Antitrust Compliance Guidelines Facilitator review and SDT acceptance of March 9-12, 2010 Phoenix SDT meeting summary
1:10	Review of Meeting Objectives, Agenda and Meeting Guidelines- *Bob Jones*
1:15	Review and Discussion of CSO 706 SDT Workplan and Schedule - March-December, 2010- *Stu Langton*
1:45	Updates on other related cyber security initiatives- *NERC Staff and SDT Members*
1:55	Update on CIP Communication Plan and May 2010 Technical Workshop - *Carl Dombek*
2:15	Overview of Single Text- CIP-002-4 & Security Controls Requirements
2:45	*Break*
3:00	Review of Revised CIP-002-4 Draft Final and SDT Industry Response Document- *CIP-002-4 Drafting Team, John Lim et al.*
3:30	Full Team Consensus Testing on Refinements of draft final CIP 002-4
5:25	Review of Proposal for Wednesday Agenda
5:30	*Recess* ▪ *Possible Security Controls Requirements Sub Team Meetings- Evening* ▪ *If needed, CIP-002 Drafting Team to meet to finalize draft and present for adoption Wednesday morning.*

Wednesday	**April 14, 2010**
8:00	Welcome and Agenda Review, Roll Call and Antitrust Guidelines- *John Lim, Phil Huff, Joe Bucierro*
8:10	Final Review of CIP-002-4 as revised
9:00	Security Governance Requirements- Overview and Consensus Testing
10:30	Break
10:45	Personnel and Physical Security Requirements and Guidance- Overview and Consensus Testing
12:15	Working Lunch
1:00	Operations Security Requirements and Guidance - Overview and Consensus Testing
2:30	Break
2:45	Recovery and Response Requirements- Overview and Consensus Testing
3:45	Access Control and Auditing- Requirements- Overview and Consensus Testing
5:00	Change Management, System Lifecycle and Information Management- Requirements- Overview and Consensus Testing
6:15	*Recess* ▪ *Possible Security Controls Requirements Sub Team Meetings- Evening*

Thursday	**April 15, 2010**
8:00	Welcome and Agenda Review, Roll Call and Antitrust Guidelines- *John Lim, Phil Huff, Joe Bucierro*
8:10	Security Controls Sub-Teams Refinement Sessions
10:00	Break
10:15	Security Controls Sub-Teams Refinement Sessions
12:00	*Working Lunch*

1:00	Full Team Review and Consensus Testing on Final Draft
3:00	Break
3:15	Full Team Consensus Testing on Refinements-*Continued*
4:15	Motion to Adopt in Concept Draft CIP 002 and Security Controls Requirements for Informal Comment Posting Review Any Drafting Assignments and Friday Agenda
5:00	*Recess* ▪ *As needed ad-hoc drafting groups- Evening*

Friday	**April 16, 2010**
8:00	Welcome and Agenda Review, Roll Call and Antitrust Guidelines- *John Lim, Phil Huff, Joe Bucierro*
8:10	Sub-Team Development of Guidance Documents
10:15	*Break*
10:30	SDT Review and Suggested Refinement of CIP Guidance Documents
11:15	Review of May 2010 Technical Workshop Planning and Preparation
11:45	Review of Dallas Agenda and Agree on Next Steps and Meeting Evaluation
12:00	*Adjourn & Lunch*

Appendix # 2 Attendees List
March 9-12, 2010, Phoenix, Arizona

Attending in Person — SDT Members and Staff

1. Rob Antonishen	Ontario Power Generation
2. Jim Brenton	ERCOT (T/W/Th)
3. Jay S. Cribb	Southern Company Services
4. Sharon Edwards	Duke Energy
5. Jeff Hoffman	U.S. Bureau of Reclamation, Denver
6. Gerald S. Freese	America Electric Pwr. (T/W/Th)
7. Phillip Huff, Vice Chair	Arkansas Electric Coop Corporation
8. Doug Johnson	Exelon Corporation – Commonwealth Edison
9. Frank Kim	Hydro One Networks Inc. (T/W/Th)
10. Rich Kinas	Orlando Utilities Commission (Th/F)
12. John Lim, Chair	Consolidated Edison Co. NY
13. David Norton	Entergy (T/W/Th)
14. David S. Revill	Georgia Transmission Corporation
15. Scott Rosenberger	Luminant Energy (T/W/Th)
16. Jonathan Stanford	Bonneville Power Administration
17.Tom Stevenson	Constellation
18.Keith Stouffer	National Institute of Standards & Technology (T/W/Th)
19. John Van Boxtel	WECC
20. John D. Varnell	Technology Director, Tenaska Power Services Co.
21. William Winters	Arizona Public Service, Inc.
Scott Mix	NERC
Howard Gugel	NERC
Joe Bucciero	NERC/Bucciero Consulting, LLC
Robert Jones	FSU/FCRC Consensus Center
Hal Beardal	FSU/FCRC Consensus Center
Stuart Langton	FSU/FCRC Consensus Center
Tom Hoffstetter	NERC (Thurs a.m. by phone)

SDT Members Attending via ReadyTalk and Phone

22. Jackie Collett	Manitoba Hydro
23. Patricio Leon	Southern California Edison (T/W/Th)
24. Kevin Sherlin	Sacramento Municipal Utility District (Th)

SDT Members Not Participating

Joe Doetzl	Kansas City Pwr. & Light Co

Others Attending in Person

Jim Fletcher	AEP
Brian Newell	AEP
Bryn Wilson	OGE
Clyde Poole	TDITX
Rod Hardiman	Southern Company
Elizabeth Moses	Georgia Transmission
Jason Marshall	Midwest ISO

Others Attending via WebEx and Phone

Andres	Lopez	andres.lopez@usace.army.com
Justin	Kelly	FERC
John	Fridye	jfridye@rrienergy.com
Steve	Newman	srnewman@midamerican.com
Maggy	Powell	margaret.powell@constellation.com
Bill	Keagle	william.a.keagle.jr@constellation.com
Steve	Newman	srnewman@midamerican.com
Jerome	Farquharson	jfarquharson@burnsmcd.com

Appendix # 3 — NERC Antitrust Compliance Guidelines

I. General

It is NERC's policy and practice to obey the antitrust laws and to avoid all conduct that unreasonably restrains competition. This policy requires the avoidance of any conduct that
violates, or that might appear to violate, the antitrust laws. Among other things, the antitrust laws forbid any agreement between or among competitors regarding prices, availability of service, product design, terms of sale, division of markets, allocation of customers or any other activity that unreasonably restrains competition.

It is the responsibility of every NERC participant and employee who may in any way affect
NERC's compliance with the antitrust laws to carry out this commitment.

Antitrust laws are complex and subject to court interpretation that can vary over time and from one court to another. The purpose of these guidelines is to alert NERC participants and employees to potential antitrust problems and to set forth policies to be followed with respect to activities that may involve antitrust considerations. In some instances, the NERC policy contained in these guidelines is stricter than the applicable antitrust laws. Any NERC participant or employee who is uncertain about the legal ramifications of a particular course of conduct or who has doubts or concerns about whether NERC's antitrust compliance policy is implicated in any situation should consult NERC's General Counsel immediately.

II. Prohibited Activities

Participants in NERC activities (including those of its committees and Sub-groups) should refrain from the following when acting in their capacity as participants in NERC activities (e.g., at NERC meetings, conference calls and in informal discussions):

- Discussions involving pricing information, especially margin (profit) and internal cost
- information and participants' expectations as to their future prices or internal costs.
- Discussions of a participant's marketing strategies.
- Discussions regarding how customers and geographical areas are to be divided among competitors.
- Discussions concerning the exclusion of competitors from markets.

- Discussions concerning boycotting or group refusals to deal with competitors, vendors or suppliers.

III. Activities That Are Permitted

From time to time decisions or actions of NERC (including those of its committees and Sub-groups) may have a negative impact on particular entities and thus in that sense adversely
impact competition. Decisions and actions by NERC (including its committees and Sub-groups) should only be undertaken for the purpose of promoting and maintaining the reliability and adequacy of the bulk power system. If you do not have a legitimate purpose consistent with this objective for discussing a matter, please refrain from discussing the matter during NERC meetings and in other NERC-related communications.

You should also ensure that NERC procedures, including those set forth in NERC's Certificate of Incorporation and Bylaws are followed in conducting NERC business. Other NERC procedures that may be applicable to a particular NERC activity include the following:

- Reliability Standards Process Manual
- Organization and Procedures Manual for the NERC Standing Committees
- System Operator Certification Program

In addition, all discussions in NERC meetings and other NERC-related communications should be within the scope of the mandate for or assignment to the particular NERC committee or Sub-group, as well as within the scope of the published agenda for the meeting.

No decisions should be made nor any actions taken in NERC activities for the purpose of giving an industry participant or group of participants a competitive advantage over other participants. In particular, decisions with respect to setting, revising, or assessing compliance with NERC reliability standards should not be influenced by anti-competitive motivations.

Subject to the foregoing restrictions, participants in NERC activities may discuss:

- Reliability matters relating to the bulk power system, including operation and planning matters such as establishing or revising reliability standards, special operating procedures, operating transfer capabilities, and plans for new facilities.
- Matters relating to the impact of reliability standards for the bulk power system on

- electricity markets, and the impact of electricity market operations on the reliability of the bulk power system.
- Proposed filings or other communications with state or federal regulatory authorities or other governmental entities.
- Matters relating to the internal governance, management and operation of NERC, such as nominations for vacant committee positions, budgeting and assessments, and
- employment matters; and procedural matters such as planning and scheduling meetings.

Any other matters that do not clearly fall within these guidelines should be reviewed with NERC's General Counsel before being discussed.

APPENDIX # 4
CSO 706 SDT MEETING SCHEDULE
APRIL –DECEMBER 2010

Schedule Convergence: Full CIP V4 Package		
Date	**Week of**	**CIP Task**
SDT Meeting-Atlanta, (4/13-16)	4/12/2010	**Present Controls draft for full team review and comment. Sub team drafting. Finalize draft for Informal Comment, Full Package**
	4/19/2010	**NERC Prepares Full Package for Industry Comment**
	4/26/2010	**SDT Reviews and Approved Full Package for 30-day Industry Comment Period**
5/3/2010	5/3/2010	***Informal Comment Posting for full package starts Completes on 6/2/2010***
SDT Meeting-Dallas, (5/11-14)	5/10/2010	**Prepare for Industry Workshop**
5/19 & 5/20/2010	5/17/2010	**1.5-day Industry Technical Workshop (Dallas, TX)**
	5/24/2010	**SDT Considers Comments from Workshop**
6/4/2010	*5/31/2010*	***2nd Informal comment period ends***
6/2/2010		***Comment Period Ends***
6/3-6/4/2010		***SDT Summarizes Comments Received***
SDT Meeting, Sacramento (6/8-11)	6/7/2010	**SDT Meeting: Comment review, response process, re-drafting, as needed**
	6/14/2010	Sub team meetings
	6/21/2010	Sub team meetings
6/29/2010	6/28/2010	Sub team meetings. SDT interim online meeting.
	7/5/2010	Subteams Package modifications into Standard documents
SDT Meeting, Pittsburgh, (7/13-16)	7/12/2010	**Finalize & Approve Documents for posting for 45 day formal comment period**

Schedule Convergence: Full CIP V4 Package		
Date	**Week of**	**CIP Task**
	7/19/2010	***NERC Prepares Materials/SDT Approves Revisions/NERC Seeks SC Approval for Ballot***
7/26/2010	7/26/2010	***45 Day formal comment period starts (completes 9/8/10) /Ballot Pool formation (completes 8/25/10)***
	8/2/2010	**Industry Comments on Standards**
SDT Meeting, TBD, (8/10-13)	8/9/2010	**SDT Meeting: Prepare for Industry Webinar**
8/18/10	*8/16/2010*	***Hold Industry Webinar***
8/25/2010	8/23/2010	***30 Ballot Preview/Initial Comment Preview ends/Ballot Pool formed***
8/30/2010	*8/30/2010*	***Initial Ballot Starts***
SDT Meeting Winnipeg, (9/7-10)	9/6/2010	**Respond to comments received. Drafting revisions. Review Ballot Results and Additional Comments**
	9/8/2010	**Initial Ballot Ends**
	9/13/2010	Sub team meetings
9/24/10	9/20/2010	Sub team meetings; Full SDT on-line meeting to adopt revised draft of documents
	9/27/2010	NERC Staff Review of Documents and SDT Approval for Re-ballot
10/4 to 10/13/10	10/4/2010	Re-Ballot Period Begins
SDT Meeting TBD, (10/12-15)	10/11/2010	**Prepare responses to 2nd ballot comments**
10/19/2010	*10/18/2010*	***Sub-teams meet to adjust requirements***
10/29/2010	10/25/2010	***Prepare & Finalize revisions to standards and responses to comments on standards***
	11/1/2010	NERC Staff Review of Documents and SDT Approval for Re-ballot
11/8 to 11/17/2010	11/8/2010	3rd Ballot Period Begins

Schedule Convergence: Full CIP V4 Package		
Date	**Week of**	**CIP Task**
SDT Meeting TBD, (11/16-19)	11/15/2010	**Prepare responses to 3rd Ballot comments**
	11/22/2010	*NERC & SDT finalize responses to ballot package*
	11/29/2010	*Seek SC & BOT Approval for Filing*
	12/6/2010	*Seek SC & BOT Approval for Filing*
SDT Meeting TBD, (12/13-17)	12/13/2010	**SDT Meeting to review Filing and Celebrate Project Completion**
	12/24/2010	*Submit for Regulatory Approval*

Appendix #5

CSO 706 SDT DRAFTING SUB-TEAMS

Sub-Team	NERC Standards and DHS Control Families	Team Members
Security Governance	CIP-003 – R1, R2, R3; CIP-005 R4, CIP-007 R8 DHS 2.1 Security Policy, DHS 2.2 Organizational Security, DHS 2.7 Strategic Planning, DHS 2.17 Monitoring and Reviewing Control System Security Policy, DHS 2.18 Risk Management and Assessment, DHS 2.19 Security Program Management	Jon Stanford (Lead), Jerry Freese, Dave Norton
CIP 002-4	Draft revisions to CIP-002-4, and Summary of Responses to Industry comments	John Lim, Dave Revill, Rich Kinas, Jim Brenton, Jackie Collett, Bill Winters, Dave Norton *Rod Hardiman (Observer)*
Personnel and Physical Security	CIP-004 – R1, R2, R3, CIP-006 R1 through R6 DHS 2.3 Personnel Security, DHS 2.11 Security Awareness and Training DHS 2.4 Physical and Environmental Security,	Doug Johnson (Lead), Rob Antonishen, Patrick Leon, Kevin Sherlin
Operations Security	CIP-005 R1, R3 CIP-007 R2, R3, R4, R6 DHS 2.8 System and Communication Protection DHS 2.14 System and Information Integrity	Jay Cribb (Lead), Jim Brenton, Jackie Collette, John Varnell
Recovery and Response	CIP-008 R1 & R2 CIP-009 R1 through R5 Incidence Response and Contingency Planning	Scott Rosenberger (Lead), Joe Doetzl, *Observer Participants: Jason Marshall*
Access Control and Auditing	CIP-003 R5; CIP-005 R2; CIP-007 R5; CIP 004 R4 DHS 2.15 Access Control DHS 2.16 Audit and Accountability	Sharon Edwards (Lead), Jeff Hoffman, Frank Kim *Observer Participants: Sam Merrell*
Change Management, System Lifecycle and Information Management	CIP-003 R6; CIP-007 R1, R7 CIP-003 R4; CIP-005 R5.1.1, R5.1.3 DHS 2.5 System and Services Acquisition, DHS 2.6 Configuration Management and System Lifecycle, DHS 2.10 System Development and Mainten. DHS 2.9 Information and Document Mgt. DHS 2.13 Media Protection	Keith Stouffer, Phil Huff (Lead) *Observer Participants: John Fridye*

Security Controls Sub-Team Principles and Drafting Guidance

CSO 706 SDT SECURITY CONTROLS SUB-TEAM DRAFTING PRINCIPLES

(ADOPTED BY CSO 706 SDT, JANUARY, 2010)

1. Applicability [NERC ROP] Each reliability standard shall clearly identify the functional classes of entities responsible for complying with the reliability standard, with any specific additions or exceptions noted.	**9.Practicality** [NERC ROP] – Each reliability standard shall establish requirements that can be practically implemented by the assigned responsible entities within the specified effective date and thereafter.
2.Reliabiliy Objective [NERC ROP] Each reliability standard shall have a clear statement of purpose that shall describe how the standard contributes to the reliability of the bulk power system.	**10. Consistent Terminology** [NERC ROP] To the extent possible, reliability standards shall use a set of standard terms and definitions that are approved through the NERC reliability standards development process.
3.Performance Requirement or Outcome (NERC ROP) Each reliability standard shall state one or more performance requirements, which if achieved by the applicable entities, will provide for a reliable bulk power system, consistent with good utility practices and the public interest.	**11. Commensurate Controls for BES Impact Categories.** Security controls shall be commensurate with the identified level of BES impact categories.
4. Measurability (ROP) Each performance requirement shall be stated so as to be objectively measurable by a third party with knowledge or expertise in the area addressed by that requirement.	**12. Change Documentation.** Changes from prior versions of CIP Standards have clear rationale. These include the following types of changes: a. Above and beyond the current standards; b. Removal of requirements; and c. Major formatting changes.
5.Technical Basis in Engineering and Operations [NERC ROP] Each reliability standard shall be based upon sound engineering and operating judgment, analysis, or experience, as determined by expert practitioners in that particular field.	**13. Reduce Administrative Overhead**. Administrative documentation shall be kept to the minimum that is necessary
6. Completeness (NERC ROP) Reliability standards shall be complete and self-contained. The standards shall not depend on external information to determine the required level of performance.	**14. Priority.** Implementation plans for the Standards are prioritized according to level of BES impact.
7. Consequences for Non-Compliance [NERC ROP] In combination with guidelines for penalties and sanctions, as well as other ERO and regional entity compliance documents, the consequences of violating a standard are clearly presented to the entities responsible for complying with the standards.	**15. Eliminate or Minimize TFEs.** Security controls shall eliminate or at least minimize the need for TFEs. Allow for compensating controls to mitigate the need for a TFE.
8. Clear Language [NERC ROP] – Each reliability standard shall be stated using clear and unambiguous language. Responsible entities, using reasonable judgment and in keeping with good utility practices, are able to arrive at a consistent interpretation of the required performance.	

SECURITY CONTROLS SUB-TEAM
PROCESS AND DRAFTING GUIDANCE AND DELIVERABLES

Guidance from the January, 2010 Tucker Meeting and the February 2010 Austin Meeting

For the purpose of maintaining consistency across the teams and capturing interim decisions and change documentation, each team should utilize the following development process:

1. **DHS Catalogue of Controls:** Begin by identifying applicable controls that are enumerated in the *DHS Catalog of Control System Security Recommendations* for High Impact Cyber Systems.
2. **Cross Reference CIP Version 3 Requirements/sub-Requirements:** For each security control identified in step 1, cross reference the CIP version 3 Requirement/sub-Requirement or validate previous mapping work.
3. **Specific not Prescriptive:** As a general rule, be specific but not prescriptive in writing the requirements.
4. **"What" not "How":** In general, seek to draft a "what" requirements, not "how" requirements.
5. **Develop the requirement language** for each security control identified in step 1.
   a. When mapping to existing CIP requirements, use language from CIP, making improvements where needed.
   b. When no associated requirement from CIP exists, develop the new requirement using language from the *DHS Catalog*.
6. **Document significant changes to CIP Standards:** Document significant changes made to previous versions of the CIP Standards. Conceptual or broad changes can be captured by a single statement.
7. **Incorporate existing CIP requirements not mapped to the *DHS Catalog*.** If a requirement is no longer necessary because the intent was captured elsewhere, then include this in the change documentation.
8. **Address specific directives from FERC Order 706** that may be applicable to the requirement.
9. **Analysis and Determination of Requirements for Medium and Low Impact:** In the analysis and determination of applicability of requirements to Medium and Low Impact Cyber Systems, consider the cost in relation to the security benefits (i.e., a minimal cost requirement that significantly mitigates risk would apply to *ALL* Cyber Systems. Similarly, a significant cost requirement that minimally reduces risk or provides little additional security may apply only to *HIGH* impact Cyber Systems).
10. **Specify Applicability to Environments:** Specify applicability of a requirement to Generation, Transmission, and/or Control Center environments.
11. **Apply Requirements to BES Cyber System:** Requirements should apply to either:
    (a) The BES Cyber System as a whole, or
    (b) Components of the BES Cyber System. However, when a requirement only applies to specific types of components, Sub-Teams should describe those types of components to determine where component classes exist.

(c) Requirements specific to boundary protection or ESP can be written to the interface of the BES Cyber System.

12: **Level of Requirements:** Sub-Teams should generally write the requirements at a high enough level to avoid applicability of specific technology. Where there are applicable CIP requirements, start with the CIP words and tweak if needed to include some DHS language/concept. However, the "level" of the requirements text should be raised, if needed.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Agenda
Cyber Security Order 706 SDT — Project 2008-06

May 27, 2010 | 9:00 am – 3:00 pm Eastern Time
FERC Offices

1. **Administrative Items**
   a. Introductions — All
   b. Agenda and Objectives — John Lim (SDT Chair)

2. **Project 2008-06 Cyber Security Order 706**
   a. Overview of draft CIP-010-1, Cyber Security — BES Cyber System Categorization – John Lim (SDT Chair)
   b. Overview of draft CIP-011-1 Cyber Security — BES Cyber System Protection – Philip Huff (SDT Vice-Chair)
   c. Workshop Review and Topics of Discussion
   d. Implementation Plan Discussion
   e. Summary of standard drafting team's resolutions of FERC directives included in Cyber Security Order 706
   f. Discussion - All

3. **FERC Staff Questions of the Standard Drafting Team**

4. **Standard Drafting Team Questions of FERC Staff — SDT**

5. **Next Steps — John Lim & Philip Huff**

6. **Adjourn**

116-390 Village Blvd.
Princeton, NJ 08540
609.452.8060 | www.nerc.com

Standard Drafting Team Preliminary Questions of FERC Staff — SDT

a. Does FERC see any "gaps" in the draft CIP Standards as published? Please describe. If so, please provide some direction on how they should be closed.

b. Does FERC see any "show stoppers" in the current set of draft CIP Standards that would cause the standards to not be approved?

c. Please provide feedback on the new proposed structure of the CIP Standards (CIP-010 & CIP-011 vs. CIP-002 through CIP-009). State any likes and dislikes.

d. Please provide feedback on the proposed table structure for the draft requirements in CIP-011. Suggest any improvements that should be made.

e. Please provide input concerning the proposed "bright lines" defined in the new draft CIP Standards, as presented in Attachment 2 to CIP-010.

f. Please provide input on the proposed schedule for completion of the current draft version of the CIP Standards (CIP-010 & CIP-011).

g. In its proposed schedule, the drafting team has deferred addressing a small subset of the Order 706 directives that are very complex and would require extensive industry deliberation in addressing them. Please provide any comment or feedback on this approach. .

h. Please provide input on the proposed Implementation Plan concepts for the CIP-010 & CIP-011 standards.

i. Please describe FERC's plans to support the individual drafting sub-teams and the full SDT going forward.

j. Specific discussion topics include:

   1) Immediate revocation requirements included in FERC Order 706
   2) Appropriate application of TFEs for the new draft standards

k. Please discuss the list of items/issues (if any) that are still open that must be resolved prior to approval of the new draft CIP Standards.

l. Please provide a sense of acceptability of the new draft CIP Standards to FERC staff. What improvements or changes in direction are needed to achieve acceptability?

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Minutes
Cyber Security Order 706 SDT — Project 2008-06

May 27, 2010
FERC Office
Washington, DC

Atmosphere was cordial and professional, and the meeting was constructive.

FERC staff agreed that the approach taken in the draft CIP-010 and CIP-011 standards could work, but acknowledged that a lot of work is still needed in clearly defining the requirements, tables, and Attachment II of CIP-010.

FERC staff expressed concern that the Low impact level requirements are insufficient and need to be bolstered. The Low baseline is too low.

The proposed 36-month review of the categorization needs to be shortened, at least for the first review cycle (possibly to 12 months)

Beware of hidden requirements in the purpose statements of the requirements, and review with the intent to minimize the adjectives used in the text (e.g., sufficient, proper, adequate, etc.) and clarify what is required with respect to auditability and enforceability.

The bright line thresholds stated in Attachment II need to be justified or at least explained.

The SDT must ensure that all of the requirements are auditable.

Concern was expressed on the deferring of some FERC directives until next year.

FERC staff recognizes that the schedule of the project is ambitious, and appreciates the monumental effort being performed by the SDT in creating these standards.

Introductions and Anti-Trust Guidelines

Regis Binder, FERC, welcomed the NERC SDT members, industry stakeholders, and other participants to the meeting and covered meeting logistics. Joe Bucciero conducted a roll call of members and participants in the room and on the conference call, and reviewed the need to comply with NERC's Antitrust Guidelines.

John Lim, SDT Chair, thanked FERC for hosting the meeting and providing the meeting room and facilities. He also reviewed the proposed meeting agenda.

FERC staff stated that they are not speaking for the Commission, and they recognize the importance of the cyber security issues to the industry and the country. FERC staff recognized the magnitude of the herculean effort and the excellent hard work being done by the SDT, in addition to everyone's day jobs, and stated this effort was fully appreciated.

The proposed agenda for the meeting is included as an attachment to this meeting summary. FERC staff was encouraged to ask questions throughout the presentation/discussion offered by the SDT regarding the new draft CIP standards.

Review of CIP-010-1

John Lim reviewed the strategy, approach, and history of CIP-010-1. The primary objectives of this standard are to: (1) help scope the electric system assets that are within the purview of the CIP-010 and CIP-011 standards; and (2) establish a list of reliability functions and "bright-lines" for categorization of the BES cyber systems.

a. Discussion of Scope

The process and criteria currently being used today for identifying critical assets in the electric system are thought to be inadequate. For example, less than 5% of the existing generation facilities around the country are considered to be critical assets, so the SDT has identified a new approach in the new CIP-010-1 standard.
The scoping process in the existing CIP-002 standard calls for identification of critical bulk electric system assets, then the associated critical cyber assets. In CIP-010, there are no 'out of scope' bulk electric system assets; instead a categorized list of those assets and their related cyber systems is required. That is one of the major differences between CIP-002 and CIP-010.

Attachment I of the draft CIP-010 standard is meant to provide the definition of scope and applicability. CIP-010 requires the categorization of cyber systems by defining a list of the real-time reliability functions that could have an impact on the reliable operation of the bulk electric system, and if a cyber system is doing any of those functions, then it is within scope.

Categorization of the electric system assets and the cyber systems based on multiple levels (High/Medium/Low) of their potential impact on the reliable operation of the bulk electric system is key aspect of the new draft CIP-010 & CIP-011 standards. Attachment II of the draft CIP-010 standard is meant to provide the criteria or "bright lines" to identify the potential impact (High/Medium/Low) on the reliable operation of the bulk electric system if the electric system asset or its cyber systems are destroyed, degraded, misused, or otherwise rendered unavailable. The concept is to take a more holistic view and move away from consideration of individual critical cyber asset issues, and place more focus on 'system' impacts.

One of the significant concepts behind collapsing the CIP-003 to CIP-009 standards into a single standard was to clarify the requirements for audit purposes and reduce the incumbent paper work thereby providing focus on the security of the key cyber systems. The SDT is concerned about the auditability of the requirements, and wants to ensure that the CIP-010 and CIP-011 requirements are auditable.

b. Discussion of CIP-010-1 Attachment I

The CIP-010 requirements apply to cyber systems that are relevant to real-time operations (not long term planning or systems that do engineering or marketing). The current benchmark parameter is "impactful within 15 minutes", where the 15 minutes relates to when the incident occurs. Discussion and feedback from the industry to determine if the 15 minute parameter is appropriate has been solicited through the recent informal posting and comment form for the draft CIP-010 and CIP-011 standards. FERC staff suggested that the drafting team consider adding security systems, both electronic and physical, to the list of Functions Essential to Reliable Operation, although the 15-minute rule probably shouldn't apply.

c. Discussion of Bright Lines

Question: In CIP-010 R1, the phrase "execute or enable" is used; what is meant by enable?

In some cases, a cyber system directly performs a function (as identified in Attachment I), but in other cases (e.g., data collection/aggregation or display) it is providing information to an operator or other systems to enable functions.

FERC staff observations: Once these draft CIP standards are filed, they will create a different benchmark or situation from the existing CIP standards for the industry to consider. Are we improving or not? What is the key yard stick? There seems to be a general belief that the number of assets identified to be critical to reliable operation of the BES under CIP-002 is inadequate (i.e., not enough assets being identified, less than 5% of generation). When these new draft CIP standards are filed, how can it be demonstrated that the key assets are identified? The size of unit is not the necessarily the key. What is the impact of the Contingency Reserve clause? Why is it appropriate; isn't

it similar to an N-1 analysis which the Commission rejected for applying CIP-002? Is the "medium" level of impact adequate for the number of units that can potentially fall into that category?

The intent is for the new CIP-010 standard to be comprehensive, in that all bulk electric system and cyber system assets will be covered to some level of impact. The "bright lines" are being provided to help clarify the assignment of the appropriate level of impact to each of the BES Cyber System assets. The SDT recognizes that measuring impact against what is considered 'critical' today is not good enough since today's results are not acceptable.

The SDT is looking for guidance from all industry participants with a stake in the game as to what is acceptable for the bright lines, and hoping to receive some guidance through the informal comments from the industry.

Allen Mosher: The draft CIP-010 standard is an improvement over what we have today, and we need to implement it soon. It's difficult to compare it to what we have today, because we have a different paradigm. We want to maximize our effort to identify the most critical assets and focus on the control systems. We should worry most about common use failures and wide spread loss of the bulk electric system.

Gerry Adamski: What are the criteria for identifying if an approach is adequate? What is adequate, and how do we identify it to help tweak the product? A thoughtful dialogue may be needed to better define the "bright lines" in Attachment II.
While the number of megawatts or the size of a unit can be one of the criteria used, the impact on day-to-day operations is also very important. The SDT should have a solid basis for the numbers used in Attachment II to define the "bright lines" that are used in the draft CIP-010 standard.

For example, generators, units, plants, etc. that are used intermittently, are they single or multiple control systems? The number of generation MWs connected to assets or to the control systems? If three units combined are over 2000 is it a High impact system? Are three separate control systems that are networked together a single cyber system? How does contingency analysis factor into the impact level criteria evaluation, if at all?
It might be helpful if the SDT can quantify the number of MWs of generation that would be classified as High impact using the new draft CIP-010 standard vs. today under the CIP-002 standard.A re-ordering the "bright lines" criteria identified in Attachment II should be considered, putting the control center criteria first.

FERC staff expressed concern that the requirements applicable to the Low impact criteria are not sufficient, and that the Low/Medium impact bright line is set too high.
Throughout CIP-010 there are references to quantities of MW; how were those quantities selected? Adding insight into how the values were determined (e.g., was a study done; is it from operating experience) would be very helpful. NERC indicated that many of the bright-line values came from a variety of resources available to NERC, plus active

participation and input from OC & PC members in the development of the standards. FERC does not have a magic study to use in its review and assessment of the bright lines.

d. Discussion of Guidance and Auditing

The SDT members agree that guidance is necessary for each of the requirements. There hasn't been enough time spent to-date to fully develop or flesh out guidance on each requirement. There is reason to believe not everyone knows or can identify all the key assets that auditors are concerned about, since the auditors learn something new every time they perform an audit.

Two NERC auditors have been engaged with the process of defining these new draft CIP 010 & CIP-011 standards as well as participation from the regional entities. There were many auditors involved in last week's SDT technical workshop held in Dallas, TX. The easiest standard to audit is a checklist, but that is the worst way to audit. Transparency is needed on how an entity is audited. The entity needs to know how the audit will be approached. In the filing, a summary description of what discretion is left to the entity may be helpful.

NERC will have its audit department staff review the draft CIP standards and provide comments from an auditor's perspective. Are the "bright lines" bright enough, including the concept of shared cyber systems?

e. Discussion of Compliance Review Schedule

The draft CIP-010 R3 requires at least a 36 month review cycle, since the bulk electric system doesn't change that much that often. Currently a three year process is used by the entities as a review trigger for going back to look at the standards and consider if any changes have occurred that would impact the High/Medium/Low categorizations. What are the triggering events for this review? Possibly the SDT should consider that a one to two year review cycle is needed at first, and then followed by the traditional three year cycle.

How assets are allowed to move from one category to another over time may be critical. Where should these requirements be addressed; in the audit process? Also, do we need to address assets that may be critical to a neighboring entity but may not be critical to my entity even though my entity controls the assets?

1. Review of CIP 011-1

Phil Huff provided an overview of CIP-011 and led the discussion. The overall approach by the SDT was to combine CIP-003 through CIP-009 into one standard, taking into account the FERC directives, the SDT's review of the DHS catalogue of cyber security requirements, and incorporation of those requirements that would be beneficial to the reliability of the BES.

a. Discussion of One vs. Multiple Standards

CIP-011 is presented as one standard with many parts. As such, putting all of the requirements together in one standard would tend to minimize the need to make conformance and cross-reference revisions solely because an associated CIP standard was modified.

Retaining the multiple standards approach carries with it some difficulties with synchronization of the requirements and versioning of the multiple standards. Retaining the multiple standards approach would possibly make it easier for entities to split up the CIP requirements for implementation and monitoring in a way to match the unique organization of the entities.

The SDT is divided on the issue of format for CIP-011 – formatting it in one standard communicates the standards should be seen as one. A multiple standards format makes it easier to change individual standards separately. The single standard approach would simplify the ability to incrementally change the full standard. However, implementation questions have been raised related to the substantial change it represents from the Version 3 numbering of standards and requirements.

The multiple standards approach carries the compliance issue of potentially multiple violations across multiple standards for the same identified problem. On the other hand, when violations are reported by standard, the single standard approach may result in this standard standing out in the violations report by combining so many requirements into one standard.

The SDT asked a question regarding format of the CIP-011 standard to gain some industry feedback, since the SDT itself could not reach a super majority decision on the best format approach.

b. Discussion of the Requirement Tables

A new feature in CIP-011 is how the requirements are presented, which is based on applicability/impact on the reliable operation of the BES. There are several subject areas identified in CIP-011, including: security governance and policy; personnel training, awareness, and risk assessment; physical security; electronic access control; etc. Each requirement has several characteristics identified, and each requirement is assigned to one

of the subject areas. A requirement is represented in the CIP-011 draft standard through a table that groups together all of the requirement's characteristics.

A few questions were raised by FERC staff regarding the requirements tables in CIP-011. For example, what is the intent of the 'blank' entries in a table? Are entities required to do anything? Can an entity be found in violation of a requirement if the corresponding table entry is blank? Should entities look at the rows in a table to determine compliance with the requirement?

c. Discussion of Specific Requirements and Wording

CIP-011 R1.3: What is the intent? The requirement to clearly identify a senior manager is not really stated in the requirement. The requirement is for the entities to designate a single official. How do you determine that, and when do you have to designate this individual? Nothing specifically says an entity shall designate this individual.
The training requirements seem to be scattered around the CIP-011 draft standard. Possibly a consolidation of the training requirements would be helpful. Also the choice and use of words such as 'training' vs. 'education', vs. 'credentials' needs to be reviewed for consistency of meaning. What is 'sufficient' training? Need to include a sense of frequency and magnitude around the training requirements.

Overall, the SDT needs to review the draft CIP standards with respect to the use of adjectives (e.g., sufficient, proper, adequate, etc.) and clarify what is required with respect to auditability and enforceability. For example, R5 vs. R16/R18 states "ensuring" vs. "guaranteeing". Which one is correct?

The SDT acknowledged that this draft of CIP-011 was prepared by multiple subteams within the SDT, and the multiple teams did not always use consistent language in developing the requirements. The SDT has been focused on developing compliance elements, but is now focused on writing the requirements clearly while also minimizing the need for TFEs.

d. Form and Format Issues

The Enforcement office at NERC is looking at the draft CIP standards with respect to the needs for enforceability and compliance, as well as the table structure of requirements. CIP 011 covers the requirements previously included in CIP-003 thru 009; have these requirements been incorporated or do the requirements from CIP-003 thru CIP-009 need to be maintained?

Some of the more document-focused requirements are no longer in the new draft standards. Does that meet the equally protective criteria? The intent is to improve the standards by removing the administrative requirements that do not improve reliability in any way.

The need for more than paper evidence of compliance may lead to actual need to demonstrate compliance. For example, current requirements call for paper demonstration rather than allow for actual demonstration of the protection system; the latter improves security. Creation of paper lists of authorized personnel is a Chinese fire drill that does not improve system security.

A mapping will be done to identify gaps in the standards that we will address in the version coming out in July for industry comment and ballot. The idea is to explain clearly why the gaps are there, and that these gaps do not affect the reliability of the BES. One of the biggest issues is the perception of a culture of compliance. Now you have multiple violations of the same standard, and from the way it would be reported today, it would stick out. NERC/FERC need to make sure this does not present a skewed view of the CIP standards.

Concern was raised about the status of the components that make-up the tables. The 'R' (for requirement) is not used for the components in the table. How does that relate to the roll-up methodology; what is and is not a requirement? What is the status of the actual wording in the parent requirement (ahead of the table), and how does it relate to the components in the table?

In Tables R4 to R9, there seems to be a general formula for the requirement, which is each responsible entity shall apply the criteria with a goal of preventing unauthorized access to BES cyber systems. However, a responsible entity that has a Low impact BES cyber system does not have an entry in the table that indicates that the entity has to address any of the subcomponents. Is that entity still subject to the requirements of R5? Similarly, if a Medium impact cyber system has in fact restricted physical access according to 5.1, but there is in fact an unauthorized access – would that be a violation of R5? The intent of the entries in the tables and the requirements needs to be clarified. How will the goal of preventing unauthorized access be accomplished on assets with Low impact, when there is no requirement defined?

e. Discussion of Applicable Time Barometer

The discussion centered around why a 15 minute time period was selected as the barometer for the impact time stated in the draft CIP-010 standard. Isn't it dependent on current system conditions? Whatever time period is chosen will it be readily evident to the entities?

How quickly can it be determined that there is an impact on the bulk electric system? When does the impact happen? Is it objective enough for an entity to determine for purposes of verifying for audits?

Is a qualifier needed for peak electric system conditions or most stressful conditions? Time of year and load conditions may impact the determination of the time used.

The draft CIP standard is written around how the set of functions impact the reliable operation of the bulk electric system; some functions have more immediate impacts and others take longer to impact the BES.

Misuse of a system may have a longer lead time, far longer than fifteen minutes, but an equally devastating impact. The SDT might need to revisit the definition or application of the fifteen minute time period.

2. Implementation Plan

Scott Mix provided a high level overview of the implementation plan concepts and issues being considered by the SDT. A subgroup has been formed to prepare the text for the Implementation Plan. They will likely start meeting during the SDT Meeting in June 2010 in Sacramento.

Scott Mix presented the slides he recently gave at the SDT Workshop in Dallas, TX. He noted that the plan is to retire CIP 002 and CIP 003-009 within a transition period as CIP-010 and CIP-011 become effective.

a. Discussion of Implementation Plan Issues

The SDT is working on relevant timetables for implementation of the draft CIP-010 and CIP-011 standards, including how to prioritize the effort in terms of importance and in terms of timing.

The SDT needs to try to identify in a general sense which assets will eventually fall into each of the High/Medium/Low impact categories and how many assets will be in each category. A significant benchmark between the CIP-002 and the CIP-010 & CIP-011 standards will be the number of assets involved, and has that number increased in size and scope.

How should the industry be incentivize to implement the new CIP-010 & CIP-011 standards, but not the Medium or Low impact controls at the expense of first focusing on the High impact assets. Possibly a 'rolling' implementation of the standards is in order. What is the impact categorization of a BES cyber system if it moves up or down an impact level? How should it be considered in the implementation plan?
The Implementation Plan subteam will also work with the nuclear folks to discuss policies and impacts vs. an implementation schedule. Two stakeholders from the nuclear industry will be part of the implementation plan subteam.

Some level of reporting to FERC on implementation plan development (including content and schedule) is encouraged. The reporting should be designed to provide review of justifications, milestones, and accountability while offering a degree of oversight.
One possible scenario for implementation plan development would be for the entities to quickly develop their lists of categorized assets, immediately followed by the

establishment of their respective implementation plan. The responsible entities should then report their implementation plans to the respective regional entity for approval. Guidance documents will be prepared by the SDT to provide a level of consistency and assistance in the development of the implementation plans. Potential conflicts between compliance deadlines and audit schedules must also be considered.

Allow entities to be compliant early especially through implementation of system upgrades that will need to be compliant later. We'll need to recognize that some entities may need additional time to do the job right while maintaining appropriate levels of oversight. For example, larger organizations may have a larger portion of assets affected by the new standards.

During the discussion, Allen Mosher suggested that a possibility to consider would be to base the implementation plan on the current mitigation plan process. The discussion of this idea continued with many including FERC staff seeing possible merit to this approach.

b. Discussion of Transition and Migration

A transition plan from the existing CIP-002 to CIP-009 requirements to the new draft CIP-010 and CIP-011 requirements is needed. Some CIP-011 requirements are a direct replacement for those in CIP-003-009 and a migration plan should be developed for those, while other requirements are new and an implementation plan is needed. Plans to guide the entity may be helpful to both the entity and the auditors. A roadmap for the transition/migration activities would help in the development of a schedule to accomplish these tasks.

The draft CIP-011 standard does not appear to provide a significant base level of protection for the low and medium impact controls. FERC staff expressed concern that the controls requirements for the "low" impact systems do not provide an adequate level of protection. The blank entries in the tables in CIP-011 might imply that there are no control requirements.

c. Discussion of Physical Controls

Physical items or locations may have protection but may not be auditable as a NERC standard, which focuses on cyber assets. For example, substations have physical protection, but how can an auditor be convinced that the physical fence or padlock was there thirty days ago.

The focus of the SDT is on cyber security. The team considered a separate SAR for physical security. The issue is not when the fence went up, but was it secured and was the lock actually locked – actually visiting remote sites to prove this might be too much.

Too much energy goes into such audits without corresponding benefit of protecting the system. An auditor might randomly select a few remote sites – because selection is random, but an entity would need to protect them all.

d. Discussion of Immediate Revocation

It's questionable if the industry can meet targets for "immediate revocation of access". Do timeframes of 72 hours work? May need a primary and secondary revocation applied to remote and/or physical access – this will also depend on the "cause" for revocation.

What does "immediate" really mean in these cases? For example, an entity may need to revoke access of an individual before letting the person go for cause. "Immediate" is not auditable, even if we set a time period. "As soon as possible" would be a better phrase or a set time period would be sufficient. If it is a planned termination, then it can be immediate because it precedes the termination. If it is part of an emergency, revocation may need a reasonable time period.

e. Discussion of Security Systems Protection

FERC staff suggested adding a fourth column to the tables in CIP-011 that would list the physical/cyber security system protection required for each asset. The intent is to apply the appropriate level of security. It was also suggested that a function be added to the table in Attachment I of CIP-010 for security/protection systems.
Security systems impact the BES. Passwords – maximize use without being prescriptive – suggested language – cut down on TFE's

f. Beyond CIP-010 and CIP-011

FERC Order 706 included some directives (e.g., defense in depth) that have not been addressed so far. The SDT felt there was too little time to accomplish these requirements and that tackling them might have derailed the process to this point.
Concern is that some of the items may have been part of the paradigm shift FERC was asking for in Order 706. How can some of these items in the order be defined, or implemented, or audited, etc.?

Implementation of an active vulnerability assessment (testing) can be contrary to reliability and security. Special care and guidelines are needed for this requirement.
The December 2010 date for filing of the new draft CIP standards for approval by FERC is not one of the Commission directives. It can become an informational filing, since it is not making law, and may be changed with FERC approval. Need to implement improvements sooner, but may not be able to resolve issues now.

The SDT is planning to file the new draft CIP-010 and CIP-011 standards by December 2010, and will start in January 2011 to look at the other remaining issues – may be a continuously moving target.

The recent SDT Technical Workshop was aimed in part at telegraphing this schedule to the industry and thereby telling them the new standards are not a completed deal. Scott Mix stated that 'Defense in depth' is implementation of guidance or guidelines for layered security, which is guidance for designing but not necessarily an auditable requirement. Concern was expressed that 'Defense in depth' was a difficult concept to define as enforceable requirements.

The SDT would benefit from a shared dialogue with FERC Staff on defense in depth and other issues about what we are trying to achieve, the overall objective, and what is needed for the industry to reach it. This dialogue would go beyond just the standards, but could also cover how you approach audits and compliance. NERC and the SDT still have to legally deal with the directives in FERC Order 706. The SDT may ask for clarification of specific parking lot issues, or maybe a separate filing on those issues should be developed.

3. Closing

The dialogue and sharing of information during this meeting was constructive and has been very useful. The FERC staff reminded us that they do not speak for the Commission. They may not agree with the statements or agreements reached. However, with continued dialogue and progress on the issues we may at least achieve a mutual understanding of the problems and concerns being addressed.

Gerry Adamski asked FERC staff about their general sense of acceptability of the body of work to date? Also, what needs more work? The approach is responsive, but as discussed earlier, there are many questions remaining, including how the impact levels will be applied. There is still a lot of work to be done to achieve the filing by the end of 2010. It is a very aggressive schedule, but there is recognition of the quality and amount of effort involved.

Meeting adjourned.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Draft Agenda

Cyber Security Order 706 SDT — Project 2008-06

June 8, 2010 | 8 a.m.–5 p.m. PDT
June 9, 2010 | 8 a.m.–5 p.m. PDT
June 10, 2010 | 8 a.m.–5 p.m. PDT
June 11, 2010 | 8 a.m.–noon PDT
Sacramento, California

NOTE:

1. Agenda Times May be Adjusted as Needed during the Meeting
2. Drafting Team Meetings May Not Have Access to Telephones and Ready Talk

Tuesday, June 8, 2010 8 a.m.–5 p.m. PDT

1. Introduction, Welcome and Opening Remarks
2. Discussion of Work Plan and Schedule: June-December 2010 — *Stu Langton*
3. Review and Seek Agreement on Drafting Team Proposal for refining the SDT Consensus Procedures
4. Updates on other related Cyber Security Initiatives — *NERC Staff and SDT Members*
5. Review Results of the May 27, 2010 Meeting with FERC and Guidance for Sub-teams
6. Technical Workshop Overview and Results
7. Overview of Industry Response to Request for Informal Comments — Scott Mix
8. Review of Industry Input on CIP Format and Consensus Testing on CIP Format going Forward
9. Sub-Teams Meet to Review and Discuss Industry Comments, Suggestions, and Changes to the Draft CIP Standards

Wednesday, June 9, 2010 8 a.m.–5 p.m. PDT

1. Sub-Team Initial Reports — Key Issues
2. Sub-Team Meetings
3. Sub-Team Reports

Thursday, June 10, 2010 8 a.m.–5 p.m. PDT

1. Sub-Team Reports and SDT Review of Industry Comments and Possible Changes

Friday, June 11, 2010 8 a.m.–noon PDT

1. Review Next Steps and Sub-Team Schedule

116-390 Village Blvd.
Princeton, NJ 08540
609.452.8060 | www.nerc.com

2. Review the SDT Pittsburgh Meeting Agenda and Perform the Meeting Evaluation
3. Sub-Team Meetings
4. Implementation Plan Drafting Team Report
5. Guidance Document Drafting Team Report

1. Chairman	**John Lim**, CISSP Department Manager, IT Infrastructure Planning	Consolidated Edison Co. of New York New York, New York
2. Vice-Chairman	**Philip Huff** Manager, IT Security and Compliance	Arkansas Electric Cooperative Corporation Little Rock, Arkansas
Members		
3.	**Robert Antonishen** Protection and Control Manager, Hydro Engineering Division	Ontario Power Generation Inc. Niagara-on the-Lake, Ontario
4.	**Jim Brenton**, CISSP-ISSAP Director, CIP Standards Development	Electric Reliability Council of Texas, Inc. Taylor, Texas
5.	**Jackie Collett** Cyber Security Operations Engineer	Manitoba Hydro Winnipeg, Manitoba
6.	**Jay S. Cribb** Information Security Analyst, Principal	Southern Company Services, Inc. Atlanta, Georgia
7.	**Joe Doetzl** Manager, Information Security	Kansas City Power & Light Co. Kansas City, Missouri
8.	**Sharon Edwards** Project Manager	Duke Energy Cincinnati, Ohio
9.	**Gerald S. Freese** Director, Enterprise Information Security	American Electric Power Columbus, Ohio
10.	**Jeffrey Hoffman** Chief Architect IT Policy & Security Division	U.S. Bureau of Reclamation Denver Federal Center Denver, Colorado
11.	**Doug Johnson** Operations Support Group Transmission Operations & Planning	Exelon - Commonwealth Edison Lombard, Illinois
12.	**Patricio Leon-Alvarado** Engineer, E&TS Compliance and Quality	Southern California Edison Pomona, California
13.	**Frank Kim** Director, Power System Information Tech.	Hydro One Networks, Inc. Barrie, Ontario
14.	**Richard Kinas** Manager of Standards Compliance	Orlando Utilities Commission Orlando, Florida
15.	**David L. Norton** Policy Consultant - CIP	Entergy Corporation New Orleans, Louisiana
16.	**David S Revill** Group Lead, Electronic Maintenance	Georgia Transmission Corporation Tucker, Georgia
17.	**Scott Rosenberger** Director, Security and Compliance	Luminant Dallas, Texas

18.	**Kevin Sherlin** Manager, Business Technology Operations	Sacramento Municipal Utility District Sacramento, California
19.	**Jon Stanford** Chief Information Security Officer	Bonneville Power Administration Portland, Oregon
20.	**Thomas Stevenson** Gen Supv. Engineering Projects Generation Services Dept	Constellation Energy Baltimore, MD
21.	**Keith Stouffer** Program Manager, Industrial Control System Security	National Institute of Standards & Technology Gaithersburg, Maryland
22.	**John Van Boxtel** CIP Compliance Engineer	Western Electricity Coordinating Council Vancouver, WA 98662
23.	**John D. Varnell** Director, Asset Operations Analysis	Tenaska Power Services Co. Arlington, Texas
24.	**William Winters** IS Senior Systems Consultant	Arizona Public Service Co. Phoenix, Arizona
Consultant to NERC	**Joseph Bucciero** President and Executive Consultant	Bucciero Consulting, LLC 3011 Samantha Way Gilbertsville, Pennsylvania 19525
Facilitator Consultant	**Hal Beardall**	FCRC Consensus Center Florida State University
Facilitator Consultant	**Robert M. Jones**	FCRC Consensus Center Florida State University
Facilitator Consultant	**Stuart Langton, PhD**	FCRC Consensus Center Florida State University
NERC Staff	**Gerard Adamski** Vice President and Director of Standards	North American Electric Reliability Corporation Princeton, New Jersey
NERC Staff	**Howard L. Gugel** Standards Development Coordinator	North American Electric Reliability Corporation Princeton, New Jersey
NERC Staff	**Roger Lampila** Regional Compliance Auditor	North American Electric Reliability Corporation Princeton, New Jersey
NERC Staff	**Scott R Mix** Manager Infrastructure Security	North American Electric Reliability Corporation Princeton, New Jersey
NERC Staff	**David Taylor** Manager of Standards Development	North American Electric Reliability Corporation Princeton, New Jersey
NERC Staff	**Todd Thompson** Compliance Investigator	North American Electric Reliability Corporation Princeton, New Jersey

CSO 706 SDT SCHEDULE: FULL CIP-010 & CIP-011 PACKAGE		
Week Of	***Key Dates***	***CIP Task***
4/12/2010	**SDT Meeting** **Atlanta, GA (Southern Co)** **(4/13-16)**	**Present Controls draft for full SDT review and comment. Sub team drafting. Finalize draft for Informal Comment, Full Package**
4/19/2010	4/19-4/23/2010 4/23/2010	**SDT Sub-Teams and Leads Meet to Finalize Documents** **NERC Receives and Prepares Full Package for Industry Comment**
4/26/2010	**4/26/2010** **4/27/2010** **4/28/2010** **4/29/2010**	**SDT Sub-Teams Develop Package** **SDT Reviews with NERC Staff Proposals** **SDT Scoping Meeting on Documents** **SDT Reviews and Approves Full Package for 30-day Industry Comment Period**
5/3/2010	**5/4/2010**	**Informal Comment Posting for full package starts Completes on 6/3/2010**
5/10/2010	**SDT Meeting** **Dallas, TX (Luminant) (5/11-13)**	**Review Parking Lot Issues, Prepare for Industry Workshop and Begin Development of Guidance Documents**
5/17/2010	5/19 & 5/20/2010	**1.5-day Industry Technical Workshop (Dallas, TX)**
5/24/2010	5/24 to 5/28/2010 5/27/2010	**SDT Considers Comments from Workshop** **Meeting with FERC Staff to Review Draft Standards and Posting**
5/31/2010	6/3/2010 6/4/2010	**Informal comment period ends** **SDT Reviews Comments Received** **Sub team meetings to Review Comments Received**
6/7/2010	6/7/2010 **SDT Meeting, Sacramento, CA (SMUD) (6/8-11)**	**Sub team meetings to Review Comments Received** **Industry comment review, response process, re-drafting, as needed**
6/14/2010		Sub team meetings to prepare sections for review
6/21/2010	SDT Meeting and Sub-teams via ReadyTalk	SDT interim online meetings and Sub-team meetings to prepare sections for review
6/28/2010	SDT Meeting and Sub-teams via ReadyTalk	SDT interim online meetings and Sub-team meetings to prepare sections for review
7/5/2010	NERC Staff review	Sub teams complete all work assignments & NERC Review
7/12/2010	**SDT Meeting, Pittsburgh, PA (CERT) (7/13-16)**	**Finalize & Approve Documents for posting for 45 day formal comment period**

CSO 706 SDT SCHEDULE: FULL CIP-010 & CIP-011 PACKAGE		
Week Of	***Key Dates***	***CIP Task***
7/19/2010	7/19/2010 7/21/2010 7/21/2010	**-NERC seeks SC Approval for Ballot** **-Post CIP Standards for Formal Comment** **-45 Day formal comment period begins (closes on 9/3/2010)** **-Begin Ballot Pool Formation**
7/26/2010		**Formal comment period for CIP standards** **Prepare for industry webinar**
8/2/2010		**Formal comment period for CIP standards** **Prepare for industry webinar**
8/9/2010	**SDT Meeting, Chicago, IL (ComEd) (8/10-13)**	**Formal comment period for CIP standards** **Finalize presentation for industry webinar**
8/16/2010	8/17/2010 8/19/2010	**Hold Industry Webinar (tentative)** **Ballot Pool Formation Ends**
8/23/2010	8/25/2010	**Initial Ballot Begins**
8/30/2010	9/3/2010	**Initial Ballot Ends**
9/6/2010	**SDT Meeting Winnipeg, Canada (Manitoba Hydro) (9/7-10)**	**Review ballot results** **Respond to comments received** **Draft revisions to standards**
9/13/2010		Sub-team meetings
9/20/2010	9/20/2010 9/24/2010	Sub-team meetings, NERC Staff Review Full SDT on-line meeting to approve revised draft of documents for re-ballot
9/27/2010	9/27 to 10/6/2010	Re-Ballot Period
10/4/2010	10/6/2010	Re-Ballot ends; comments received by SDT
10/11/2010	**SDT Meeting, Toronto, Canada (OPG) (10/12-15)**	**Prepare responses to 2nd ballot comments**
10/18/2010		**Sub-teams meet to adjust requirements, as needed**
10/25/2010	10/25/2010 10/29/2010	**-Prepare and finalize revisions to standards** **-NERC Staff review** **-SDT Approval for re-ballot (if needed)**
11/1/2010	11/1 to 11/10/2010	3rd Ballot Period (if needed)
11/8/2010	11/10/2010	Ballot period ends

CSO 706 SDT SCHEDULE: FULL CIP-010 & CIP-011 PACKAGE		
Week Of	***Key Dates***	***CIP Task***
11/15/2010	**SDT Meeting, Baltimore, MD (Constellation Energy) (11/16-19)**	**Prepare responses to 3rd Ballot comments**
11/22/2010		*NERC and SDT finalize responses to ballot package*
11/29/2010		*Seek SC and BOT Approval for Filing*
12/6/2010		*Seek SC and BOT Approval for Filing*
12/13/2010	**SDT Meeting Tampa, FL (FRCC) (12/13-17)**	**SDT Meeting to review Filing Completion of Phase 2**
12/24/2010		***Submit for Regulatory Approval***

Proposed Refinements to CSO 706 SDT Consensus Guidelines
(June 2010)

(Draft Procedure including Electronic Mail procedure drafted by Bill Winters and John Van Boxtel)

The Cyber Security for Order 706 Standard Drafting Team (Team) will seek consensus on its recommendations for any revisions to the CIP standards.

Consensus Defined. Consensus is a participatory process whereby, on matters of substance, the Team strives for agreements which all of the members can accept, support, live with or agree not to oppose. In instances where, after vigorously exploring possible ways to enhance the members' support for posting CIP standards documents for industry comment or balloting, and the Team finds that 100% acceptance or support of the members present is not achievable, decisions to adopt standards documents for balloting will require at least 75% favorable vote of all members present and voting. This super majority decision rule underscores the importance of actively developing a Team consensus on substantive issues, which the industry will need to approve, by a 2/3's vote.

Postings for Industry Comment. For decisions on CIP standards documents to be posted for industry comment where the Team finds that 75% acceptance or support is not achievable but an option or options under consideration had greater than 50% support from the Team, the Team's accompanying Comment form will seek industry input to help the Team resolve any differences and select an option going forward.

Quorum Defined. The Team will make decisions only when a quorum is present. A quorum shall be constituted by at least 2/3 of the appointed members being present in person or by telephone.

Electronic Mail Voting. Electronic voting will only be used when a decision needs to be made between regular meetings under the following conditions:

- It is not possible to coordinate and schedule a conference call for the purpose of voting, or;
- Scheduling a conference call solely for the purpose of voting would be an unnecessary use of time and resources, and the item is considered a small procedural issue that is likely to pass without debate.

Electronic voting will not be used to decide on issues that would require a super majority vote or have been previously voted on during a regular meeting or for any issues that those with opposing views would feel compelled to want to justify and explain their position to other team members prior to a vote. The Electronic Voting procedure shall include the following four steps:

1. The SDT Chair or Vice-Chair in his absence will announce the vote on the SDT mailing list and include the following written information: a summary of the issue being voted on and the vote options; the reason the electronic voting is being

conducted; the deadline for voting (which must be at least 4 hours after the time of the announcement).

2. Electronic votes will be tallied at the time of the deadline and no further votes will be counted. If quorum is not reached by the deadline then the vote on the proposal will not pass and the deadline will not be extended.
3. Electronic voting results will be summarized and announced after the voting deadline back to the SDT+ mailing list.
4. Electronic voting results will be recapped at the beginning of the next regular meeting of the SDT.

Consensus Building Techniques and Robert's Rules of Order. The Team will develop its recommendations using consensus-building techniques with the leadership of the Chair and Vice Chair and the assistance of the facilitators. Techniques such as brainstorming, ranking and prioritizing approaches will be utilized. The Team's consensus process will be conducted as a facilitated consensus-building process. Only Team members may participate in consensus ranking or votes on proposals and recommendations. Observers/members of the public are welcome to speak when recognized by the Chair, Vice Chair or Facilitator. The Team will utilize Robert's Rules of Order *(as per the NERC Reliability Standards Development Procedure),* as modified by the Team's adopted procedural guidelines, to make and approve motions. However, the 75% super-majority voting requirement will supersede the normal voting requirements used in Robert's Rules of Order for decision-making on substantive motions and amendments to motions. The Team will develop substantive written materials and options using their adopted facilitated consensus-building procedures, and will use Robert's Rules of Order only for formal motions once the Chair determines that a facilitated discussion is completed.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

CSO 706 SDT DRAFTING SUB-TEAMS

May, 2010

Sub-Team	
CIP 010 (002-4) BES System Categorization	John Lim, Rich Kinas, Jim Brenton, Jackie Collett, Bill Winters, Dave Norton, Jay Cribb *Rod Hardiman (Observer)*
Governance	Jon Stanford, Jerry Freese
Personnel and Physical Security	Doug Johnson (Lead), Rob Antonishen, Patrick Leon, Kevin Sherlin
System Security and Boundary Protection	Jay Cribb (Lead), John Varnell John Van Boxtel,
Incident Response and Recovery	Scott Rosenberger (Lead), Joe Doetzl, Tom Stevenson, (*Observer Participants: Jason Marshall*
Access Control	Sharon Edwards (Lead), Jeff Hoffman, Frank Kim *Observer Participants: Sam Merrell*
Change Management, System Lifecycle and Information Protection and Maintenance	Dave Revill (Lead), Keith Stouffer, Bill Winters, Phil Huff *Observer Participants: John Fridye*

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Notes
Cyber Security Order 706 SDT — Project 2008-06

June 8, 2010, | 8 AM to 5 PM PST
June 9, 2010 | 8 AM to 5 PM PST
June 10, 2010 | 8 AM to 5:00 PM PST
June 11, 2010 | 8 AM to 12:00 PM PST

Unanimously Adopted, July 15, 2010

Robert Jones, Stuart Langton, and Hal Beardall
Facilitation and Meeting Design
FCRC Consensus Center, Florida State University

Joe Bucciero, Bucciero Consulting, LLC

http://www.nerc.com/filez/standards/Project_2008-06_Cyber_Security.html

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

CSO706 SDT June 8-11, 2010 Meeting Summary Contents

CSO706 SDT JUNE 8-11, 2010 MEETING
SACRAMENTO, CA

EXECUTIVE SUMMARY

On Tuesday morning, the Chair, John Lim welcomed the members to the SDT's 23rd meeting. Joe Bucciero conducted a roll call of members and participants in the room and on the conference call *(See Appendix #2*). The host Kevin Sherlin, a SDT member, welcomed everyone to the Sacramento, California SMUD meeting facilities and covered logistics. Mr. Bucciero reviewed the need to comply with NERC's Antitrust Guidelines *(See Appendix #3).* The Chair reviewed the proposed meeting objectives. Bob Jones, facilitator, reviewed the proposed timed meeting agenda *(See appendix #1*). On Thursday morning the SDT approved without objection the meeting summary for the May 11-13, 2010 SDT session in Dallas, Texas.

Keith Stouffer, an SDT member, noted the release in the next couple of weeks of a new draft from NIST committee. Scott Rosenberger noted that Cyberstorm-3 will be taking place in the Fall of 2010 and they are looking again for volunteers.

Mr. Van Boxtel reviewed the proposed addition of an electronic voting section to the Team's Consensus Procedures with the Team. He noted it was narrowly designed to address those instances where the SDT could not secure a quorum for a face-to-face or conference call. The Team agreed to deleting the section "Posting of Industry Comment" as it would only apply to informal industry comment postings and agreed to extend the time for decision in the email vote procedure from 4 to 12 hours. The motion passed with 17 yeas and 1 nay. Dave Revill noted his concern was that the procedure was too narrow in that it did not allow electronic vote for posting documents for comments or ballot.

The SDT reviewed and discussed the schedule and work plan at several points during the Sacramento meeting. On Tuesday there was a discussion generally on the current plan that the Team adopted in May, 2010 to complete work and post for formal comment CIP 010 and 011 at the conclusion of the Pittsburgh meeting in July, 2010.

Phil Huff presented a draft schedule for the next four weeks to complete its work in Pittsburgh and file the CIP 010 and CIP 011 for formal comment and balloting. He noted the necessary deliverables including: CIP 010 and 011 standards/requirements; VSL's, measures, guidance document; FERC directives summary; CIP version 3 mapping; informal comment summary; and comment form for the formal comment posting.

Bob Jones summarized the context for the schedule which the Team had discussed noting the possibility of two rounds instead of three and using the additional time to improve product. Stu Langton reviewed the dynamic current political context and the need felt to demonstrate that the industry can produce a good product in a reasonable amount of time. However, as the Team has

discussed, once it sends the standard out for the first ballot they will lose flexibility in making changes.

It was noted that the Standards Committee was meeting concurrent with the SDT's Tuesday morning discussion. Following lunch on Tuesday, Howard Gugel reported to the Team on the Standards Committee call. He noted that NERC President Gerry Cauley and Standards Committee Chair Alan Mosher felt strongly a need to present some cyber security standards changes to FERC and Congress by the end of the year. CEOs in the industry have expressed concern that CIP 010 and 011 may not pass by end of the year and that there may be a need for a "Plan B" which might take CIP-010 with high and medium bright lines and then add CIP-003-009 as is. Jason Marshall noted that President Cauley is focused on responding to Congress.

Phil Huff reported on the Sub-team leads lunch discussion regarding schedule adjustments – think complete revisions based on comments by July, push formal posting until after August – it is not feasible to post prior to August 20th – also assumes support from NERC staff for drafting and adjusting the membership on some sub teams. The SDT Leadership will talk to standards committee and NERC management to seek pushing the initial posting back 31 days from the current plan which would mean the Chicago meeting in August. The end of year deadline depends on the level of industry acceptance in formal posting and ballots.

After discussion about the time frame and content the facilitators suggested a straw poll on different extensions of time assuming the same SDT monthly meeting schedule and interim conference calls and assuming that all FERC directives will be addressed including the "Post Version 4" directives. Members expressed their preferences among one of three options. Each option included the 38 days to the Pittsburgh meeting plus:

- **Option A.:** adding 30 more days, that is to the SDT Chicago meeting-August 10-13, (Sub-team leads proposal) and then to initial ballot – **2 members**.
- **Option B:** adding 60 more days, that is to the SDT Winnipeg, September 7-10 meeting, and then to initial ballot – **8 members.**
- **Option C**- adding 90 more days, that is to the SDT Toronto October 12-15 meeting, and then to initial ballot – **12 members.**

Following this, John Van Boxtel proposed a motion that was discussed and revised as follows:

> Based on the results of industry feedback from the informal comment period, and the need to send a quality product out to the industry to gain acceptance of the new standard, the SDT should compose a letter to the Standards Committee and key NERC staff identifying these issues and ask for an extension for the posting of the CIP draft standards in October 2010 to be added to the schedule to develop the CIP-010 and CIP-011

The Vote on the motion to adopt was: **11 yea – 5 nay (69%).**

Bob Jones suggested that the SDT is unanimous that it needs more time to do a quality job based on the industry comments, Order 706 directives and FERC comments. The Chair thanked the Team and suggested the Chair and Vice Chair would take this as guidance in their discussion on Friday morning with the Chair of the Standards Committee.

On early Friday morning, John Lim and Phil Huff reported to the SDT on a conference with the chair of the Standards Committee, Allen Mosher. They discussed with him the time and schedule for the CSO706 Project, and the Standards Committee was agreeable to a 90 day extension to complete the CIP-011 work if there could be a CIP-010 product going out to industry in July. Mr. Mosher requested the SDT to create a schedule for moving forward with both CIP-010 and CIP-011, and he suggested that in the interim until implementation of CIP-010 and CIP-011 that the SDT use an amended CIP-002 to address the issue of critical assets. Phil noted that he and John raised the remaining Order 706 directives issue, and Mr. Mosher understood the difficulty of getting both out by end of year but expressed the need for something by end of year if not the full package.

Phil Huff reviewed with each of the Sub-teams where each team was in summarizing the comments. Three teams are still working on summaries while others have identified key issues. None have moved on to consider how to address the comments and changes to the requirements. He noted that there was a possibility, if needed, to split up Jay Cribb's team into two sub-teams (005 and 007) and he would consult with Jay and other team members before a decision was made.

Following the morning call with the Standards Committee leadership, the SDT Chair and Vice Chair decided to schedule a SDT conference call meeting to discuss a proposed new schedule.

Bob Jones reviewed the documents compiled for the SDT's review of industry comments. He summarized an overall set of results showing the percentage of support or opposition for key components and questions. Scott Mix had sent out over the weekend a "consideration of comments" document that included over 900 pages.

The Chair noted that the Team received a significant amount of input from the industry and FERC since the posting, and the SDT will need to review and consider what kinds of revisions may be needed for the CIP-010 and CIP-011 requirements based on these comments and the SDT's continuing development of these requirements. He noted that the next phase will include a pre-ballot review followed by formal ballot, and underscored the point that there is a lot of work ahead of the SDT. The comment period closed on June 3, which did not give the SDT much time to review the comments prior to the Sacramento meeting. The SDT will need to rely on and trust that Sub-Teams will work to address the comments and share with the full SDT their summary of those comments.

The Team has maintained an ongoing "parking lot", a table list of issues raised in the course of the development and discussion of CIP-010 and CIP-011, and as part of the SDT's review of the industry comments. These were presented and discussed by the Team and a table that defines

these issues and identifies how they were or will be resolved or handled going forward is included as an appendix to this summary.

Joe Bucciero provided the SDT with a meeting summary that offered an overview of the FERC/SDT meeting held on May 27th at FERC's offices in Washington, DC (*See Appendix #X)*. John Lim noted that the atmosphere for the meeting was cordial and professional, and the meeting brought forth constructive input and ideas. In general, FERC staff agreed with the approach taken in the draft CIP-010 and CIP-011 standards, but acknowledged that a lot of work is still needed in clearly defining the requirements. Joe noted that FERC staff expressed the following issues and concerns:

- The Low impact level requirements are insufficient and need to be bolstered, i.e. the Low baseline is too low.
- The proposed 36-month review cycle for the impact categorization needs to be shortened, at least for the first review cycle (possibly to 12 months).
- Beware of hidden requirements in the purpose statements of the requirements, and review with the intent to minimize the adjectives used in the text (e.g., sufficient, proper, adequate, etc.) and clarify what is required with respect to auditability and enforceability.
- The bright line thresholds stated in Attachment II need to be justified or at least explained.
- The SDT must ensure that all of the requirements are auditable.
- Concern was expressed on the deferring of some FERC directives until next year.

FERC staff recognizes that the schedule of the project is ambitious, and appreciates the significant effort being performed by the SDT in creating these standards. Jan Bargen, FERC, noted that they recognize the considerable amount of work of the SDT so far, but believes there is still more to be done including both the justification and baseline issues – e.g., how do you address the minimum requirements, are we moving forward if more of the electric system is not covered, need to explain why this is better. There are too many items not currently included. What else is being brought in to the new standards? Is the baseline for protection of BES equipment set at the right level. The SDT also discussed the issue of "immediate revocation", the baseline for Low Impacts, Physical Security, bright lines, and avoiding the prescriptive (how) in drafting standards.

The SDT also held an industry technical workshop in Dallas, TX on May 19-20, 2010 as a form of outreach to the industry concerning the new cyber security requirements. The Chair noted that this was the first time NERC has used such a workshop in the context of a standards development process and any lessons learned would be helpful for NERC to consider. He suggested that there was excellent industry turnout for the workshop, and some excellent questions were raised and suggestions offered that the SDT should consider going forward. The Team discussed ways to make future workshops more interactive.

The Chair proposed that the Sub-teams meet to review and summarize industry comments and report back to the full SDT.

Bob Jones presented an overview of Industry responses for Question 9 regarding the format for CIP 011.

CIP 011 COMBINED REQUIREMENTS FORMAT

	Totals	*%*
Keep CIP 011-1 as one document-	(48)	40.3 %
Break CIP 011-1 into multiple standards	(38)	31.9 %
No preference-	(23)	19.3 %
Not checked -	(10)	8.4 %
Total:	(119)	100

Keep CIP 011-1 as one Document- Comment Topics

1. Better Organization and Organizational Review *(8 comments)*
2. Auditing and Multiple Violations of Single Standard *(6 comments)*
3. Format *(2 comments)*
4. Table Format *(1 comment)*
5. Revisions *(1comment)*
6. Alignment with Other Standards *(1comment)*

Break up CIP 011-1 into Multiple Standards- Comment Topics

1. Retain CIP-003-009 Format *(10 comments)*
2. Audit/Enforcement/Compliance and Negative Perceptions *(9 comments)*
3. Suggested Standard Format Combinations *(8 comments)*
4. Level of Effort and Cost of Changing Format *(6 comments)*
5. Use Functional Areas *(3 comments)*
6. Consistency with Other Industry Cyber Protection Standards *(2 comments)*
7. Makes Easier Ownership Assignment and Referencing *(1 comment)*
8. Monitoring Changes *(1 comment)*
9. Aids the Revision Process *(1 comment)*
10. Focus on Security *(1 comment)*
11. Approve as a Complete Set *(1 comment)*
12. CIP Standards Should Stand Alone *(1 comment)*

No Preference or Not Checked- Comment Topics

1. Implementation, Updates and Revisions *(4 comments)*
2. Focus on Defining Auditable Requirements *(3 comments)*
3. Reporting at a Requirement Level *(2comments)*
4. Simpler Management *(2 comments)*
5. Table Format *(1comment)*

Stu Langton reviewed with the SDT four key comments *(see below)* noting EEI and APPA represent approximately 60% of the industry. What are their arguments? Ameren suggests it will be easier to find requirements in one standard and use. EEI argued for the legacy of CIP-003-009 or at least a way similar to it as being easier for the industry to recognize and preserve sunk costs. APPA suggested sub-headings in CIP-011 are illustrative of the need to separate into multiple standards and that multiple standards would be simpler to work with and revise in the future. IRC suggested functional areas with each standard being a stand-alone. The discussion of these comments covered issues related to Compliance Enforcement and Reporting.

The facilitators initially suggested first taking a straw poll on which of the two formats members favored then ask members for propose a motion on the format. The straw poll resulted in 10 members favoring multiple standards (CIP-011 to CIP-021) based on the eleven sections of the CIP-011 standard, and 9 members favoring the one standard format of CIP-011. Following this there was a motion (Doug Johnson, second by John Lim) to adopt multiple standards (CIP-011 to CIP-021) resulting in 11 yeas (61%) and 7 nays (39%). The facilitators suggested revisiting this question at a later point noting the sentiment on the Team has appeared to shift in favor of multiple standards for CIP-011, but it fell short of the 75% needed to make a SDT decision on this question.

John Van Boxtel provided an initial presentation on a possible improvement in the format utilized for definition of the CIP-011 standard. He provided an overview of the standard format used by PCI (DSS standard format).

The facilitators reviewed the process for reviewing the group reports which presented summaries of the industry comments for each of the 54 questions in the Comment Form. He noted that he wants each sub-team to help ensure that we have identified the right issues and determine who needs to address them.

Phil Huff reviewed with the Team the responses to Question #54. There included comments on clarity or wording; on definitions especially hourly: moving definitions to NERC glossary, appreciate local definitions, separate attachment for all local definitions; timing issues; implementation plan –about “gap” in compliance programs, sufficient time for categorization, CIP-010 may require more time; categorization issues; consistency issues.

Phil Huff provided the overview for Question #53 including 66 comments, with 57 specific comments addressing: TFEs (passwords, malicious code, appropriate use, system hardening, security event monitoring, wireless and remote address, communication and date integrity) device characteristics, write clear requirements, and TFE process improvements.

John Lim provided the overview of industry comments for CIP-010 focusing on three questions: #1 – definitions, #6 – the Attachment 1 functions, and #7 – Attachment 2 categorization of BES cyber assets. Jim Fletcher presented a summary of the industry responses for question #6 with 58% of industry agreeing but suggesting the attachments need more definition, examples, and guidance especially in Attachment 1.

Rod Hardiman presented a summary of the industry responses to Question #7 including that 75% of the respondents disagree.

Dave Revill introduced his Sub-team's work noting it covered Questions 11 on Security Governance and Policy, and Questions #40-48. Question #47 on BES Cyber System maintenance included concerns about the interaction between the list of personnel in Table 26.1 and the lists granting authorized electronic and physical access; about the interaction with other user/account management requirements; regarding the allowance for emergency maintenance situations; requirements on maintenance devices should include system hardening; all maintenance devices should be documented in a list; and Ensure that systems used for maintenance do not act as an unauthorized access point. He noted they also received comments on the definition of "maintenance" – some said to consider that any temporary connection also have appropriate controls.

Sharon Edwards presented the following summary of industry comments on Question 17, Electronic Access control which included: Need a strategy for designing baselines by impact levels – we missed the mark; revocation of access – do not like the time parameters for revocation, transferred personnel should not be treated as risk, and clarify when the clock starts for no longer needing the access plus a distinction should be made in the standard between "primary" access and "secondary" access; clarity and definitions on acceptable use, account types, system access, remote access, external connectivity, wireless, etc.; separate remote and wireless access; consistency; and quarterly review is excessive.

Scott Rosenberg presented the overview of industry comments on response and recovery including: Guidance on cyber security incident classification highlighted; Definitions; Incident response for low impact or non routable connections should be removed; Consistency between requirements related to impact level; Single versus multiple incident response plans and testing issues; Combine incident response testing and review/update; Review results of incident response tests in other than 60 days; Recovery testing; Data retention identification requirements of personnel responsible; Coordination of physical aspects of cyber security incidents; Incident response and recovery plan reviews and question around changes required; Suggestions for re-wording; and Coordination of backup plans.

Jay Cribb noted and summarized the industry responses to System Security Questions #35-39 which covered more than 100 pages and addressed: malware prevention; patch management; system hardening; data and communications integrity; boundary protection and system boundary; and protective systems.

Doug Johnson presented the summary of industry comments on personnel and physical security including Question #12, R2, R3 R4, R5 and R6.

On Thursday the Team took up how to address FERC Order 706 issues that have been termed "post Version 4 issues" that include:

- Access Control Redundancy/~~Defense in Depth~~ (two or more diverse security measures in constructing electronic and physical security perimeter)
- Active vulnerability assessments every three years
- Forensic data collection

The Team agreed that it will take time to address these issues, but they should be included in the provisions of CIP-010 and CIP-011 if the SDT has some more time to complete the task. The SDT agreed they need to reach out to experts for assistance (e.g., Carnegie Mellon on Forensics) and increase the two-way communication concerning what FERC is asking for, i.e., the intent of the request. Jan Bargen, FERC, noted her understanding is that you do not have cyber security if you do not have security in-depth – too severe an interpretation that it has to be all or nothing and cannot been done in pieces – you can explain progress and point to it in the requirements and note what else needs to be worked on – recognize you are working on a new paradigm and have a window of opportunity.

Scott Mix presented the implementation plan concepts and approach. The Team asked him to develop and present options for proceeding.

On Thursday, Scott Mix offered the following Implementation Plan options for the SDT's consideration and consensus testing was performed on the options by the SDT:

1. Multiple fixed dates (based on connectivity and dependent on impact level)
   4 -6; 3 -8; 2 -5; 1-0 = **58 (3.2 of 4)**

2. Entity-specific implementation plan
   a. need to develop boundaries and approval guidance
   b. resource issues at regions for approving plans
   c. multiple versions in play at the same time for audits
   d. will require "true-up" of CIP 011 requirements for connectivity, etc.
   e. consistent with current NGP plans
   4 -3; 3 -11; 2 -4; 1 -1 = **54 (2.8 of 4)**

3. Single fixed date (independent of impact level)
   4 -4; 3 -9; 2 -3; 1 -2 = **51 (2.8 of 4)**

4. Fixed date for each requirement, for each impact level
   a. some requirements would be the same for all levels
   b. may have issues with "early compliance"
   c. will require a separate plan for NGP
   4 -0; 3 -1; 2 -14; 1 -4 = **35 (1.8 of 4)**

The Team discussed the low impact baseline and how to provide more detail in the standard including featuring the baseline in each table for each requirement.

Following the Sacramento meeting it was agreed there would be a need for weekly sub-team meetings and possible sub-team leads meetings. Later in June the schedule would be adjusted to reflect this and include some SDT meetings to develop drafts for NERC staff to review in advance of the July meeting in Pittsburgh. The Chair suggested convening the SDT to review a new draft schedule the following week once more information was available from NERC and the Standards Committee.

The Chair thanked SMUD and especially Kevin Sherlin for his excellent support for the SDT in hosting this meeting.

The meeting adjourned at 11:00 p.m. on Friday, June 11, 2010

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

23RD MEETING SUMMARY

Cyber Security Order 706 SDT — Project 2008-06
June 8-11, 2010
Sacramento, CA

I. AGENDA REVIEW, SDT WORKPLAN AND CONSENSUS PROCEDURES

A. Meeting Objectives and Agenda Review

On Tuesday morning, the Chair, John Lim welcomed the members to the SDT's 23rd meeting. Joe Bucciero conducted a roll call of members and participants in the room and on the conference call *(See Appendix #2*). The host Kevin Sherlin, a SDT member, welcomed everyone to the Sacramento, California SMUD meeting facilities and covered logistics.

Mr. Bucciero reviewed the need to comply with NERC's Antitrust Guidelines *(See Appendix #3).* He urged the team and other participants in the process to carefully review the guidelines as they would cover all participants and observers. He urged all to avoid behaviors or appearance that would be anti-competitive nature and also reminded the group of the sensitive nature of the information under discussion.

The Chair reviewed the following proposed meeting objectives:

- To review the CSO 706 SDT 2010 Work plan and Schedule;
- To review and adopt CSO 706 SDT 2010 Consensus Procedures draft;
- To receive updates on other related cyber security initiatives;
- To review the results of the FERC/NERC May 27 Meeting;
- To review the results of the May 19-20 Dallas Technical Workshop;
- To review the documents to be produced for the July, 2010 CIP posting;
- To receive an overview of the industry informal comments on CIP 010 and 011;
- To review industry input on the CIP format and to test SDT consensus on CIP format going forward;
- Sub-teams review industry input from the Technical Workshop and informal comments and propose any potential changes in the draft standards;
- SDT reviews Sub-Team reports on industry input from workshop and informal comments and any proposed changes in the draft standards;
- To review progress on the Implementation Plan Drafting Group and the Guidance Document Drafting Group; and
- To agree on next steps and assignments

Bob Jones, facilitator, reviewed the proposed timed meeting agenda *(See appendix #1*). On Thursday morning the SDT approved without objection the meeting summary for the May 11-13, 2010 SDT session in Dallas, Texas.

B. Related Cyber Initiatives

Keith Stouffer, an SDT member, noted the release in the next couple of weeks of a new draft from NIST committee. Scott Rosenberger noted that Cyberstorm-3 will be taking place in the Fall of 2010 and they are looking again for volunteers. John Van Boxtel noted that there is a concern that the result is already pre-determined. Gerry Freese suggested that even if it is pre-determined it is a good experience for people to better understand circumstances.

C. Review and Adoption of Revised SDT Consensus Procedures

At the Dallas SDT meeting, the Team reviewed some proposals for updating the consensus procedures originally adopted by the Team in November, 2008. At the conclusion of the discussion, the Chair asked John Van Boxtel and Bill Winters to serve as a drafting team and address the email voting procedure.

Mr. Van Boxtel reviewed the proposed addition of an electronic voting section with the Team *(See Appendix #5)*. He noted it was narrowly designed to address those instances where the SDT could not secure a quorum for a face-to-face or conference call and "will not be used to decide on issues that would require a super majority vote or have been previously voted on during a regular meeting or for any issues that those with opposing views would feel compelled to want to justify and explain their position to other team members prior to a vote."

The Team agreed to deleting the section "Posting of Industry Comment" as it would only apply to informal industry comment postings and agreed to extend the time for decision in the email vote procedure from 4 to 12 hours.

Jon Van Boxtel made a motion which Dave Norton seconded to adopt the proposed revisions. The motion passed with 17 yeas and 1 nay. Dave Revill noted his concern was that the procedure was too narrow in that it did not allow electronic vote for posting documents for comments or ballot.

II. REVIEWING THE CSO 706 SDT PROCESS AND SCHEDULE

A. Initial SDT Workplan Review

The SDT reviewed and discussed the schedule and work plan at several points during the Sacramento meeting. On Tuesday there was a discussion generally on the current plan that the Team adopted in May, 2010 to complete work and post for formal comment CIP 010 and 011 at the conclusion of the Pittsburgh meeting in July, 2010 (*See Appendix #4).*

Members and Participants Discussion Comments

- Are we talking about from now until early July to have weekly meetings? FERC recognized our schedule is ambitious. Before the SDT last posting in April the time crunch pushed members to vote yes even thought they still had questions and concerns to address and resolve.
- Jan Bargen, FERC, noted that the work plan schedule is aggressive and that FERC staff is interested in a quality product that represents the next cyber security paradigm for the industry and addresses the directives. Perhaps at the end of this meeting, the SDT needs to assess if they can get there or not – assess what it can do in the time – or express what could be done by when. Between now and the formal posting is the best time to improve the product.
- Mike Keene, FERC, noted that FERC staff would prefer a better product later than meeting a self imposed deadline – they would rather wait six months if necessary to get a quality result to review.
- NERC staff noted that NERC President Gerry Cauley has "put a stake in the ground" that the SDT, NERC and the industry will have a cyber security product approved by industry to present to FERC by the end of 2010 that would indicate the progress the industry is making in this area.
- NERC put in that schedule – if we could change President Cauley's mind, how could we get an extension of time without a new order?
- In the Short term between now and Pittsburgh there are 38 business days.

B. Proposed Revised Schedule

Phil Huff presented a draft schedule for the next four weeks to complete its work in Pittsburgh and file the CIP 010 and CIP 011 for formal comment and balloting. He noted the necessary deliverables including: CIP 010 and 011 standards/requirements; VSL's, measures, guidance document; FERC directives summary; CIP version 3 mapping; informal comment summary; and comment form for the formal comment posting.

Member Comments

- This is unrealistic – initial revisions of the requirements by the Sub-teams to NERC staff by end of next Tuesday? Then one week to compete?
- We haven't fully documented the industry informal comments to be addressed and only two days for meeting and finish, two days not already on our calendars – this is not ambitious, it is impossible.
- If Tuesday is unrealistic can the Sub-teams target of COB on Friday of the following week for revisions to requirements but send as they become available to Howard with June 18th deadline to complete all revisions?

Difficult to get this done if different sub teams are on different pages – how do we get the whole SDT onto the same page. We can get material out but are we trying to get this right?

- In addition, there are several cross and coordinating issues that have not been addressed and these may not possible to work out by next Friday.

Bob Jones summarized the context for the schedule which the Team had discussed noting the possibility of two rounds instead of three and using the additional time to improve product. Stu Langton reviewed the dynamic current political context and the felt need to demonstrate that the industry can produce a good product in a reasonable amount of time. However, as the Team has discussed, once it sends the standard out for the first ballot they will lose flexibility in making changes.

Member and Participant Discussion Comments

- If the SDT turns out a product industry cannot live with they will vote it down – the Team needs time to get it right than get it out sooner but wrong – lot of frustration that process will result in a changes that will not bring security and increase compliance problems.
- This has to be right. We can't allow ourselves to be beat into submission by politicos who do not understand the cyber security system – we are industry volunteers with real jobs.
- In light of the substantial level of informal comments, we can imagine the time needed in the formal comment phase and we have to respond to each comment.
- Can the July posting be another informal so we can address without responding to every single one?
- Want to propose the Team changes the deadline – sub-team leads can meet over lunch to determine how much additional time is needed?
- In the industry, if we know we cannot hit deadline with a good product, we change the deadline and add resources. Can the SDT get others (NERC staff) to review and compile the comments?
- Not sure clerks could have done the job – we have a window to get it right – the proposed schedule is too brittle and short and will not allow us to create a quality product. We should not live with a schedule dictated to us or have others determine what is the time needed. NERC executives do not fully understand the situation.
- Jan Bargen, FERC staff, noted that at the May 27th FERC meeting, FERC staff expressed concern that we need a quality product. The deadline at the end of the year is not being imposed by FERC.
- There is consensus in the room for a new deadline that provides for more time to get it right.
- We need to be careful and keep our focus is on reliability of the BES – not serving the industry with a less than quality product. It is not serving industry to remove an opportunity for comments – only two balloting periods is not realistic given the substantive change reflected in CIP 010 and 011.

- We need a motion to request a new deadline from NERC.

C. Standards Committee Input

It was noted that the Standards Committee was meeting concurrent with the SDT's Tuesday morning discussion. Howard Gugel was on that call and will bring back information. Might be wise to give him a chance to fill in context before moving forward. The Chair noted that if the SDT requests an extension, we will need to give an alternative schedule saying what we think it will take to get it done and by when. Phil Huff proposed meeting with the Sub-Team leads over lunch to discuss possible ideas for alternative schedule.

Following lunch, Howard Gugel reported to the Team on the Standards Committee call. He noted that NERC President Gerry Cauley and Standards Committee Chair Alan Mosher felt strongly a need to present some cyber security standards changes to for FERC and for Congress by the end of the year. CEOs in the industry have expressed concern that CIP 010 and 011 may not pass by end of the year and that there may be a need for a "Plan B" which might take 010 with high and medium bright lines and then add CIP 003-009 as is. Jason Marshall noted the President Cauley focused on responding to Congress.

Member Discussion Points

- This idea is to present "something" by end of year? Posted and balloted or just making progress?
- This is "something approved by industry to show Congress and FERC of progress being made.
- Does NERC have a plan B to finish this work or this team being asked to prepare a plan B? It is not clear.
- "Something" that meets deadline that also meets industry and Congressional concerns?
- Plan B may refer to perception on the Hill that industry has not responded to their concerns – such a plan may kick in after first ballot if the first ballot indicates an unreasonably low level of acceptance and low expectation of passage.
- There has not been much discussion of how 706 directives will be addressed by this "Plan B"-- 010 with CIP 003-009 package.
- The "Plan B" approach may be doable and can address 706 which points out what to address in the existing structure.
- We should consider a motion to draft a letter to NERC requesting an extension.

D. Sub-Team Leads Review of Schedule Needs and Review of Options

Phil Huff reported on the Sub-team leads lunch discussion re schedule adjustments – think complete revisions based on comments by July, push formal posting until after August – it is not feasible to post prior to August 20th – also assumes support from NERC staff for drafting and adjust membership on some sub teams – leadership talk to standards committee and NERC management to seek pushing posting back 31 days from the current plan which would mean in Chicago in August. The end of year deadline depends on the level of industry acceptance in formal posting and ballots.

After discussion about the time frame and content the facilitators suggested a straw poll on different extensions of time assuming the same SDT monthly meeting schedule and interim conference calls and assuming addressing all FERC directives including the "Post Version 4" directives. Members expressed their preferences among one of three options. Each option included the 38 days to the Pittsburgh meeting plus:

- **Option A.:** adding 30 more days to the SDT Chicago meeting-August 10-13 (Sub-team leads proposal) then to initial ballot – **2 members**.
- **Option B:** adding 60 more days to Winnepeg, September 7-10 SDT meeting, September and then to initial ballot – **8 members.**
- **Option C**- adding 90 more days to the SDT Toronto October 12-15 meeting- October and then to initial ballot – **12 members.**

SDT Discussion of Straw Poll

- Jay Cribb's issues may have an underlying problem of agreement that time alone may not address. May need to consider a change the members in the group to facilitate development of the requirements.
- Need a clearer rationale. E.g. discovery that industry is concerned abuot the post v4 issues discussed earlier which FERC has directed NERC to address.
- This is a request to extend time when the first formal posting takes place. We need time and full meeting to address comments and refine draft requirements.
- Also discussed shuffling to share the work load among the teams
- Feel 31 days is too short – need time to discuss and then develop guidance too – I can give another week in this month but not more – I think we need at least two more face to face meetings.
- June 2011 for end (a six month extension). If you go to the well, better be sure we get enough water.
- Assume that all of these options include a request for additional help from NERC. We can request it, but we may not get it

Following this, John Van Boxtel proposed the following motion, with Doug Johnson as a second.

> **1st Motion:** "Due to the amount of work remaining, and the need to send a quality product out to the industry to gain acceptance of the new standard, the SDT should compose a letter to the Standards Committee and key NERC staff asking for additional time to be added to the schedule to develop the CIP 010 and CIP 011 standards."

SDT Discussion Motion #1

- We need to state exactly what we are asking for – need team agreement on the time we are requesting and then add to the motion Concerned about only 31 days – not sure what we need but the schedule is tight and brittle – need to ask for more time, how much is still open but needs to be answered before sending the letter – industry comments suggest a lot of work.

- John noted he was amenable to a specific time frame being added to the motion.

Revised Motion #1: Based on the results of industry feedback from the informal comment period, the desire to address the FERC 706 directives (including the former post Version 4 issues), and the need to send a quality product out to the industry to gain acceptance of the new standard, the SDT should compose a letter to the Standards Committee and key NERC staff identifying these issues and ask for an extension for the posting of the CIP draft standards in October 2010 to be added to the schedule to develop the 010 and 011

Discussion of 1st Revised Motion #1

- Concerned about putting in "706" reference without saying "fully address" – okay with post v4 issues.
- Suggest putting such details in the letter to be drafted if motion passes.
- Not comfortable with the parenthetical related to post version 4 issues –this was covered by "fully address all"
- Question is the end date – asking for an end date to deliver to FERC?
- However, the end date is not in your control – discussion is how much time will it take the SDT to get to first formal posting.
- Asking Standards Commission for permission will get a "no". We should advise them we need more time and move forward with that schedule unless we hear otherwise from the Committee.
- Writing a letter starts a conversation – need communication between our leaders and NERC management – also need more resources to support volunteer effort – just agree to ask our leaders to seek extension from management to assure quality product.
- The Chair and Vice Chair have a conference call Friday morning with Standards Committee Chair. They need guidance on how much time we need – 90 days to complete the work in front of them based on comments and input from FERC – more staff is not the issue.
- Possible scenario – ask for more time for 010 and 011 and they go with plan B of 010 and CIP 003-009 for balloting process.
- Plan B would be voted down
- The scenario doesn't make sense – if we are struggling, the industry will not understand that plan B proposal.
- How much time will it take us to responsibly post for formal comment?
- Plan B will take it out of the hands of the drafting team/
- The more time we ask for, the more likely it is to be denied and taken away to assign plan B to be developed elsewhere.

John Van Boxtel (and Doug Johnson as a second) agreed to the following in light of the discussion as friendly amendments:

2nd Revised Motion #1: Based on the results of industry feedback from the informal comment period, and the need to send a quality product out to the industry to gain acceptance

of the new standard, the SDT should compose a letter to the Standards Committee and key NERC staff identifying these issues and ask for an extension for the posting of the CIP draft standards in October 2010 to be added to the schedule to develop the 010 and 011

Vote on the motion above to adopt the motion: 11 yea – 5 nay (69%)

Bob Jones suggested that the SDT is unanimous that it needs more time to do a quality job based on the industry comments, 706 directives and FERC comments. The Chair thanked the Team and suggested the Chair and Vice Chair would take this as guidance in their discussion on Friday morning with the Chair of the Standards Committee.

E. Discussion of Further Input from the Standards Committee Chair

On early Friday morning, John Lim and Phil Huff reported to the SDT on a conference with the chair of the Standards Committee, Alan Mosher. They discussed with him the time and schedule and the Standards Committee was agreeable to a 90 day extension to complete the CIP 011 work if there could be a 010 product going out to industry in July. Mr. Mosher requested the SDT create a schedule for moving forward with both 010 and 011 and suggested that in the interim between implementation of 010 and 011 that the SDT use an amended 002 to address the issue of critical assets. Phil noted they raised the remaining 706 directives and Mr. Mosher understood the difficulty getting both out by end of year but expressed the need for something by end of year if not the full package.

Member Comments on Standards Committee Call

- Confusing to throw out 010 without 011. We must be careful how we do it
- In terms of the implementation of the 010 and 011, we can't just put out 010 and attach CIP 003-009 – effectiveness of 010 comes from 011
- The modification of 002 will include what? Not sure but looking for something to use before effective date of implementation of CIP 010 and 011. Perhaps something to give bright line of critical assets – not sure how that works well given limited time – details still need to be worked out – entities may be concerned with using one set and then implementing another soon after this.
- Disappointed that NERC and the Standards Committee don't understand the situation. An interim change as a bridge may be another chase down a rabbit hole.
- This is essentially plan B
- The SDT needs to focus and not be distracted by political expediency – add ninety days and six more months
- We do not have to work on the 002 option – this is what they will be doing while we try to complete our work – this is the reality – while recognizing the technical difficulties – we do not work in a vacuum.
- We will be held accountable for technical shortfall pushed by politics – we need to keep 010 and 011 connected to avoid confusion.

- Keep in mind industry feedback – industry confused when 010 put out first time without support – putting medium up to high protections brings a ton of facilities and may cause further confusion if we are not careful
- We have not been assigned to amend 002 – we move forward on our own – that is a parallel path – meanwhile we get more time with ninety day extension – need to make use of that time – this team still engaged and owning its product.
- This was informal discussion with the Standards Committee Chair. He asked to come back with a formal schedule. We need to say can not meet end of year and offer an alternative that includes getting something out by end of year
- We are still operating under the original order which did not have a timeline – now the Standards Committee is imposing a timeline – this may be a fundamental change in the original charter – we will be held accountable for the final product – if they want us to meet a timeline then put it out to the public and we can react.
- We do not have to rush to get revised schedule out
- What do we do starting next Monday? What is the revised work plan? When is the next deadline for product?
- The Standards Committee has to drive this while we continue to work on CIP 010 and 011.
- We need to keep working at our pace to get job done – the short schedule proposed yesterday is not reasonable.
- That schedule is not workable nor feasible.
- We need to know if 010 is being decoupled from 011 – this is not a good idea but it does impact our work plan. Do we just guess? If decoupled and 010 has to go out in July then focus on 010 at a different pace.
- Industry said last time they wanted a whole package to react to – waste resources on splitting up – need one unit – we do the right thing – if they want something else then let them do it – we need to look back with pride on our product
- Start Monday with addressing industry comments and get to NERC by next Friday
- We need a sequencing calendar of the next few weeks leading to Pittsburgh and then to Chicago and communicate it to members soon to guide their work.
- We have comments that we need to process with requirements we have – get output to NERC for them to work with starting the end of next week for them to review – it is not the final product – hopefully by then we have more clarity on the schedule – yesterday 90 days seemed acceptable to the team.
- Plan B is not our problem, we still have charter to fill.
- Jan Bargen, FERC noted that FERC was concerned in January about splitting 002 from CIP 003-009 and industry was too. However things are different now. If 010 proceeded first, it could be filed later with CIP 011 and this also might give industry more time to consider impacts and coverage.
- Howard Gugel, NERC staff, recommended that the SDT should think of this as staggering the work vs. “decoupling.” Get CIP 010 out then CIP 011 later with overlap in the comment period – also staggers the work load of responding to formal comments

– before no one knew what 011 would look like, now the industry has an idea what to anticipate now - also allows more full group review.

- Final filing does not have to be staggered and would include implementation plan – already a stagger between 010 and 011 since you have to do 010 first to then implement 011.
- I think we can move to ninety day and understand that a separate tiger team may be ready to go on CIP 002 amendment. Our team cannot provide guidance to the NERC tiger team on our draft by next week. We are not even done compiling and reviewing comments
- What if tiger team at NERC scrubs for consistency then drafts initial VSLs, measures etc. – addresses issues we discussed yesterday as a base for Sub-teams to begin addressing the comments. This can also handle the grammar and structure and work from what you have already identified.
- Won't be hard to add lines to tables – send any concepts for us to put in draft and get you started.
- Phil Huff reviewed with each of the Sub-teams where each were in summarizing the comments. Three teams are still working on summaries while others have identified key issues. None have moved on to consider how to address the comments in changes to the requirements. He noted that there was a possibility, if needed, to split up Jay Cribb's team into two sub-teams (005 and 007) and he would consult with Jay and other team members before a decision was made.
- Following the morning call with the Standards Committee leadership, the SDT chair and vice chair would schedule a SDT meeting to discuss a proposed new schedule.

III. REVIEWING INDUSTRY AND FERC COMMENTS ON CIP 010 & 011

A. Overview of Industry Input

Bob Jones reviewed the documents compiled for the SDT's review of industry comments. He summarized an overall set of results showing the percentage of support or opposition for key components and questions. *(See, Appendix #10).* Scott Mix had sent out over the weekend a "consideration of comments" document that included over 900 pages.

The Chair noted that the Team received a significant amount of input from the industry and FERC since the posting and the SDT will need to review and consider what kinds of revisions may be needed for the CIP 010 and 011 requirements based on these comments and the SDT's continuing development of the CIP. He noted that the next phase will include a pre-ballot review followed by formal ballot and underscored the point that there is a a lot of work ahead of SDT. The comment period closed on June 3 which did not give the SDT much time to review prior to the Sacramento meeting. The SDT will need to rely on and trust that Sub-Teams will work to address the comments and share with the full SDT their summary of those comments.

Member Comments

- What do the percentages actually tell us?
- One vote could represent more than one individual or company
- Many may have disagreed but only wanted to tweak one or two words
- I stressed that respondents should provide constructive suggestions. Comments like "I don't like it" doesn't carry much weight without a suggestion for improvement.
- We can say we understand their concern, address it, include it, or explain why we keep it the same.
- We will publish a summary of comments and responses.
- Can we change the responses to substantially agree with and substantially disagree with to more accurately reflect responses?
- Yes, in future comment questions we can frame it that way.
- Can we use a 4-3-2-1 next time to gauge the level of concern – we may have gotten a ton of "3's" with minor concerns instead of "disagree"
- The percentages are based on the checked boxes – not a qualitative assessment of the responses.
- I most concerned where the percentages are close to even. These are where we need to understand the concern and address them as a group.
- Physical security section may be an indication of desire to move into a separate section

- We were told not to be prescriptive but many response comments asked for more prescription to clarify.
- System security put R15-19 together – may require more work to separate out the comments per requirement – may also account for low percentages for "agree"

B. "Parking Lot" Issues Raised by the SDT in the Development of the Draft 010 and 011

The Team has maintained an ongoing "parking lot" a table list of issues raised in the course of the development and discussion of CIP 010 and 011 and as the SDT is reviewing the industry comments. These were presented and discussed by the Team and a table setting these issues out and how they were or will be resolved or handled going forward is included as an appendix to this summary *(See, Appendix #7)*

C. Review of May 27 FERC/NERC Meeting

Joe Buchierro provided the SDT with an overview of the meeting summary distributed to the SDT members (*See, Appendix #6).* John Lim noted that the atmosphere for the meeting was cordial and professional, and the meeting brought forth constructive input and ideas. In general, FERC staff agreed with the approach taken in the draft CIP-010 and CIP-011 standards, but acknowledged that a lot of work is still needed in clearly defining the requirements. Joe noted that FERC staff expressed the following issues and concerns:

- The Low impact level requirements are insufficient and need to be bolstered, i.e. the Low baseline is too low.
- The proposed 36-month review of the categorization needs to be shortened, at least for the first review cycle (possibly to 12 months).
- Beware of hidden requirements in the purpose statements of the requirements, and review with the intent to minimize the adjectives used in the text (e.g., sufficient, proper, adequate, etc.) and clarify what is required with respect to auditability and enforceability.
- The bright line thresholds stated in Attachment II need to be justified or at least explained.
- The SDT must ensure that all of the requirements are auditable.
- Concern was expressed on the deferring of some FERC directives until next year.

FERC staff recognizes that the schedule of the project is ambitious, and appreciates the significant effort being performed by the SDT in creating these standards. Jan Bargen, FERC, noted that they recognize the considerable amount of work of the SDT so far, but believes there is still more to be done including both the justification and baseline issues – e.g. how do you talk about the minimum, are we moving forward if more of the electric system is not covered, need to explain why is this better. There are too many items not currently included. What else is being brought in to the new standards? Is the baseline for protection of BES equipment set at the right level.

Member Comments

- **Immediate revocation.** There was also discussion of the "immediate revocation" issues – how can that be defined to allow for prompt but effective responses and which items may not rise to immediate level?
- **Low Impacts.** Is low is too low? What does that mean and how do we set it? What is the rationale?
- There is a worry that something will fall through since the low has few requirements.
- Take input and address where appropriate – do not necessarily need more requirements – FERC staff is speaking as staff, not for the commission – treat as part of the informal comment period
- Regulators are not happy with the level of coverage now. Are they asking for every asset to be covered?
- Mike Keene, FERC noted that it is not the amount of equipment but does the low have enough protection for the low equipment – some level of protection for low equipment, not just blank
- Jan Bargen, FERC, asked if there are not requirements does that mean it does not need any protection? Then the baseline may look like there is no protection where you find blanks in the tables.
- All these discussions must be couched with "in relation to what?" What are we defending against? Everything against anything?
- FERC is trying to prompt us to look at the watt levels, etc., not just the H-M-L categories – looking for measurable standards.
- Concerned about having to create lists of low for audits – need to demonstrate you have a security program rather than a site-by-site list for purposes of audits.
- We are doing something for the low categories but this may not need to be a list subject to fines – we are doing something to protect or we wouldn't be in business.
- Mike Keene, FERC, noted that policies or procedures for low impact would be a good approach.
- **Physical Security.** Things are being done for the low but the SDT may want to think about moving physical security out into its own standard. There may be no way to marry our process with adequate protection of physical assets – we have discussed this as a team but we may need to revisit.
- Question of audits for physical security – there is a level of security for those but we do not want them brought into the meticulous audit process of today – this has been a big stumbling block for many members of this team.

Bright lines

- Need to be sure the numbers we use and how we arrived at those numbers are understood by a wider audience.
- Mike Keene, FERC, noted that FERC staff wondered about the "bright line issue" that distinguished medium and high – are they in the correct spot? Not as concerned with the low.
- **Avoid the prescriptive (how).** Clarify the standard but do not be prescriptive – identify the program and what it covers – identify what needs to be covered but not necessarily "how" to cover them – must have a documented program that covers these assets.

D. Review of Dallas Workshop Process and Results

The Chair noted that this was the first time NERC has used such a workshop in the context of a standards development process and any lessons learned would be helpful for NERC to consider. He suggested there was a good industry turnout for the workshop and some excellent questions were raised and suggestions offered that the SDT should consider going forward. He expressed surprise that during the interactive open session on day that only a limited number of people stepped up. He asked what other members thought of the workshops and the following points were offered for improvements on the process:

- The highly structured questions on day one limited the interactivity.
- That is why on day two we offered an open mike session to offer the opportunity for that interaction.
- Ideally, it would have been better to have scheduled the workshop a few weeks before so that participants could process the workshop results and prepare their comments on the posting.
- Should consider allowing for break out sessions next time to encourage more interactive discussions.
- Need to think about how to clarify what are the objectives of such a workshop. Some participants may have perceived that "this was a done deal, this is how it is, and there was no need to make comments."

E. Review of the SDT's Full and Sub-Team Process for Considering Industry Comments

The Chair proposed that the Sub-teams meet to review and summarize industry comments and report back to the full SDT.

Member Comments on Proposal

- Concerned letting sub teams review comments without full group review
- Wonder if breaking into sub-teams is still doing us any good – better to look at as a full group – may be slower but addresses the overlaps with the diversity of the full group.
- Bob Jones noted the Chair's proposal is not to look at how to respond but intended to enhance the full team discussion – attempting to make the most of the limited time with the scope of the complex task. He offered as an example of the challenge of summarizing th industry comments by looking at question 9 on format since it is not part of any sub-team. *(See Section F, Format below)* and tried to provide and organize the comments by topic. This suggests that the SDT will have to go through each industry comment and 900+ pages as a full group. The full SDT will have a chance to review and provide guidance on possible revisions. This will be enhance by an initial effort to summarize and not have to repetitively review similar comments.
- Good approach –but remain bothered anytime agenda says break into groups. The schedule is wagging the dog here. We should just do the best job we can then take our lumps.

- Concerned we did not get a full chance to review in full team the sub team work before this last cycle of review.
- Splitting up work can be good and efficient, but we need to do our work prior to coming to these meetings in order to use our time together most effectively – feel like we come to class without doing our homework first
- Note that in the Version 1 SDT we also broke up to write standards but then spent hours on the phone reviewing every word of the first set of standards at the end.
- We need to spend our time here to do that and use conference calls to do homework and prepare for in person discussions
- Just as a note, we have not been able to get the "homework" done prior to the in person meeting – sub groups between meetings successful about 50% of the time – requires a level of commitment to get work done prior to coming together to create products we can use – in this case there was no time to work on prior to this meeting so we need to take some time now to do that so we can then review together – have to do the pre-processing today and tomorrow – group the comments together by topics and frequency, do not decide what to do with them yet – then use final day and a half to review as a group
- Support the ideal process of using in person time together but having to deal with the comments on short turn around as JL pointed out – we did not have enough time from close of comment period to allow for processing – in July we need to be sure we have a product ready to make the best use of in person time
- In July we may also have some initial vetting by NERC – also note there are other items that need to be added for the formal posting such as measures
- Use the sub team time now to organize comments for full group review?

F. Review of Industry Input on CIP Format (Question #9)

1. Overview of Industry Format Reponses

Bob Jones presented an overview of Industry responses for Question 9 (*See, Appendix 8)*: *Do you prefer the currently proposed format for CIP-011-1, which contains a complete single set of requirements? Do you prefer the alternate format, where the requirements are grouped in separate standards? Or do you have no preference?*

CIP 011 COMBINED REQUIREMENTS FORMAT

	Totals	***%***
Keep CIP 011-1 as one document-	(48)	40.3 %
Break CIP 011-1 into multiple standards	(38)	31.9 %
No preference-	(23)	19.3 %
Not checked -	(10)	8.4 %
Total:	**(119)**	**100**

Keep CIP 011-1 as one Document- Comment Topics

1. Better Organization and Organizational Review *(8 comments)*

2. Auditing and Multiple Violations of Single Standard. *(6 comments)*
3. Format *(2 comments)*
4. Table Format *(1 comment)*
5. Revisions *(1 comment)*
6. Alignment with Other Standards *(1 comment)*

Break up CIP 011-1 into Multiple Standards- Comment Topics
1. Retain CIP 003-009 Format *(10 comments)*
2. Audit/Enforcement/Compliance and Negative Perceptions *(9 comments)*
3. Suggested Standard Format Combinations *(8 comments)*
4. Level of Effort and Cost of Changing Format *(6 comments)*
5. Use Functional Areas *(3 comments)*
6. Consistency with Other Industry Cyber Protection Standards *(2 comments)*
7. Makes Easier Ownership Assignment and Referencing *(1 comment)*
8. Monitoring Changes *(1 comment)*
9. Aids the Revision Process *(1 comment)*
10. Focus on Security *(1 comment)*
11. Approve as a Complete Set *(1 comment)*
12. CIP Standards Should Stand Alone *(1 comment)*

No Preference or Not Checked- Comment Topics
1. Implementation, Updates and Revisions *(4 comments)*
2. Focus on Defining Auditable Requirements. *(3 comments)*
3. Reporting at a Requirement Level *(2comments)*
4. Simpler Management *(2 comments)*
5. Table Format *(1comment)*

Member Discussion of Format Comments
- The industry is even more split than the team with no strong preference for either format – suggest leaving it as proposed given the results
- Has anyone discussed with NERC anyone not liking on requirement and voting down the standard – can industry vote on the individual requirements rather than the whole standard?
- For ballot is it a vote on 11 as a whole?
- Standard 11 is an up or down – do not get to pick or choose – historically that is the way it has been done
- Historical observation – these are informal comments and not sure how much attention we got from the industry as a whole – have we had three different sets of the industry responding each time we go out – will we get a different response in a formal comment period
- So what – we have to move forward – we cannot assess whether that is true or not
- Yes, we need to move forward, but be aware of the possibility
- Have to look at the individual comments to determine if they are by a group or association versus an individual or individual company

Stu Langton reviewed with the SDT four key comments *(see below)* noting EEI and APPA represent approximately 60% of the industry. What are their arguments? Ameren suggests it will be easier to find requirements in one standard and use. EEI argued for the legacy of CIP 003-009 or at least a way similar to it as being easier for the industry to recognize and preserve sunk costs. APPA suggested sub-headings in 011 are illustrative of the need to separate into multiple standards and that multiple would be simpler to work with and revise in the future. IRC suggested functional areas with each standard being a stand-alone.

Specific Industry Trade Associations and Task Force Comments on Format

9.83	Ameren	Keep CIP-011-1 as one document	It is much easier to find all the requirements when all contained is a single document and the chance of discrepancies between documents is greatly reduced. However, the CMEP should be updated to monitor and report violations by standard and requirement not just standard. Otherwise, CIP-011 will always be in the list of Top 10 most violated standards and create a misleading impression that utilities cannot figure out how protect the reliability of the BES.
9.35	EEI	Break CIP-011-1 up into multiple standards	It would be easier for entities to recognize and understand the similar or different requirements in version 4 if they were broken up in a manner similar to legacy CIP-003-009. Many organizations have made significant investments in training, policies, procedures, and document management systems that are based on the legacy CIP standard Requirement numbering structure. Staying with the legacy structure, to the degree that it is possible, may reduce stranded investment that needs to be recreated simply as a function of the name and numbering of the requirements.
9.42	APPA Task Force	Break CIP-011-1 up into multiple standards	The APPA Task Force believes the addition of sub-headings to CIP-011 is illustrative of the need to separate this standard into multiple standards. We also feel with multiple standards the revision process would be simplified. If only one section needs to be revised, then NERC could just post that particular section for industry comment.
9.17	IRC Standards Review Committee	Break CIP-011-1 up into multiple standards	(i) We disagree with the current structure. We'd suggest the SDT to establish new standards by functional areas and ensure there is not a circular loop relating to other standards. Each standard should be standalone(ii) We understand the need for this standard to take care of cyber security concern when there does not currently exist an across-the-board cyber protection standards that apply generically to all sectors that utilize cyber components and cyber access for control and data exchange. However, over time, we urge NERC and the electric industry to assess if indeed it needs to have its own cyber

			protection standards at all. Cyber protection is not unique to the electric industry. Other sectors - airline industry, national security/ defense, financial sector, banking system, etc. all employ a high level of cyber security to protect fraud and invasions. Wouldn't the electric industry be better served if owners of BES Cyber Systems be required to adopt similar practices of these other sectors as opposed to developing it own very detailed set of requirements which, for the most part, seem to replicate the other sectors' requirements? It will be desirable to have a generic set of Cyber protection standards that is applicable to all sectors that use Cyber Systems - may they be for BES control or access to airline reservation, air traffic control, e-banking, security trading, etc. NERC and the electric industry should take the lead to initiate a continent-wide effort to consolidate all such standards and practices to avoid redundant efforts.

Format Discussion Comments

- What did we learn from this we did not know before? Any new gems we need to think about?
- We have to think about why people commented or not – those who commented favored splitting it up while those favoring one standard did not comment.
- Support for one over the other is not clear
- We should note that some votes may represent more than one entity, e.g. EEI, etc.
- The weight of the vote and comments are not the same – not sure the comments reflect the weight of the vote, many who support said "however, …"
- **Compliance Auditing, Enforcement and Reporting.** This hinges on the compliance reporting and whether it is done at the standard or requirement level.
- NERC will have to address it differently –
- The number of comments for each category (for against, no preference) is not relevant – if you agree, then less likely to add a comment
- This result gives us a sense the industry is not clear either. The Team needs to make the best choice for the industry then to judge. It there anything here that changes any of our minds? Issue comes down to compliance and auditing for multiple versus single standard
- NERC is still asking for clarification of the compliance/auditing issue. Did talk to compliance about the compounding issue – they said compounding is done by requirement, not by standard.
- Is compliance the same as enforcement?
- The person at NERC answering the compliance issue is with enforcement. Also talked to those in reporting about changing reporting to a requirement-by-requirement basis. There is support for this as it improves granularity of analysis.
- How does that improve organizations response?

- The perception in Congress is that cyber security is not being addressed. That perception and letting industry learn from others mistakes would be improved if reported by requirement.
- Favored single format in Atlanta – but now favor multiple standards – can we take a straw poll on where we are today. This is a structural issue we need to resolve.
- You asked the question and got industry comments – my sense the industry does not think this is worth the time we are putting into this question.
- Heard many say informally they may favor multiple standards but probably harking back to CIP 003-009. But note the SDT has already moved away from CIP 003-009.
- We asked industry what would best help them make everything secure – I did not put up a big fight before because I wanted industry to respond to the question.
- This is not a big deal to industry so let's split it and move on.
- The SDT reached a consensus decision on moving away from CIP 003-009 and then we asked industry for preference on one or multiple standards. Since last time the SDT had a clear preference for one CIP 011 and industry did have a strong preference in either direction, we should stick with the single standard
- Do not agree with that analysis. The comments, not the raw count, suggest we look again at CIP 003-009 -
- The Chair noted the SDT already voted a super majority (over 75%) to move to a new format.
- Everyone needs to review the comments in response to Question 9 before we vote on this issue.
- What does the option for multiple standards mean? We have eleven sections – would that mean eleven standards?
- Some comments suggest cramming the eleven back into the CIP 003-009 format. Need to precisely state what the two options are before we vote.
- But nothing will change between now and Friday – the split means the eleven sections we have now into eleven standards. We have already decided to move on from CIP 003-009 –
- Note that we have some new areas that may not fit into the old CIP 003-009. We are spending too much time on format.
- The SDT already voted to move forward. The debate now is how to do it – writing new content and standards now, that means industry will have to change.
- We moved away from CIP 003-009 because of version confusion – need a new set of standards – important not to fall back into the old regime.
- What was the SDT asked to do? We were not asked to rewrite everything. We were asked to take industry comments into account, not just throw it out because we had a previous vote
- If we reopen the vote then we need to look at the tables again.
- The vote to go forward with the posting was a result of months of work. I thought we all felt good about the product – the remaining concern was a minor one of format – going back to CIP 003-009 would create substantive and substantial problems.
- We asked for industry input because we did not have a super majority on the SDT to present a team proposal on the format.

- Scott Mix noted again that NERC Compliance suggested that violations are cited by requirement and not by standards.
- This is not a critical path element – lets spend the SDT's time fixing requirements – Do we need to vote on this now?
- By Friday this may become a critical path decision in order to redraft requirements for posting.
- The Chair noted the SDT's need to resolve the format issue once and for all – we left Atlanta with a super-majority but short of 75% to post CIP 011 as one standard and ask industry. The industry said we don't really care. My thinking is just leave it as one
- We may need to defer this in case we have to work on plan B stuff – not precluding making the decision later. We have the CIP 011 categories and can move forward.
- We need to look past the raw votes into the reasons one way or another offered in the comments and look at the level of concern and from what proportion of the industry – changing it is arbitrary and causes pain
- I do not conclude that someone who voted for but did not make a comment is not strong in their comment – to say we are not improving is unfair – we can move forward and maintain progress without deciding it now
- Even splitting it back into 011-021 doesn't address Dave's concern – if numbers change, it is the same concern
- While the difference in the comment votes was only 10 but some were by trade associations that may represent far more than one vote in the final analysis. Those associations seem to be on the side for multiple standards for CIP 011.

2. SDT Consideration of Single or Multiple Standard Format for CIP 011

The facilitators initially suggested first taking a straw poll on which of the two formats members favored then ask members for propose a motion on the format. The straw poll resulted in 10 members favoring multiple standards based on the eleven sections (011-021) and 9 members favoring the one standard format of CIP 011. Following this there was a motion (Doug Johnson, second by John Lim) to adopt multiple standards (011-021) resulting in 11 yeas (61%) and 7 nays (39%). The facilitators suggested revisiting this question at a later point noting the sentiment on the Team has appeared to shift in favor of multiple standards for CIP 011, but it fell short of the 75% needed to make a SDT decision on this question.

3. Standard Format Example- PCI DSS

John Van Boxtel provided an initial presentation on a possible improvement in the format displayed for the CIP. He provided an overview of PCI DSS standard format (*See Appendix 10 for the presentation slides).*

Member Comments

- Audits more programmatic rather than a specific requirement? Requires more experienced auditors.
- John is proposing we look at the format and adopt as appropriate – not asking to look at audits though PCI audits are more efficient and allows for them to look at other things – with PCI you do not get fined for everything and more focused on if you have met requirements to be recertified to process cards.
- Main differences is the measure is up in the table? (Yes) What else? (using the measurements for auditing) So it is format and content.
- Measurements would need to be substantially written different from those today sense they are the basis of the audit – like the way the guidance is built in but not the focus for audits.
- Fits with the NERC results based process puts the guidance up with the requirement and the measures in the table would be different – audit only to the requirements and not to the measures as directed by FERC.
- FERC would approve the requirement column and applicability column and not the measures column – but this puts everything in and allows us to consider what in the measures needs to be in the requirement column for purposes of audits.
- Wish we had seen this when drafting CIP 001 – given what we have in place not sure this works.
- Jan Bargen, FERC, indicated this would address much of the angst she has heard in the discussions and she like the way it integrates guidance for audits and how to meet the requirement. On the question of how it fits in current audit system, keep in mind you are creating a new paradigm and we may need to do something different on the audit side too. Integrating this into the requirement helps FERC review especially the blanks in the table – make your case for process changes.
- If FERC understood this made for one rule across regions, they may consider the change as a better approach
- It is similar to NIST approach.
- We may just need to change a few action words in the requirement to take into account the measures
- Also may address the baseline concern expressed in the FERC meeting on the 27th.
- We will work with Howard Gugel to see if it would work – think we could move forward with this format.
- Should help in drafting the requirements – clarifies and makes them more actionable and improving the auditability.
- Asking for more time – showing them this way of improving and solving the TFE and audit mess would help the argument for more time.
- Not sure but we may need to work on the question of TFE a little more to clarify how it would work.
- Should we incorporate this format going forward? Work on the requirements and let NERC staff focus on the format

- Howard Gugel– this fits in with the paradigm pursued by the vegetative standards group – there may be ways to make this work within our paradigm.

G. Sub-Team Meetings and Reports

The facilitators reviewed the process for reviewing the group reports. Stu Langton reviewed the progress to date with the SDT meeting all the deadlines and gotten industry approval to date with a very large group here, diverse, talented and bright – 38 day period to address issues – Talented basketball teams that play together the best succeed. For most part this Team has been able to achieve our 75% level for decisions. But now have less air time, need more focus and suggestions for improvement. We need to stay focused, those who like to talk may need to talk less and give more focused responses – think in terms of what we as a group need to do to get the job done.

1. **Open Question (Question 54)**

Phil Huff reviewed with the Team the responses to Question #54 noting we want the Team to help us be sure we have identified the right issues and determine who needs to address them. There were:

- 19 comments on clarity or wording: blank fields, several overall language improvements, and minimize use of adjectives.
- 12 comments on definitions especially hourly: move definitions to NERC glossary, appreciate local definitions, separate attachment for all local definitions.
- Timing issues – 11 comments.
- Implementation plan – 11 comments concerned about "gap" in compliance programs, sufficient time for categorization, CIP-010 may require more time.
- Categorization – 10 comments: remove low impact requirements, possible increase in risk as focus on med/low impact areas.
- Consistency – 10 comments: move requirements in the table, remove "authorship" of sub teams, requirements language referencing the table.
- Other comments on: audits and guidance, address remaining FERC directives now, access control and system boundary protection.
- Two major approaches suggested from Entergy and Progress Energy (latter regarding nuclear)

Member Questions and Comments

- Produce guidance documents – who, how and when?
- This will be done for posting by a team
- Many complained about lack of definitions where it was supplied in other area, giving all definitions in one place is a good one
- If move to multiple standards, then one glossary will be helpful

- Entergy – fully laid out approach offered for consideration – our requirements are binary, apply one or not – looking at NIST approach calls for a layered approach – also discussion of focusing resources on key risks in routable protocols.
- 853 approach may not apply to low category.
  It is not just the impact but the type of equipment that needs to be considered – we have not noted the differences between systems.
- Need to look at this for cyber vulnerability, not physical risks of natural disasters
- Did not look at scoping activities for consistency.

2. Question 53

Phil Huff provided the overview:

- 66 comments, with 57 specific comments: several referenced TFEs
- TFE comments: passwords, malicious code, appropriate use, system hardening, security event monitoring, wireless and remote address, communication and date integrity – we will need to farm several of these out to appropriate group
- Other comments: device characteristics, write clear requirements, TFE process improvements

Any comments the SDT needs to look at in particular?

- Are we going to go through each TFE requirement to make changes or considering supplying entities with flexibility? How are we going to put parameters around each requirement?
- Not all requirements are created equal. Not all requirements should be eligible for TFE though most should be – may need a black list of those not eligible for TFE
- FERC order allowed many flavors of TFEs such as legal requirements, or safety requirements, not just technical feasibility
- Directive acknowledged flexibility needed but that "business judgment" was over used – still can use or request exceptions under other categories
- Suggest not to put TFEs in specific requirements – develop a broad statement without specifying the applicable requirements
- 16 comments on passwords may suggest we need to take it up a notch and not be so granular

3. CIP 010

John Lim provided the overview of industry comments.

4. Questions 1-8, with subparts- Overall

The Sub-team in particular looked at three questions: #1 – definitions, #6 – the Attachment 1 functions, and #7 – Attachment 2 categorization of BES cyber assets.

Question 1a

1.a. BES Cyber System Component — One or more programmable electronic devices (including hardware, software and data) organized for the collection, storage, processing, maintenance, use, sharing, communication, disposition, or display of data; which respond to a BES condition or Disturbance; or enable control and operation.

34 (31%)= Agree with proposed definition
76 (69%)= Disagree with proposed definition

Dave Nortion summarized the industry comments to Question 1a:

- 71 responses were "no" with comment. Someone complained about each word in the definition
- From that created a suggested alternative definition
- Many do not think data should be there
- A definition is not "one or more" component(s) – it is just one component
- Look at systems, then components of a system, then individual items
- 11 "yes" with comments
- Separate out by operating systems suggested
- Suggestion to offer examples

SDT Member Comments and Questions

- What would be your recommendation in approach to making changes?
- Interesting observations – not sure what the implications are – first impression, we may need to make it simpler or more general or generic.
- Difficult in a definition to identify what is included in BES cyber system – have we provided enough guidance?
- Comments run the gamut of interpretation – some industry comments suggested it be "skinnied" down to just routable protocols and dial ups or it will be a monster to implement – everyone had heart burn with some word in the definition

Question 1c – control center

1.c. Control Center — A set of one or more BES Cyber Systems capable of performing one or more of the following functions for multiple (i.e., two or more) BES generation Facilities or Transmission Facilities, at multiple (i.e., two or more) locations:

- Supervisory control of BES assets, including generation plants, transmission facilities, substations, Automatic Generation Control systems or automatic load-shedding systems,
- Acquisition, aggregation, processing, inter-utility exchange, or display of BES reliability or operability data for the support of real-time operations,
- BES and system status monitoring and processing for reliability and asset management purposes (e.g., providing information used by Responsible Entities to make real-time operational decisions regarding reliability and operability of the BES),
- Alarm monitoring and processing specific to operation and restoration function, or
- Coordination of BES restoration activities.

42 (40%)= Agree with proposed definition
63 (60%)= Disagree with proposed definition

- 23 pages – 63 disagreed, 40 agreed and many with no preference still had a comment.
- Control center should have "two or more" of the functions listed ("not one or more" functions)
- "…this standard is not the correct place to redefine BES and any language that does will force a no vote …"
- Some wanted definition of control centers
- "Multiple locations" mean geographic locations or multiple generating units?
- EEI comment: suggested a new definition
- Another comment attempted to scale down the scope of the requirement
- Does "location" refer to physical or electrical(?) locations?
- Generation plants refer to power plant or generation facility?
- Control center a cyber asset or a physical location?
- Remove AGC systems from function 1?
- Suggestion that in bullet 3 "asset management" may not be appropriate and should not be included
- Suggestion to remove bullet 4 as redundant.
- Bullet 5 comments suggest removing it
- Some real nuggets in the 23 pages we need to mine to improve the definition overall

Member Comments

- On restoration as not a cyber function – much of the communication system for manually switching needs to be considered from transmission center point of view.
- High level coordination has to occur to make sure it is safe and secure.

Question 6:
CIP-010-1 Attachment I contains a listing and brief description of Functions Essential to Reliable Operation of the Bulk Electric System. Do you have any suggestions that would improve the proposed criteria? If so, please explain and provide specific suggestions for improvement.
62 (58%)= Agree
45 (42%)= Disagree

Jim Fletcher presented a summary of the industry responses:

- 58% agree
- The one issue dominated the comments – the attachments needs more definition, examples and guidance in attachment 1
- Next better definition of real-time and the 15 minute window
- One suggestion to use 30 minutes but that seems beyond "real-time"

Summary data (slashes indicate repeat comments)
____ – "condition" not correct in context
No – use 30 minutes to match EOP std
No – Attachment 1 clarity, needs guidance //////

No – Attachment 1 should be guidance, not part of the standard /
No – "communications" implies voice
No – avoid using undefined terms or redefining preexisting NERC terms
No – when does the 15 minute period commence //
Yes – situational awareness of current state of bes results in too broad a scope ////
Yes – "functions" of Attachment 1 confusing overlap and ambiguous //////
Yes - need cut out for nuclear facilities covered by NRC
Yes – "shutdown condition" definition
Yes – concern for 15 minute window and real time adverse impact //
Yes – mitigation of event within 15 minute window needs to be included
Yes – voltage control needs to reference bes voltage
Yes – inter-entity communication too broad could include signal paths covered by other standards /
Yes – boundary for without external assistance /
Yes – need specific examples for reliability functions ///////////
Yes – delete attachment /
Yes – real time definition needed /
Yes – monitoring and control too broad
Yes – substitute NERC adequate level of reliability document for attachment 2
Yes – need to refer to other document for system restoration functions rather than make a definition here
Yes – remove 15 minute window /
Yes – treat control and monitoring as separate functions ////
Yes – inter-entity communications could imply voice
Yes remove inter-entity communications unless BES cyber systems can be defined to include components from multiple entities
Yes – system restoration is not a function supporting reliable operation
Yes – remove attachment 1
Yes – include more definition of functions supporting reliability of the bes in standard
Yes – should explicitly exclude voice systems

SDT Member Comments

- In terms of reliability determination something is lost in scoping – need to look at subject from the reliability coordinators perspective

Question 7 Attachment II

Question 7: CIP-010-1 Attachment II contains criteria for categorization of BES Cyber Systems for High, Medium and Low impact categories. The criteria were originally developed in collaboration with representatives of the Operating and Planning Committees, some of whom continued to provide input during the drafting of Attachment II. Do you have any suggestions that would improve the proposed criteria? If so, please explain and provide specific suggestions for improvement.

72 (67%)= Agree with proposed definition
35 (33%)= Disagree with proposed definition

Rod Hardiman presented a summary of the industry responses including the following points:

- If look at question then more accurate to note as much as 75% actually disagree
- Blackstart is not high impact/only include units in regional plan/openly include primary blackstart units – 24 comments

- "must run" is inappropriate term – 12 comments, 5 more related
- Should have a "no impact" level below low – 10 comments, 5 more related
- Provide justification for thresholds/thresholds are arbitrary – 10 comments
- Categorization should be based on engineering studie/need waivers from thresholds -9 comments
- Define "primary cranking path" – 9 comments
- Questions about defining "transmission line", local area , transmission facility, etc.
- Sorted attachment 2 categories by the number of times commented on

SDT Member Comments

- Top three deal with generation and transmission support centers –
- Some called for combining the generation categories, as well as the transmission categories
- Comments on 1.14 and 1.13? RAs and TOPs running at less than high given their coordination and communication? If interconnected, should all, even small ones be considered "high" to establish high trust levels?
- There is a level of protection at the application level but hard to put into the standard here
- Important to have some sort of protection from injection attacks – have some level of data protection – appropriate that industry pushes forward to get vendors to produce product

Other issues in 010

- Requirement R3 for updating lists and categorization – have not had a chance to review comments, assume many significant comments and will need to review in the next call – Question 5
- Variable generation is important to wind and solar providers and how it fits

5. Governance, Change Management, System Lifecycle and Information Protection and Maintenance Sub-Team

Dave Revill introduced the Sub-teams work noting it covered Questions 11, and 40-48.

SECURITY GOVERNANCE AND POLICY Question 11 – R1

11. Requirement R1 of draft CIP-011-1 states, "Each Responsible Entity shall develop, implement, and annually review formal, documented cyber security policies that address the following for its BES Cyber Systems:" and then provides a list of topics that must be addressed. Do you agree with this proposal and list? If not, please explain why and provide specific suggestions for improvement.

58(56%)= Agree with proposed definition
46(44%)= Disagree with proposed definition

John Stanford presented an overview of industry comments:

- Seeking clarity in the list, policy phraseology, or definitions of terms (19)

–Examples include: Formal, annually, boundary protection, sanitization, security roles and responsibilities, authorized access, personnel, third-party, non-employees, addresses.
–Desire to have terms used in later requirements defined here

- Seeking clarity in the policy expectations, purpose or structure (11)
  –Desire to have all access related issues defined here
  –Numerous questions on what is meant by policy language
  –Several concerns about how to demonstrate compliance with a policy
- Concerns about the term "annually" (9)
  –Numerous suggestions on alternate wording for clarity
- Questions about Senior Manager (8)
  –Mostly delegation or approval concerns, possible conflict with R3, or claims of double jeopardy between R1 and other requirements
- Concerns about burden of proof, compliance, legal or ownership (4)
  –Several concerns about allowing for non-ownership or non-operation of BES Cyber Systems
  –A few raised contractual obligation concerns
- Concerns about policy being too prescriptive (5)
  –Seems to be confusion about general policy hierarchy
- Suggested edits without actual disagreement (4)
  –All over the map
- Generic references, non-substantive comments, or misplaced (3)
  –Examples include comments about change management or "ditto" and "me too" comments submitted by others on other requirements

SDT Discussion Comments

- Need to be clearer on the overall intent here
- Some may be looking at results based requirements – looking for the what rather than the how
- Many comments want to clarity about what you are asking – clearly getting mixed message of clarity on what is expected versus being too prescriptive
- Would a guidance document help here?
- The phraseology may be asking for a lexicon – how far do we want to go there?
- Maybe there are some things we can glean from the responses to clarify the language rather than saying we need to teach them what we mean
- Some interpretations may need to be left to legal but others are terms of art that we may need to clarify with purpose of our intent
- Some concern about why governance and policy structure is a regulated area
- This is a balance between binary requirements and a policy structure
- Reinforcing the value of policy in a good security program
- FERC looking for management responsibility and policy is a linchpin
- Complying with the controls may not be enough – need good policy to drive compliance
- If done right policy can set a good foundation
- "annually" was mentioned here and in other groups – needs to be addressed

6. BES CYBER SYSTEM MAINTENANCE (R26) Question 47, R26

47. Requirement R26 of draft CIP-011-1 concerns procedures for BES Cyber System maintenance. Do you agree with the list of criteria that are included in Requirements Table R26? Please explain and provide any suggestions for modification. Are there any additional criteria that you believe should be included in the table? Please explain and provide any suggestions for modification.

41 (48%)= Agree with proposed definition
45 (52%)= Disagree with proposed definition

Dave Revill presented the following overview of industry comments:

- Concerns about the interaction between the list of personnel in 26.1 and the lists granting authorized electronic and physical access (13)
- Concerns about the interaction with other user/account management requirements (12)
- Comments regarding the allowance for emergency maintenance situations (2)
- Requirements on maintenance devices should include system hardening (2)
- All maintenance devices should be documented in a list (2)
- Ensure that systems used for maintenance do not act as an unauthorized access point (1)

He noted they also got comments on the definition of "maintenance" – some said to consider the temporary connection also have appropriate controls.

SDT Comments

- Overlap on responsibilities that we may need to address
- Some entities may not have specific devices set aside for maintenance – but may be burdensome the random use of a laptop to perform maintenance
- What is "maintenance"? What are the devices are you connecting for maintenance activities, such as field devices
- In guidance document may want to put in something about how you can provide evidence of compliance with this requirement

7. ELECTRONIC ACCESS CONTROL (R7 –R14)

Question 17. Requirement R7 of draft CIP-011-1 states "Each Responsible Entity shall document BES Cyber System accounts by incorporating the criteria specified in CIP-011-1 Table R7 – Account Management Specifications to prevent malicious operation of BES Elements by maintaining control of access to its BES Cyber Systems." Do you agree with the list of electronic access control requirements that are included in Requirements table R7? Please explain and provide any suggestions for modification. Are there any additional criteria that you believe should be included in the table? Please Explain and provide any suggestions for modification.

56 (58%)= Agree with proposed definition
40 (42%)= Disagree with proposed definition

Sharon Edwards presented the following summary of industry comments:

- Misunderstand that they are to define acceptable use
- Local definition/description of account types
- Soft language
- Top themes:
- 1 - Need a strategy for designing baselines by impact levels – we missed the mark
- Strategy going forward include policy requirements, verification of implementation
- 2 – revocation of access – do not like the time parameters for revocation, transferred personnel should not be treated as risk, and clarify when the clock starts for no longer needing the access
- make distinction between "primary" access and "secondary" access; primary access includes the domain user account, remote access credentials, and physical access; etc.
- 3 – clarity and definitions on acceptable use, account types, system access, remote access, external connectivity, wireless, etc.
- 4 – separate remote and wireless access
- 5 - consistency
- 6 – quarterly review is excessive
- Discussion – if we take this approach it needs to be justified and segmented appropriately in h-m-l

SDT Questions or comments

- Don't make distinction between BA, TO, TOP, GO? Those are the comments? That is surprising in terms of the parameters for revocation.
- Comments may be coming from control centers who want to relax the requirement – this is in contrast to the request to make it "immediate."
- May need to segregate requirements and make distinction for those terminated for cause and others who are lower risk
- Are we addressing privileged accounts? This is a case were you need to run, not walk.
- Yes, but it is not under revocation
- Need to coordinate revocation ahead of termination of those with key access
- Highly recommend not using "primary" or "secondary" access – you either have access or don't – need a three level recognition of revocation including those with privileged accounts
- "quarterly review" – assumption the this included quarterly reauthorization – that would be a burden – need to clarify quarterly reauthorization is not part of the requirement
- need to coordinate the timing required in other requirements
- need to look for overlaps and need for coordination between the teams
- quarterly review is part of the monitoring, not reauthorization – need to clarify proposal
- quarterly review is meant to catch and fix those we missed – should not have to self report those.

8. Response and Recovery

CYBER SECURITY INCIDENT RESPONSE (R27 –R29)

49. Requirements R27 to R29 of draft CIP-011-1 concern procedures for Cyber Security Incident response. Do you agree with the list of criteria that are included in each Requirements Table for Requirements R27 to R29? Please explain and provide any suggestions for modification. Are there any additional criteria that you believe should be included in the tables? Please explain and provide any suggestions for modification.

54 (61%)= Agree with proposed definition
34 (39%)= Disagree with proposed definition

50. Tables R27 to R29 provide direction concerning what impact level of BES Cyber Systems to which Requirements R27 to R29 apply. Do you agree with the impact levels as indicated? If not, what specific changes would you suggest?

52 (60%)= Agree with proposed definition
34 (40%)= Disagree with proposed definition

BES CYBER SYSTEM RECOVERY (R30 –R32)

51. Requirements R30 to R32 of draft CIP-011-1 concern procedures for BES Cyber System Recovery. Do you agree with the list of criteria that are included in each Requirements Table for Requirements R30 to R32? Please explain and provide any suggestions for modification. Are there any additional criteria that you believe should be included in the tables? Please explain and provide any suggestions for modification.

39 (46%)= Agree with proposed definition
46 (54%)= Disagree with proposed definition

52. Tables R30 to R32 provide direction concerning what impact level of BES Cyber Systems to which Requirements R30 to R32 apply. Do you agree with the impact levels as indicated? If not, what specific changes would you suggest?

52 (65%)= Agree with proposed definition
28 (35%)= Disagree with proposed definition

Scott Rosenberg presented the overview of industry comments:

- Guidance on cyber security incident classification highlighted.
- Definitions
- Coordination with 001
- Incident response for low impact or non routable connections should be removed?
- Consistency between requirements related to impact level?
- Single versus multiple incident response plans and testing issues.
- Combine incident response testing and review/update.
- Review results of incident response tests in other than 60 days
- Recovery testing
- Recover plan testing clarifications
- Data retention identification requirements of personnel responsible
- Coordination of physical aspects of cyber security incidents
- Incident response and recovery plan reviews and question around changes required
- Suggestions for re-wording

- Coordination of backup plans

SDT Questions or comments

- FERC said we may not have enough requirements? More important to set a base line, focus on quality not quantity with security need in mind – not the number of requirements but the right ones
- Timing questions – can NERC develop a Gant chart of the timing requirements?
- Summarized in one place would be helpful to entities
- Good appendix to a guidance document
- Helpful to team for coordinating and consistency across the requirements
- A table of all the timings? Yes
- "annual" is across several requirements – may need a joint effort to define a common understanding
- Proposing the team draft glossary definition of "annual"?
- Careful – this may become an audit issue – may need to be given to the Standards Committee.
- Define for local purposes – how does the team want to use the word? Do we mean 365 days? Once a calendar year?
- When we use time related items, need to identify what we are trying to achieve – think about a flexible window for compliance and auditing.
- Any time based requirements? Quarterly?
- Good to have a base line approach to incident response.
- Need to present context without putting into requirements
- Taking requirements and putting into a table? Are there requirements for how to do that from NERC?
- Industry has said it makes sense and offered suggestions for refinement – may need to identify multiple requirements in the same table or split them out
- Can we put up an example of a table for comparison? Send out by email then take a look at together tomorrow.
- Backup control center – some asked why do I need to do anything else?
- Might put in words to say fully function backup center is sufficient for recovery
- Still need a recovery plan.
- This is a cyber incident possibility – a hot backup may be corrupted or could lose both – cold backup is less likely to be corrupted in the same incident.
- Business continuity to keep operating and then there is restoration of the original assets
- This is recovery of the cyber system – not a backup system
- Need to recovery ability to execute control – differs from recovery of the assets
- Three levels: recover capability, recover the assets, and recover.
- Purpose to protect the grid or the assets?

9. Systems Security (R15 –R19)

35. Requirements R15 to R19 of draft CIP-011-1 concern procedures for system security protection. Do you agree with the list of criteria that are included in each Requirements Table for Requirements R15 to R19? Please explain and provide any suggestions for modification. Are there any additional criteria that you believe should be included in the tables? Please explain and provide any suggestions for modification.

25 (27%)= Agree with proposed definition
67 (73%)= Disagree with proposed definition

36. Tables R15 to R19 provide direction concerning what impact level of BES Cyber Systems to which Requirements R15 to R16 apply. Do you agree with the impact levels as indicated? If not, what specific changes would you suggest?

40 (45%)= Agree with proposed definition
49 (55%)= Disagree with proposed definition

BOUNDARY PROTECTION (R20 –R22)

37. Requirements R20 to R22 of draft CIP-011-1 concern procedures for boundary protection. Do you agree with the list of criteria that are included in each Requirements Table for Requirements R20 to R22? Please explain and provide any suggestions for modification. Are there any additional criteria that you believe should be included in the tables? Please explain and provide any suggestions for modification.

28 (31%)= Agree with proposed definition
62 (69%)= Disagree with proposed definition

38. Do you agree with the proposed definition of electronic access point? Please explain and provide any suggestions for modification.

49 (56%)= Agree with proposed definition
38 (44%)= Disagree with proposed definition

39. Tables R20 to R22 provide direction concerning what impact level of BES Cyber Systems to which Requirements R20 to R22 apply. Do you agree with the impact levels as indicated? If not, what specific changes would you suggest?

38 (46%)= Agree with proposed definition
44 (54%)= Disagree with proposed definition

Jay Cribb noted that the industry responses to Questions 35-39 covered more than 100 pages.

R15 – Malware Prevention

15.Requirements R5 and R6 of draft CIP-011-1 concern procedures for physical security, which were previously contained in CIP-006. Do you agree with this proposal? If not, please explain why and provide specific suggestions for improvement.

37(40%)= Agree with proposed definition
56(60%)= Disagree with proposed definition

Jay Cribb summarized the industry responses as:

- Don't' require malware testing
- Very difficult to audit current language
- Need device class language or many TFEs

SDT Comments and Questions

- What is the problem with malware testing?
- Language looks like you are ask to put malware into your system to test the system
- Need to clarify we are trying to prevent propagation of malicious malware
- Testing has to take place outside the production system
- Testing the protection systems
- Test in a real world already – we know the products work – why test my antivirus when it is tested every day in the real world –
- need to clarify the language and intent
- do we need this here or is it already covered elsewhere?

R16 – Patch Management

- What starts the clock? Release vs. availability
- Fixed date of implementation

SDT Comments and Questions:

- Getting reliability tested on their systems first and certifying it is more important than the contract.
- #2 is a misnomer – the requirment asks for applying the patch and pick a date or date for mitigation – reasonable requirement –

R17 – system hardening

16. Tables R5 and R6 provide direction concerning what impact level of BES Cyber Systems to which Requirements R5 and R6 apply. Do you agree with the impact levels as indicated? If not, what specific changes would you suggest?

37(41%)= Agree with proposed definition
54(59%)= Disagree with proposed definition

Jay Cribb provided the following overiew of Question 17 industry responses:

- What is "externally accessible physical port"? (By far the most common comment)
- Physical port disabling on devices that are already secured

SDT Comments and Questions:

- Physical ports? Need to relook at this – reframe to cover accidental use
- Need to disable the local services too
- We test many best practices that do not actually add to security

R18 – security event logging and monitoring

18. Table R7 provides direction concerning what impact level of BES Cyber Systems to which Requirement R7 apply. Do you agree with the impact levels as indicated? If not, what specific changes would you suggest?

66 (69%)= Agree with proposed definition
30 (31%)= Disagree with proposed definition

Jay Cribb provided the following overiew of Question 18 industry responses:

- Is weekly manual log review really needed with continuous monitoring?
- What is a "cyber security event"?

SDT Comments and Questions:

- None.

R19 – data and communications integrity

19. At the present time, the Access Control requirements for Physical Access have not been combined with the Access Control requirements related to Electronic Access. Do you agree with this method? Or would you prefer to have the Physical Access control requirements combined with the Electronic Access control requirements? Please explain and provide any suggestions for modification.

74(80%)= Agree with proposed definition
19(20%)= Disagree with proposed definition

SDT Comments and Questions:

- Very unclear what is validation and what is satisfactory?
- True validation happens at the application layer – dependent on vendor, etc.
- Proving malicious intent of invalid data received is very problematic (impossible)

Boundary Protection

20. Requirement R8 of draft CIP-011-1 states "Each Responsible Entity shall apply the criteria specified in CIP-011-1 Table R8 – Account Management Implementation to prevent malicious operation of BES Elements by maintaining control of access to its BES Cyber Systems." Do you agree with the list of criteria that are included in Requirements Table R8? Please explain and provide any suggestions for modification. Are there any additional criteria that you believe should be included in the table? Please explain and provide any suggestions for modification. Do you agree with the impact levels for each criteria as represented in the table? Please explain and provide any suggestions for modification.

45 (48%)= Agree with proposed definition
48 (52%)= Disagree with proposed definition

Jay Cribb provided the following overview of the industry comments:

- Rename this and the tables back to ESP
- Remove or clarify the alerting timeframes (the 48/12 hrs)
- Weekly review of log entries
- Clarity – what is a "communication path", "authorized access"
- Clarify access points and their interaction with multiple BES cyber systems

SDT Comments and Questions:

- Looking at taking review of logs and alerting time frames and moving them up into the requirement – thus one requirement for system monitoring rather than in two places
- Pull physical into it too?
- Did we have a question that asked if prefer consolidated or separated?

- Comments favored keeping physical and electronic separate
- But is it the same distinction for monitoring?
- Makes sense
- But caution – physical and electronic monitoring may be done by two different sets of people – careful how it is worded

R21 – system boundary

21. Table R8 provides direction concerning what impact level of BES Cyber Systems to which Requirement R8 apply. Do you agree with the impact levels as indicated? If not, what specific changes would you suggest?

50 (55%)= Agree with proposed definition
41 (45%)= Disagree with proposed definition

Jay Cribb provided the following overview of the industry comments:

- Remove the requirement – overly prescriptive
- How does this requirement differ from R20

SDT Comments and Questions:

- Is it realistic to address and incorporate the changes suggested by this July?
- These are just the top issues from 100's
- Little more detail on system boundary – is it about the logical separation piece?
- R21 separates systems that could have a single point more than they are now – it is not just systems boundary
- Confusion about the differences between the two, some argued to combine
- Making it a requirement may be too much – putting in a best practice and making it auditable
- Point is to address shared systems and being sure they are protected to the same level – or not share – if combine the two we can achieve the same goal and reduce confusion
- Access points can be physical or electronic – need to clarify to improve understanding
- Access point is the interface and that is what you need to protect – not the same as the firewall
- Focus on the interface
- Making distinction between firewall challenge and access control(?)?
- Requirement addressed access control at the interface level

R22 – Protective systems

22. FERC has mandated immediate revocation of access privileges when an employee, contractor or vendor no longer performs a function that requires physical or electronic access to a critical cyber asset. Requirement R9 of draft CIP-011-1 states "Each Responsible Entity shall revoke system access to its BES Cyber Systems as specified in CIP-011-1 Table R9 – Access Revocation to prevent malicious operation of BES Elements by maintaining control of access to its BES Cyber Systems." Do you agree with the list of criteria that are included in Requirements Table R9? Please explain and provide any suggestions for modification, including time proposals. Are there any additional criteria that you believe should be included in the table? Please explain and provide any suggestions for modification.

27 (29%)= Agree with proposed definition
67 (71%)= Disagree with proposed definition

Jay Cribb provided the following overview of the industry comments:

- Remove and put the systems in scope of the relevant requirements
- Weaker than the current standard

Jay Cribb then noted some overall issues raised in the industry comments:

1) TFE allowances – where and how. All of our requirements will need them
2) Clarity around when the requirement applies to "systems" and "components"
3) External connectivity matters – do not require external connectivity in order to meet RQ's
4) "no impact" category needed

SDT Comments and Questions:

- approval rating for this section very low for this whole section
- many of the comments related to the existing requirements and concerns
- can we retool these requirements in 38 days?
- Doesn't need more people but need to retool timing by asking FERC to give NERC more time – need to retool the time – I think the FERC people understand, but do the NERC people – change the time
- NERC can ask for more time
- Take up and address the timing issue tomorrow as part of the schedule discussion

10. Personnel & Physical Security

Doug Johnson presented the summary of industry comments on personnel and physical security. The one on training we changed the least from the CIP garnered the most comments.

- Questions 12-14 for R2, 3 and 4
- Questions 15-16 for R5 and 6

PERSONNEL TRAINING, AWARENESS, AND RISK ASSESSMENT (R2 –R4)

12. Requirements R2 to R4 of draft CIP-011-1 concern personnel training, awareness, and risk assessment, which were previously contained in CIP-004. Do you agree with this proposal? If not, please explain why and provide specific suggestions for improvement.

23(23%)= Agree with proposed definition
77(77%)= Disagree with proposed definition

13. Do you agree with the proposed definitions for external connectivity, routable protocol, and non-routable protocol? Please explain and provide any suggestions for modification.

59(60%)= Agree with proposed definition
39(40%)= Disagree with proposed definition

14. Tables R3 and R4 provide direction concerning what impact level of BES Cyber Systems to which Requirements R3 and R4 apply. Do you agree with the impact levels as indicated? If not, what specific changes would you suggest?

43(47%)= Agree with proposed definition
48(53%)= Disagree with proposed definition

Doug Johnson presented an overview of industry comments on Question 12, R2

- What security awareness program is being referenced? (see R1)
- Replace the term "reinforcement" with "awareness material and replace "provide all" with "make available to all"

SDT Comments and Questions:

- May want to divide R1 much the way others divided into the other requirements
- What should the policy or program have in it? R1 says must have a policy
- R1 language could be adjusted to be consistent with the following – may break 1.4 into multiple parts – R1 lacks detail
- Does programmatic guidance need to be in R1 or broken out into sub parts? Approach affects other areas too
- Need to write it down and come back to for more discussion – how is the low approach depicted and approached?

R3

- 3.2 – add clarification or make it role specific
  - (the clarification is important to acknowledge that the intent is clearly not to have all personnel with electronic access to any BES cyber system to become network engineers)
- What is Annual?
- Would it be better to include the table for consistency?

STD Questions and Comments:

- "annual" appears in only one place – in R1
- here the concern is about any time frame – not the specific word
- need a consistent way to reference to be clear
- at least once every twelve months – is that not clear enough?

R4

- Why is photo ID now being required?
- Address how to better handle vendors and contactors

STD Questions and Comments:

- Not realistic to require CISCO to go through training process for remote access
- Concern about allowing third party access and support especially in an emergency to maintain reliability
- May need NERC to certify and support a third party vendor training
- Entity may need to define and document emergency situation – allow for exception in such circumstances

- Not something NERC creates – need to put into a requirement – unless willing to do that, then NERC is not going to do it – operator stuff was created by the industry – NERC will not certify appropriate persons with operator access
- Distinction is in the authorization for access control – person given temporary access working through someone with authorization – latter is required to document and have management approval
- Operator certification is provided by third parties
- NERC could not provide training for the procedures for all of the entities, especially given the diversity of entities and their procedure
- Focus here is on remote support access
- Escorted remote access? No equivalent on electronic side to the current escorted physical access – an issue for all the entities
- R3 and 4 have exception clauses for emergency to the training requirement – some better definition in the maintenance that documents the emergency clause rather than a requirement for training in emergency situation

R5

- Immediate revocation of access
- What is meant by the term monitor?

STD Questions and Comments:

- Is escorted electronic access an open issue for interpretation?
- That is not the interpretation requested
- "authorized access" is not used in the standard – the standard does not address the concept – only unauthorized physical access and granting electronic access are in the standard
- parking lot issue of combining physical and electronic access revocation – 80% of those offering comments agreed to separating the two?
- Need a single person revocation of both physical and electronic access – personnel revocation
- Are we moving forward with them as separate items? Yes
- Granting access and revocation need to be consistent

R6

- Physical Access Control Systems need to be defined
- Potential for a fourth column

STD Questions and Comments:

- Consider a fourth column where needed to where physical controls need to be applied – we do not need physical access controls lumped in with the electronic controls – do we need a fourth column?
- For end user it may be better to have a separate requirement rather than search through all of the related requirements
- Comments suggested embedding electronic controls – but keep physical controls separate

- There is a broader category here – requirements apply to BES and protective systems
- Keep physical access on their own
- Parking lot issue: protection requirements for electronic and physical access controls and systems (Phil Huff)
- May need to insert a "local" definition

Overall question for SDT

- Is it possible for an entity to have no BES Cyber Systems?

STD Questions and Comments:

- May want to address in 010
- Several hundred distribution providers who do not have BES assets but need target protection

IV. OTHER 706 ISSUES AND CIP DOCUMENT PREPARATION

A. FERC Order 706 Issues In Addition to CIP 010 and 011

On Thursday the Team took up how to address 706 issues that have been termed "post Version 4 issues" that include:

A. Access Control Redundancy/~~Defense in Depth~~ (two or more diverse security measures in constructing electronic and physical security perimeter)
B. Active vulnerability assessments every three years
C. Forensic data collection

SDT Members Discussion

- Issues raised during the workshop
- Comments also appeared in question 54 and in Doug Johnson's group
- These are non trivial and will take even more time and discussion than taken so far – trying to get 011 done first without delay.
- Willing to write single page description of each issue?
- Strong concern in industry about punting to another version – can we address in a limited manner at least as a place holder – concerned it is doomed with FERC without defense in depth for example – scope it down and phase in.
- That is not what the FERC directive said.
- Yes will take time, but is this justification for an extension from FERC.
- Rename defense in depth to access control redundancy of access perimeters
- Need to do vulnerability assessments on redundant not live systems – careful how we write – also need clarification from FERC (Mike Peters) on the issue
- Not talking about putting in two access points to perimeters
- Peters said defense in depth is fundamental and bolting on later will cause trouble for industry

- Need more two way communication as to what FERC is asking for, the intent of the request. This is too important to make assumptions and the goals are too important/
- Put in words from the actual order – paragraph 480
- Paragraph 502 also says flexibility – it also says it is not intended to create an inflexible requirement.
- Misconception written into the order – most systems already have three levels – can do three things at the same level rather than pick different levels.
- Ignore the Commission's request and tell them what they should have said
- Seeking clarification
- Paragraph 725 – need to pull out of 011? – Paragraph 710 requires data in blackout report and improved forensics.
- We need to research what the commission is asking for.
- Jan Bargen, FERC, noted her understanding is that you do not have cyber security if it is not in depth – too severe an interpretation that it has to be all or nothing and cannot been done in pieces – you can explain progress and point to in the requirements and note what else needs to be worked on – recognize you are working on a new paradigm and have a window of opportunity.
- Language in 706 says you have flexibility in how to approach concerns – by accepting phased approach to implementation in the past FERC is indicating you can apply to defense in depth and forensics.
- Putting so much protection at the boundary that you need some depth – if get through firewall you need another layer – not necessarily another duplicative firewall but cannot get through just one vulnerability.
- These don't have to be next to each other.
- We have to assume the bad guys are in your business system and you need to protect the high end assets.
- We will need to review current draft requirements to see what is already addressed, then assess what it would take to address in part or full the issues.
- Support that approach – also agree we are in a new paradigm – also need optics we are trying to deal with issues – and fourth, we need clear grounds for an extension.
- Fourth issue of operation test of the recovery plan addressed in CIP 011
- Need to review and develop possible ways to address in small team groups.
- Under forensics – half may already be dealt with under Jay's group and the rest in Scott's under recovery.
- Can we ask Carnegie-Mellon to help with this – meeting is in Pittsburgh next month
- We have now have 38 days left – Jay's sub-team is not done and it is the key – we need a backup plan – we just added to Jay's sub-team's responsibility – have to figure out how to address this soon or have a backup plan – maybe it is just a patch of the old CIP 005 and 007 and not a brand new system?
- Item B will also be addressed in Jay's group

- Item A, part 2 in my group – have not discussed yet – given volume of comments to deal with, not sure if we can get to it in the time frame we have
- We are in a countdown mode with an artificial deadline. In order to get it right, we may need to adjust the deadline

B. Implementation Plan Options

Scott Mix presented the implementation plan concepts and approach.

- Open issue about early compliance – example, implementation time frame that adds up 2 or 3 years before version 4 kicks in but buying new EMS now and want to be compliant with v4 in the new system - legal said "no" – hopefully they did understand the question, will try to discuss issue with legal further.
- Floated to FERC the concept of compliance with high in two years, medium in five years and low in ten years – focus on smaller number of assets first with the biggest bang for the buck or investment of time and resources.
- What about entity with only low assets? Do they get to wait eight years to do anything? How can we incentivize them to move quicker or start earlier?
- Implementation plan may look similar to a mitigation plan – come up with list of assets "quickly" (30-90 days?) – create an implementation plan for your entity – provide guidance and oversight with yes or no on the early compliance plan and audit to the accepted plan – regional entities are the ones who approve the plan
- May create confusion for audit teams and regions
- Cannot let industry appear to be delaying the inevitable
- Favorable reception by FERC staff for early compliance plans – at least one of the regions is considering a similar approach – proposal may still need time and attention
- Nuclear process is a similar approach
- Have a team to help draft approach

SDT Questions and Comments

- Flabbergasted – if going after highs in the first phase
- Jan Bergen, FERC, noted that it is worth exploring opportunities to implement sooner than 10 years.
- Mike Keene, FERC, suggested this function as long as requirements in 011 are done in appropriate manner – conception is an acceptable approach
- Focus on the real attack surface first – we don't have the proper focus on the appropriate attack surface – too focused on big iron and not the cyber system.
- The approach makes sense – especially for those putting in new systems now – concern from some that they do not want to have to comply with two different versions at the same time
- I am not a fan of approach – letting entities build their own plan misses the interdependence of the small and big entities – do not think one entity gets fined on a low

asset down the road from another entity that is not under compliance for anther four years – also end up with different timelines for compliance on physical protections
- Have to order the sequence of implementation – cannot do everything at once.
- Have to run a test on the low to be sure of impact before full implementation.
- Allows for quicker implementation of those easier or lower cost without waiting.
- Take care of controls in the tables to address connectivity since they were removed from 010 – where applicable
- Concerned about overhead and oversight and approval from regions – subject to subjectivity – every entity plan will have to be processed by the region
- What to demonstrate we are moving forward – if set a future date, any delay waiting for that date makes it look like industry is not forward – better to show some in industry are moving forward and not waiting.
- Disappointed that proposal offered to FERC without discussing with sub-group or full team – be careful not to introduce complexity – advantages to letting entities to move forward but danger of adding complexity – better to give industry reasonable firm times in which to comply – need to be less concerned about when low impact entities comply and focus on the high
- Scott Mix did not bring up the plan at FERC meeting– Alan Mosher did.
- Some of the "lows" have access to higher assets through IP.
- Need to file an implementation plan ready for time of posting.
- Need to start drafting soon – need direction on how to proceed.
- Is it based on a fixed date per requirement per impact or flexible date with submission of implementation plans for approval by regions?
- Come back with a formal proposal for members to express a preference.

On Thursday, Scott Mix offer the following Implementation Plan options for the SDT's consideration:

1. **Multiple fixed dates (based on connectivity and dependent on impact level)**
   4 -6 3 -8 2 -5 1 -0= **58 (3.2 of 4)**

2. **Entity-specific implementation plan**
   a. need to develop boundaries and approval guidance
   b. resource issues at regions for approving plans
   c. multiple versions in play at the same time for audits
   d. will require "true-up" of CIP 011 requirements for connectivity, etc.
   e. consistent with current NGP plans
   4 -3 3 -11 2 -4 1 -1= **54 (2.8 of 4)**

3. **Single fixed date (independent of impact level)**
   4 -4 3 -9 2 -3 1 -2=**51 (2.8 of 4)**

4. **Fixed date for each requirement, for each impact level**

a. some requirements would be the same for all levels
b. may have issues with "early compliance
c. will require a separate plan for NGP

4 -0 3 -1 2 -14 1 -4= **35 (1.8 of 4)**

SDT Questions and Comments:

- #4 – when do I need to be in compliance? I cannot give you a date, not to mention the inconsistency of being in compliance with one element before another
- Only alternative is reduce the number of dates and gloom them together – getting it done early may be detrimental – should improve reliability by allowing early compliance
- Cyber system and cyber system components are different – suppose to be looking at functions –
- This is a complex system with many components – I apply patches to individual components
- For nuclear plants – are they allowed to beyond the recommended date? Why is it an either or choice here? Is there a hybrid? Some fixed dates under #2
- Some might be fixed date but other programs may lend themselves to early implementation.
- Option 2 is more successful in nuclear arena – scope is more focused – with electric industry looking at vastly larger and more diverse set
- Favor a set date – option #3 – fixed and singular independent of impact level
- SE – difference between requirements makes for a nightmare for implementation under option #4. Option #2 may work well for entities with multiple business units
- multiple fixed dates based on connectivity and dependent on impact level as option 1
- Option 2 is based on entity registration

C. Low Impact Baseline

- Do we need to modify something in the governance section to identify low to better depict what is included in low?
- Put everything up in R1 but detail in the subsequent requirements – hard to follow – if R1 is the baseline, it only looks like an outline and needs more – Sub teams need to know how to proceed
- Sounds risky to go off and just assume it will be dealt with in R1.
- Sub teams would need to identify and shift words up to R1.
- Clarifies next steps for sub teams.
- Do we need to revisit decision to shove everything up to R1 and governance? Better to put baseline in the individual areas to tailor to the need.
- R1 doesn't have the detail needed – need the detail in the individual areas
- Jan Bargen, FERC, noted the format presentation by John Van Boxtel would offer you the opportunity to identify the detail you need in each section.
- Articulate the baseline in the table for each section?
- References in the technical controls are not tied back to R1.

- Controls do not appear to be well fleshed out at this time in current form putting everything up in R1.
- The requirements themselves are the policy – go through and identify those that need more clarity and lift them up to a table in R1.
- Should we address connectivity with low?
- Not addressing levels, applies to H-M-L – concern is to protect from upstream.
- If have a routable connection it should be higher – substations connected to control center or control system – it is the connectivity we are trying to protect, not the individual substation.
- John Van Boxtel's presentation allowed for recognizing that connectivity.
- Everything to date has focused on BES assets – paradigm shift to look at the connectivity – if routable connection to substation, it should not raise the level of every relay in the substation.
- It is the level of protection on the low item needs to be higher if it is connected – but only for certain requirements.
- Taking it down into the individual areas and put into our requirements, not sending it over to move into R1.
- Agree, but don't need policy in every requirement – do not need to write new policy requirements.

V. NEXT STEPS AND ASSIGNMENTS

Following the Sacramento meeting it was agreed there would be a need for weekly sub-team meetings and possible sub-team leads meetings. Later in June the schedule would be adjusted to reflect this and include some SDT meetings to develop drafts for NERC staff to review in advance of the July meeting in Pittsburgh.

The Chair suggested convening the SDT to review a new draft schedule the following week once more information was available from NERC and the Standards Committee.The Chair thanked Kevin Sherlin for his excellent support for the SDT in hosting this meeting.
The meeting adjourned at 11:00 p.m. on Friday, June 11, 2010

_____

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Appendix # 1— Meeting Agenda

Project 2008-06 Cyber Security Order 706 SDT
Draft 23rd Meeting Agenda
June 8, 2010, Tuesday- 8:00 AM to 5:00 PM PDT
June 9, 2010 Wednesday- 8:00 AM to 5:00 PM PDT
June 10, 2010 Thursday- 8:00 AM to 5:00 PM PDT
June 11, 2010 Friday- 8:00 AM to 12:00 PM PDT
Sacramento, California

NOTE:
1. Agenda Times May be Adjusted as Needed during the Meeting
2. Drafting Team Meetings May Not Have Access to Telephones and Ready Talk

Proposed Meeting Objectives/Outcomes:

- To review the CSO 706 SDT 2010 Work plan and Schedule;
- To review and adopt CSO 706 SDT 2010 Consensus Procedures draft;
- To receive updates on other related cyber security initiatives;
- To review the results of the FERC/NERC May 27 Meeting;
- To review the results of the May 19-20 Dallas Technical Workshop;
- To review the documents to be produced for the July, 2010 CIP posting;
- To receive an overview of the industry informal comments on CIP 010 and 011;
- To review industry input on the CIP format and to test SDT consensus on CIP format going forward;
- Sub-teams review industry input from the Technical Workshop and informal comments and propose any potential changes in the draft standards;
- SDT reviews Sub-Team reports on industry input from workshop and informal comments and any proposed changes in the draft standards;
- To review progress on the Implementation Plan Drafting Group and the Guidance Document Drafting Group; and
- To agree on next steps and assignments

Draft Agenda

Tuesday, June 8, 2010 8:00 a.m.-5:00 p.m.

- Introduction, welcome and opening remarks
- Discussion of CSO 706 SDT Work plan and schedule: June-December, 2010- *Stu Langton*
- Review and seek agreement on Drafting Team Proposal for refining the SDT Consensus Procedures
- Updates on other related cyber security initiatives- *NERC Staff and SDT Members*

- Review results of the May 27, 2010 NERC/SDT Meeting with FERC and guidance for sub-teams
- Review Technical Workshop overview and results
- Initial Overview of Industry Response to Request for Informal Comments
- Review of industry input on CIP format and consensus testing on CIP format going forward
- Sub-Teams meet to review and discuss industry comments *(Afternoon)*

Wednesday, June 9, 2010 8:00 a.m.-5:00 p.m.

- Sub-Team Meetings, Cont'd *(till mid-day)*
- Sub-Team Reports and SDT Discussion- Key Issues, Comments and Possible Changes to Requirements. *(Afternoon)*

Thursday, June 10, 2010, 8:00 a.m.-5:00 p.m.

- Sub-Team Reports and SDT Discussion- Key Issues, Comments and Possible Changes to Requirements

Friday, June 11, 2010, 8:00 a.m.-12:00 p.m.

- Review Next Steps and Sub-Team Schedule and Production of new Draft Requirements and related filing documents.
- Review the SDT Pittsburgh Meeting Agenda and Perform the Meeting Evaluation
- Review Implementation Plan Drafting Team progress and next steps
- Review Guidance Document Drafting Team progress and next steps

Appendix # 2 Attendees List
June 8-11, 2010, Sacramento CA

Attending in Person — SDT Members and Staff

1. Jim Brenton	ERCOT
2. Jay S. Cribb	Southern Company Services
3.Joe Doetzl	Kansas City Pwr. & Light Co (T/W/Th)
4. Sharon Edwards	Duke Energy (T/W/Th)
5.Gerald S. Freese	America Electric Pwr. (T/W/Th)
6. Jeff Hoffman	U.S. Bureau of Reclamation, Denver
7. Phillip Huff, Vice Chair	Arkansas Electric Coop Corporation (W/T/Fr)
8. Doug Johnson	Exelon Corporation – Commonwealth Edison
9. Patricio Leon	Southern California Edison
10. John Lim, Chair	Consolidated Edison Co. NY
11. David Norton	Entergy (T/W/Th)
12. David S. Revill	Georgia Transmission Corporation
13. Scott Rosenberger	Luminant Energy (T/W/Th)
14. Kevin Sherlin	Sacramento Municipal Utility District (W)
15. Jonathan Stanford	Bonneville Power Administration
16.Tom Stevenson	Constellation (W/Th/F)
17.Keith Stouffer	National Institute of Standards & Technology (T/W/Th)
18. John Van Boxtel	WECC (T/W/Th)
19. John D. Varnell	Technology Director, Tenaska Power Services Co.
Scott Mix	NERC
Roger Lampila	NERC
Howard Gugel	NERC
Joe Bucciero	NERC/Bucciero Consulting, LLC
Robert Jones	FSU/FCRC Consensus Center
Stuart Langton	FSU/FCRC Consensus Center

SDT Members Attending via ReadyTalk and Phone

Rob Antonishen	Ontario Power Generation (T/W)
Jackie Collett	Manitoba Hydro (W/Th/F)
Frank Kim	Hydro One Networks Inc. (Th/F)
Rich Kinas	Orlando Utilities Commission (T)

SDT Members Not Participating

William Winters	Arizona Public Service, Inc.

Others Attending in Person

Jan Bargen	FERC
Summer Esquerre	Next Era Energy (FPL)
Jim Fletcher	American Electric Power
Joel Garmon	Next Era Energy (FPL)
Michael Keane	FERC
Jerry Mercado	SMUD
Sam Merrell	CERT/Software Engineering Institute
Brian Newell	American Electric Power
Guy Zito	NPCC

Others Attending via Readytalk and Phone

June 8, 2010, Tuesday

Annette	Johnston	Mid American Energy
Justin	Kelly	FERC
Peter	Kuebeck	FERC
Drew	Kittey	FERC
Jerome	Farquharson	Burns McDonald
Daniel	Bogle	FERC
Ingrid	Rayo	Constellation
Rod	Hardiman	Southern Company
Bill	Glynn	Westarenergy
Steve	Newman	Mid American Energy

June 9, 2010, Wednesday

Rod	Hardiman	Southern Company
Ingrid	Rayo	Constellation Energy
Jerome	Farquharson	Burns McDonald
Peter	Kuebeck	FERC

June 10, 2010, Thursday

Drew	Kittey	FERC
Peter	kuebeck	FERC
Rod	Hardiman	Southern Company
Justin	Kelly	FERC
Jerome	Farquharson	Burns & McDonald
Ingrid	Rayo	Constellation Energy

June 11, 2010

Ingrid	Rayo	Constellation Energy
Rod	Hardiman	Southern Company
Annette	Johnston	Mid American Energy

Appendix #3 NERC Antitrust Compliance Guidelines

I. General

It is NERC's policy and practice to obey the antitrust laws and to avoid all conduct that unreasonably restrains competition. This policy requires the avoidance of any conduct that violates, or that might appear to violate, the antitrust laws. Among other things, the antitrust laws forbid any agreement between or among competitors regarding prices, availability of service, product design, terms of sale, division of markets, allocation of customers or any other activity that unreasonably restrains competition.

It is the responsibility of every NERC participant and employee who may in any way affect NERC's compliance with the antitrust laws to carry out this commitment.

Antitrust laws are complex and subject to court interpretation that can vary over time and from one court to another. The purpose of these guidelines is to alert NERC participants and employees to potential antitrust problems and to set forth policies to be followed with respect to activities that may involve antitrust considerations. In some instances, the NERC policy contained in these guidelines is stricter than the applicable antitrust laws. Any NERC participant or employee who is uncertain about the legal ramifications of a particular course of conduct or who has doubts or concerns about whether NERC's antitrust compliance policy is implicated in any situation should consult NERC's General Counsel immediately.

II. Prohibited Activities

Participants in NERC activities (including those of its committees and Subroups) should refrain from the following when acting in their capacity as participants in NERC activities (e.g., at NERC meetings, conference calls and in informal discussions):

- Discussions involving pricing information, especially margin (profit) and internal cost information and participants' expectations as to their future prices or internal costs.
- Discussions of a participant's marketing strategies.
- Discussions regarding how customers and geographical areas are to be divided among competitors.
- Discussions concerning the exclusion of competitors from markets.
- Discussions concerning boycotting or group refusals to deal with competitors, vendors or suppliers.

III. Activities That Are Permitted

From time to time decisions or actions of NERC (including those of its committees and Subgroups) may have a negative impact on particular entities and thus in that sense

adversely impact competition. Decisions and actions by NERC (including its committees and Subgroups) should only be undertaken for the purpose of promoting and maintaining the reliability and adequacy of the bulk power system. If you do not have a legitimate purpose consistent with this objective for discussing a matter, please refrain from discussing the matter during NERC meetings and in other NERC-related communications.

You should also ensure that NERC procedures, including those set forth in NERC's Certificate of Incorporation and Bylaws are followed in conducting NERC business. Other NERC procedures that may be applicable to a particular NERC activity include the following:

- Reliability Standards Process Manual
- Organization and Procedures Manual for the NERC Standing Committees
- System Operator Certification Program

In addition, all discussions in NERC meetings and other NERC-related communications should be within the scope of the mandate for or assignment to the particular NERC committee or Subgroup, as well as within the scope of the published agenda for the meeting.

No decisions should be made nor any actions taken in NERC activities for the purpose of giving an industry participant or group of participants a competitive advantage over other participants. In particular, decisions with respect to setting, revising, or assessing compliance with NERC reliability standards should not be influenced by anti-competitive motivations.

Subject to the foregoing restrictions, participants in NERC activities may discuss:

- Reliability matters relating to the bulk power system, including operation and planning matters such as establishing or revising reliability standards, special operating procedures, operating transfer capabilities, and plans for new facilities.
- Matters relating to the impact of reliability standards for the bulk power system on
- electricity markets, and the impact of electricity market operations on the reliability of the bulk power system.
- Proposed filings or other communications with state or federal regulatory authorities or other governmental entities.
- Matters relating to the internal governance, management and operation of NERC, such as nominations for vacant committee positions, budgeting and assessments, and
- employment matters; and procedural matters such as planning and scheduling meetings.

Any other matters that do not clearly fall within these guidelines should be reviewed

with NERC's General Counsel before being discussed.

APPENDIX # 4
CSO 706 SDT MEETING SCHEDULE
APRIL –DECEMBER 2010

CSO 706 SDT SCHEDULE: FULL CIP-010 & CIP-011 PACKAGE		
Week Of	***Key Dates***	***CIP Task***
4/12/2010	**SDT Meeting Atlanta, GA (Southern Co) (4/13-16)**	**Present Controls draft for full SDT review and comment. Sub team drafting. Finalize draft for Informal Comment, Full Package**
4/19/2010	4/19-4/23/2010 4/23/2010	**SDT Sub-Teams and Leads Meet to Finalize Documents NERC Receives and Prepares Full Package for Industry Comment**
4/26/2010	**4/26/2010 4/27/2010 4/28/2010 4/29/2010**	**SDT Sub-Teams Develop Package SDT Reviews with NERC Staff Proposals SDT Scoping Meeting on Documents SDT Reviews and Approves Full Package for 30-day Industry Comment Period**
5/3/2010	**5/4/2010**	**Informal Comment Posting for full package starts Completes on 6/3/2010**
5/10/2010	**SDT Meeting Dallas, TX (Luminant) (5/11-13)**	**Review Parking Lot Issues, Prepare for Industry Workshop and Begin Development of Guidance Documents**
5/17/2010	5/19 & 5/20/2010	**1.5-day Industry Technical Workshop (Dallas, TX)**
5/24/2010	5/24 to 5/28/2010 5/27/2010	**SDT Considers Comments from Workshop Meeting with FERC Staff to Review Draft Standards and Posting**
5/31/2010	6/3/2010 6/4/2010	**Informal comment period ends SDT Reviews Comments Received Sub team meetings to Review Comments Received**
6/7/2010	6/7/2010 **SDT Meeting, Sacramento, CA (SMUD) (6/8-11)**	**Sub team meetings to Review Comments Received Industry comment review, response process, re-drafting, as needed**
6/14/2010		Sub team meetings to prepare sections for review

CSO 706 SDT SCHEDULE: FULL CIP-010 & CIP-011 PACKAGE		
Week Of	***Key Dates***	***CIP Task***
6/21/2010	SDT Meeting and Subteams via ReadyTalk	SDT interim online meetings and Sub-team meetings to prepare sections for review
6/28/2010	SDT Meeting and Subteams via ReadyTalk	SDT interim online meetings and Sub-team meetings to prepare sections for review
7/5/2010	NERC Staff review	Sub teams complete all work assignments & NERC Review
7/12/2010	**SDT Meeting, Pittsburgh, PA (CERT) (7/13-16)**	**Finalize & Approve Documents for posting for 45 day formal comment period**
7/19/2010	7/19/2010 7/21/2010 7/21/2010	**-NERC seeks SC Approval for Ballot** **-Post CIP Standards for Formal Comment** **-45 Day formal comment period begins (closes on 9/3/2010)** **-Begin Ballot Pool Formation**
7/26/2010		**Formal comment period for CIP standards** **Prepare for industry webinar**
8/2/2010		**Formal comment period for CIP standards** **Prepare for industry webinar**
8/9/2010	**SDT Meeting, Chicago, IL (ComEd) (8/10-13)**	**Formal comment period for CIP standards** **Finalize presentation for industry webinar**
8/16/2010	8/17/2010 8/19/2010	**Hold Industry Webinar (tentative)** **Ballot Pool Formation Ends**
8/23/2010	8/25/2010	**Initial Ballot Begins**
8/30/2010	9/3/2010	**Initial Ballot Ends**
9/6/2010	**SDT Meeting Winnipeg, Canada (Manitoba Hydro) (9/7-10)**	**Review ballot results** **Respond to comments received** **Draft revisions to standards**
9/13/2010		Sub-team meetings
9/20/2010	9/20/2010	Sub-team meetings, NERC Staff Review

CSO 706 SDT SCHEDULE: FULL CIP-010 & CIP-011 PACKAGE		
Week Of	***Key Dates***	***CIP Task***
	9/24/2010	Full SDT on-line meeting to approve revised draft of documents for re-ballot
9/27/2010	9/27 to 10/6/2010	Re-Ballot Period
10/4/2010	10/6/2010	Re-Ballot ends; comments received by SDT
10/11/2010	**SDT Meeting, Toronto, Canada (OPG) (10/12-15)**	**Prepare responses to 2nd ballot comments**
10/18/2010		**Sub-teams meet to adjust requirements, as needed**
10/25/2010	10/25/2010 10/29/2010	**-Prepare and finalize revisions to standards** **-NERC Staff review** **-SDT Approval for re-ballot (if needed)**
11/1/2010	11/1 to 11/10/2010	3rd Ballot Period (if needed)
11/8/2010	11/10/2010	Ballot period ends
11/15/2010	**SDT Meeting, Baltimore, MD (Constellation Energy) (11/16-19)**	**Prepare responses to 3rd Ballot comments**
11/22/2010		*NERC and SDT finalize responses to ballot package*
11/29/2010		*Seek SC and BOT Approval for Filing*
12/6/2010		*Seek SC and BOT Approval for Filing*
12/13/2010	**SDT Meeting Tampa, FL (FRCC) (12/13-17)**	**SDT Meeting to review Filing** **Completion of Phase 2**
12/24/2010		***Submit for Regulatory Approval***

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Appendix #5 SDT Consensus Procedures
CYBER SECURITY FOR ORDER 706 STANDARD DRAFTING TEAM
Proposed Refined Consensus Guidelines (June, 2010)

The Cyber Security for Order 706 Standard Drafting Team (Team) will seek consensus on its recommendations for any revisions to the CIP standards.

Consensus Defined. Consensus is a participatory process whereby, on matters of substance, the Team strives for agreements which all of the members can accept, support, live with or agree not to oppose. In instances where, after vigorously exploring possible ways to enhance the members' support for posting CIP standards documents for industry comment or balloting, and the Team finds that 100% acceptance or support of the members present is not achievable, decisions to adopt standards documents for balloting will require at least 75% favorable vote of all members present and voting. This super majority decision rule underscores the importance of actively developing a Team consensus on substantive issues which the industry will need to approve by a 2/3's vote.

~~***Postings for Industry Comment.*** *For decisions on CIP standards documents to be posted for industry comment where the Team finds that 75% acceptance or support is not achievable but an option or options under consideration had greater than 50% support from the Team, the Team's accompanying Comment form will seek industry input to help the Team resolve any differences and select an option going forward.*~~

Quorum Defined. The Team will make decisions only when a quorum is present. A quorum shall be constituted by at least 2/3 of the appointed members being present in person or by telephone.

Electronic Mail Voting. Electronic voting will only be used when a decision needs to be made between regular meetings under the following conditions:

- It is not possible to coordinate and schedule a conference call for the purpose of voting, or;
- Scheduling a conference call solely for the purpose of voting would be an unnecessary use of time and resources, and the item is considered a small procedural issue that is likely to pass without debate.

Electronic voting will not be used to decide on issues that would require a super majority vote or have been previously voted on during a regular meeting or for any issues that those with opposing views would feel compelled to want to justify and explain their position to other team members prior to a vote. The Electronic Voting procedure shall include the following four steps:

1. The SDT Chair or Vice-Chair in his absence will announce the vote on the SDT mailing list and include the following written information: a summary of the issue being voted on and the vote options; the reason the electronic voting is being conducted; the deadline for voting (which must be at least ~~*4*~~ 12 hours after the time of the announcement).

2. Electronic votes will be tallied at the time of the deadline and no further votes will be counted. If quorum is not reached by the deadline then the vote on the proposal will not pass and the deadline will not be extended.
3. Electronic voting results will be summarized and announced after the voting deadline back to the SDT+ mailing list.
4. Electronic voting results will be recapped at the beginning of the next regular meeting of the SDT.

Consensus Building Techniques and Robert's Rules of Order. The Team will develop its recommendations using consensus-building techniques with the leadership of the Chair and Vice Chair and the assistance of the facilitators. Techniques such as brainstorming, ranking and prioritizing approaches will be utilized. The Team's consensus process will be conducted as a facilitated consensus-building process. Only Team members may participate in consensus ranking or votes on proposals and recommendations. Observers/members of the public are welcome to speak when recognized by the Chair, Vice Chair or Facilitator. The Team will utilize Robert's Rules of Order *(as per the NERC Reliability Standards Development Procedure),* as modified by the Team's adopted procedural guidelines, to make and approve motions. However, the 75% super-majority voting requirement will supersede the normal voting requirements used in Robert's Rules of Order for decision-making on substantive motions and amendments to motions. The Team will develop substantive written materials and options using their adopted facilitated consensus-building procedures, and will use Robert's Rules of Order only for formal motions once the Chair determines that a facilitated discussion is completed.

Appendix #6- FERC Meeting Summary May 27, 2010

Cyber Security Order 706 SDT — Project 2008-06
SDT Meeting with FERC Staff and Industry Stakeholders
May 27, 2010 Meeting Summary
FERC's Offices
Washington, DC
Joe Bucciero

Meeting Executive Summary

Atmosphere was cordial and professional, and the meeting was constructive.

FERC staff agreed with the approach taken in the draft CIP-010 and CIP-011 standards, but acknowledged that a lot of work is still needed in clearly defining the requirements.

FERC staff expressed concern that the Low impact level requirements are insufficient and need to be bolstered. The Low baseline is too low.

The proposed 36-month review of the categorization needs to be shortened, at least for the first review cycle (possibly to 12 months)

Beware of hidden requirements in the purpose statements of the requirements, and review with the intent to minimize the adjectives used in the text (e.g., sufficient, proper, adequate, etc.) and clarify what is required with respect to auditability and enforceability.

The bright line thresholds stated in Attachment II need to be justified or at least explained.

The SDT must ensure that all of the requirements are auditable.

Concern was expressed on the deferring of some FERC directives until next year.

FERC staff recognizes that the schedule of the project is ambitious, and appreciates the monumental effort being performed by the SDT in creating these standards.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Cyber Security Order 706 SDT — Project 2008-06
SDT Meeting with FERC Staff and Industry Stakeholders
May 27, 2010 Meeting Summary
FERC's Offices
Washington, DC

Joe Bucciero

1. Introductions and Anti-Trust Guidelines

Regis Binder, FERC, welcomed the NERC SDT members, industry stakeholders, and other participants to the meeting and covered meeting logistics. Joe Bucciero conducted a roll call of members and participants in the room and on the conference call, and reviewed the need to comply with NERC's Antitrust Guidelines.

John Lim, SDT Chair, thanked FERC for hosting the meeting and providing the meeting room and facilities. He also reviewed the proposed meeting agenda.
FERC staff stated that they are not speaking for the Commission, and they recognize the importance of the cyber security issues to the industry and the country. FERC staff recognized the magnitude of the herculean effort and the excellent hard work being done by the SDT, in addition to everyone's day jobs, and stated this effort was fully appreciated.
The proposed agenda for the meeting is included as an attachment to this meeting summary. FERC staff was encouraged to ask questions throughout the presentation/discussion offered by the SDT regarding the new draft CIP standards.

2. Review of CIP-010-1

John Lim reviewed the strategy, approach, and history of CIP-010-1. The primary objectives of this standard are to: (1) help scope the electric system assets that are within the purview of the CIP-010 and CIP-011 standards; and (2) establish a list of reliability functions and "bright-lines" for categorization of the BES cyber systems.

a. Discussion of Scope

The process and criteria currently being used today for identifying critical assets in the electric system are thought to be inadequate. For example, less than 5% of the existing generation facilities around the country are considered to be critical assets, so the SDT has identified a new approach in the new CIP-010-1 standard.
The scoping process in the existing CIP-002 standard calls for identification of critical bulk electric system assets, then the associated critical cyber assets. In CIP-010, there are no 'out of scope' bulk electric system assets; instead a categorized list of those assets and their related cyber systems is required. That is one of the major differences between CIP-002 and CIP-010.

Attachment I of the draft CIP-010 standard is meant to provide the definition of scope and applicability. CIP-010 requires the categorization of cyber systems by defining a list of the real-time reliability functions that could have an impact on the reliable operation of the bulk electric system, and if a cyber system is doing any of those functions, then it is within scope.
Categorization of the electric system assets and the cyber systems based on multiple levels (High/Medium/Low) of their potential impact on the reliable operation of the bulk electric system is key aspect of the new draft CIP-010 & CIP-011 standards.
Attachment II of the draft CIP-010 standard is meant to provide the criteria or "bright lines" to identify the potential impact (High/Medium/Low) on the reliable operation of the bulk electric system if the electric system asset or its cyber systems are destroyed, degraded, misused, or otherwise rendered unavailable. The concept is to take a more holistic view and move away from consideration of individual critical cyber asset issues, and place more focus on 'system' impacts.
One of the significant concepts behind collapsing the CIP-003 to CIP-009 standards into a single standard was to clarify the requirements for audit purposes and reduce the incumbent paper work thereby providing focus on the security of the key cyber systems. The SDT is concerned about the auditability of the requirements, and wants to ensure that the CIP-010 and CIP-011 requirements are auditable.

b. Discussion of Response Time

The CIP-010 requirements apply to cyber systems that are relevant to real-time operations (not long term planning or systems that do engineering or marketing). The current benchmark parameter is "impactful within 15 minutes", where the 15 minutes relates to when the incident occurs. Discussion and feedback from the industry to determine if the 15 minute parameter is appropriate has been solicited through the recent informal posting and comment form for the draft CIP-010 and CIP-011 standards.

c. Discussion of Bright Lines

Question: In CIP-010 R1, the phrase "execute or enable" is used; what is meant by enable?

> In some cases, a cyber system directly performs a function (as identified in Attachment I), but in other cases (e.g., data collection/aggregation or display) it is providing information to an operator or other systems to enable functions.

Staff observation: Once these draft CIP standards are filed, they will create a different benchmark or situation from the existing CIP standards for the industry to consider. Are we improving or not? What is the key yard stick? There seems to be a general belief that the number of assets identified to be critical to reliable operation of the BES under CIP-002 is inadequate (i.e., not enough assets being identified, less than 5% of generation). When these new draft CIP standards are filed, how can it be demonstrated

that the key assets are identified? The size of unit is not the necessarily the key. Is the "medium" level of impact adequate for the number of units that can potentially fall into that category?
The intent is for the new CIP-010 standard to be comprehensive, in that all bulk electric system and cyber system assets will be covered to some level of impact. The "bright lines" are being provided to help clarify the assignment of the appropriate level of impact to each of the BES Cyber System assets. The SDT recognizes that measuring impact against what is considered 'critical' today is not good enough since today's results are not acceptable.
The SDT is looking for guidance from all industry participants with a stake in the game as to what is acceptable for the bright lines, and hoping to receive some guidance through the informal comments from the industry.

Allen Mosher: The draft CIP-010 standard is an improvement over what we have today, and we need to implement it soon. It's difficult to compare it to what we have today, because we have a different paradigm. We want to maximize our effort to identify the most critical assets and focus on the control systems. We should worry most about common use failures and wide spread loss of the bulk electric system.

Gerry Adamski: What are the criteria for identifying if an approach is adequate? What is adequate, and how do we identify it to help tweak the product? A thoughtful dialogue may be needed to better define the "bright lines" in Attachment II.
While the number of megawatts or the size of a unit can be one of the criteria used, the impact on day-to-day operations is also very important. The SDT should have a solid basis for the numbers used in Attachment II to define the "bright lines" that are used in the draft CIP-010 standard.

For example, generators, units, plants, etc. that are used intermittently, are they single or multiple control systems? The number of generation MWs connected to assets or to the control systems? If three units combined are over 2000 is it a High impact system? Are three separate control systems that are networked together a single cyber system? How does contingency analysis factor into the impact level criteria evaluation, if at all?
It might be helpful if the SDT can quantify the number of MWs of generation that would be classified as High impact using the new draft CIP-010 standard vs. today under the CIP-002 standard.

A re-ordering the "bright lines" criteria identified in Attachment II should be considered, putting the control center criteria first.

FERC expressed concern that the requirements applicable to the Low impact criteria are not sufficient, and that the Low/Medium impact bright line is set too high.
Throughout CIP-010 there are references to quantities of MW; how were those quantities selected? Adding insight into how the values were determined (e.g., was a study done; is it from operating experience) would be very helpful. NERC indicated

that many of the bright-line values came from a variety of resources available to NERC, plus active participation and input from OC & PC members in the development of the standards. FERC does not have a magic study to use in its review and assessment of the bright lines.

d. Discussion of Guidance and Auditing

The SDT members agree that guidance is necessary for each of the requirements. There hasn't been enough time spent to-date to fully develop or flesh out guidance on each requirement.
There is reason to believe not everyone knows or can identify all the key assets that auditors are concerned about, since the auditors learn something new every time they perform an audit.
Two NERC auditors have been engaged with the process of defining these new draft CIP 010 & CIP-011 standards as well as participation from the regional entities. There were many auditors involved in last week's SDT technical workshop held in Dallas, TX.
The easiest standard to audit is a checklist, but that is the worst way to audit.
Transparency is needed on how an entity is audited. The entity needs to know how the audit will be approached. In the filing, a summary description of what discretion is left to the entity may be helpful.
NERC will have its audit department staff review the draft CIP standards and provide comments from an auditor's perspective. Are the "bright lines" bright enough?

e. Discussion of Compliance Review Schedule

The draft CIP-010 R3 requires at least a 36 month review cycle, since the bulk electric system doesn't change that much that often. Currently a three year process is used by the entities as a review trigger for going back to look at the standards and consider if any changes have occurred that would impact the High/Medium/Low categorizations. What are the triggering events for this review? Possibly the SDT should consider that a one to two year review cycle is needed at first, and then followed by the traditional three year cycle.
How assets are allowed to move from one category to another over time may be critical. Where should these requirements be addressed; in the audit process? Also, do we need to address assets that may be critical to a neighboring entity but may not be critical to my entity even though my entity controls the assets?

3. Review of CIP 011-1

Phil Huff provided an overview of CIP-011 and led the discussion. The overall approach by the SDT was to combine CIP-003 through CIP-009 into one standard, taking into account the FERC directives, the SDT's review of the DHS catalogue of cyber security requirements, and incorporation of those requirements that would be beneficial to the reliability of the BES.

a. Discussion of One vs. Multiple Standards

CIP-011 is viewed as one standard with many parts, and as such putting all of the requirements together in one standard would tend to minimize the possibilities for multiple violations of the same standard, and the number of violations in general. Retaining the multiple standards approach would tend to make synchronization of the requirements and versioning of the multiple standards more difficult, resulting in possible multiple reporting of violations for the same standard. Retaining the multiple standards approach would possibly make it easier for entities to split up the CIP requirements for implementation and monitoring in a way to match the unique organization of the entities.
The SDT is divided on the issue of format for CIP-011 – putting in one standard communicates the standards should be seen as one – multiple standards makes it easier to change individual standards, separately, but creates the compliance issue of potentially multiple violations across multiple standards for the same identified problem. The single standard approach would simplify the ability to incrementally change the full standard. On the other hand, given the way violations are reported now, one standard may result in this standard standing out like a sore thumb if it combines so many requirements.
The SDT wanted to ask the question regarding format of the CIP-011 standard to gain some industry feedback, since the SDT itself could not reach a super majority decision on the best format approach. The SDT wants industry feedback on the approach, including if it makes sense.

b. Discussion of the Requirement Tables

A new feature in CIP-011 is how the requirements are presented, which is based on applicability/impact on the reliable operation of the BES. There are several subject areas identified in CIP-011, including: security governance and policy; personnel training, awareness, and risk assessment; physical security; electronic access control; etc. Each requirement has several characteristics identified, and each requirement is assigned to one of the subject areas. A requirement is represented in the CIP-011 draft standard through a table that groups together all of the requirement's characteristics.
A few questions were raised by FERC staff regarding the requirements tables in CIP-011. For example, what is the intent of the 'blank' entries in a table? Are entities required to do anything? Can an entity be found in violation of a requirement if the corresponding table entry is blank? Should entities look at the rows in a table to determine compliance with the requirement?

c. Discussion of Specific Requirements and Wording

CIP-011 R1.3: What is the intent? The requirement to clearly identify a senior senior manager is not really stated in the requirement. The requirement is for the entities to

designate a single official. How do you determine that, and when do you have to designate this individual? Nothing specifically says an entity shall designate this individual.
The training requirements seem to be scattered around the CIP-011 draft standard. Possibly a consolidation of the training requirements would be helpful. Also the choice and use of words such as 'training' vs. 'education', vs. 'credentials' needs to be reviewed for consistency of meaning. What is 'sufficient' training? Need to include a sense of frequency and magnitude around the training requirements.
Overall, the SDT needs to review the draft CIP standards with respect to the use of adjectives (e.g., sufficient, proper, adequate, etc.) and clarify what is required with respect to auditability and enforceability. For example, R5 vs. R16/R18 states "ensuring" vs. "guaranteeing". Which one is correct?
The SDT acknowledged that this draft of CIP-011 was prepared by multiple subteams within the SDT, and the multiple teams did not always use consistent language in developing the requirements. The SDT has been focused on developing compliance elements, but is now focused on writing the requirements clearly while also minimizing the need for TFEs.

d. Form and Format Issues

The Enforcement office at NERC is looking at the draft CIP standards with respect to the needs for enforceability and compliance, as well as the table structure of requirements. CIP 011 covers the requirements previously included in CIP-003 thru 009; have these requirements been incorporated or do the requirements from CIP-003 thru CIP-009 need to be maintained?
Some of the more document-focused requirements are no longer in the new draft standards. Does that meet the equally protective criteria? The intent is to improve the standards by removing the administrative requirements that do not improve reliability in any way.
The need for more than paper evidence of compliance may lead to actual need to demonstrate compliance. For example, current requirements call for paper demonstration rather than allow for actual demonstration of the protection system; the latter improves security. Creation of paper lists of authorized personnel is a Chinese fire drill that does not improve system security.
A mapping will be done to identify gaps in the standards that we will address in the version coming out in July for industry comment and ballot. The idea is to explain clearly why the gaps are there, and that these gaps do not affect the reliability of the BES.
One of the biggest issues is the perception of a culture of compliance. Now you have multiple violations of the same standard, and from the way it would be reported today, it would stick out. NERC/FERC need to make sure this does not present a skewed view of the CIP standards.
Concern was raised about the status of the components that make-up the tables. The 'R' (for requirement) is not used for the components in the table. How does that relate

to the roll-up methodology; what is and is not a requirement? What is the status of the actual wording in the parent requirement (ahead of the table), and how does it relate to the components in the table?
In Tables R4 to R9, there seems to be a general formula for the requirement, which is each responsible entity shall apply the criteria with a goal of preventing unauthorized access to BES cyber systems. However, a responsible entity that has a Low impact BES cyber system does not have an entry in the table that indicates that the entity has to address any of the subcomponents. Is that entity still subject to the requirements of R5? Similarly, if a Medium impact cyber system has in fact restricted physical access according to 5.1, but there is in fact an unauthorized access – would that be a violation of R5? The intent of the entries in the tables and the requirements needs to be clarified. How will the goal of preventing unauthorized access be accomplished on assets with Low impact, when there is no requirement defined?

e. Discussion of Applicable Time Barometer

The discussion centered around why was a 15 minute time period was selected as the barometer for the impact time stated in the draft CIP-010 standard. Isn't it dependent on current system conditions? Whatever time period is chosen will it be readily evident to the entities?
How quickly can it be determined that there is an impact on the bulk electric system? When does the impact happen? Is it objective enough for an entity to determine for purposes of verifying for audits?
Is a qualifier needed for peak electric system conditions or most stressful conditions? Time of year and load conditions may impact the determination of the time used.
The draft CIP standard is written around how the set of functions impact the reliable operation of the bulk electric system; some functions have more immediate impacts and others take longer to impact the BES.
Misuse of a system may have a longer lead time, far longer than fifteen minutes, but an equally devastating impact.
The SDT might need to revisit the definition or application of the fifteen minute time period.

4. Implementation Plan

Scott Mix provided a high level overview of the implementation plan concepts and issues being considered by the SDT. A subgroup has been formed to prepare the text for the Implementation Plan. They will likely start meeting during the SDT Meeting in June 2010 in Sacramento.
Scott Mix presented the slides he recently gave at the SDT Workshop in Dallas, TX. He noted that the plan is to retire CIP 002 and CIP 003-009 within a transition period as CIP-010 and CIP-011 become effective.

a. Discussion of Implementation Plan Issues

The SDT is working on relevant timetables for implementation of the draft CIP-010 and CIP-011 standards, including how to prioritize the effort in terms of importance and in terms of timing.

The SDT needs to try to identify in a general sense which assets will eventually fall into each of the High/Medium/Low impact categories and how many assets will be in each category. A significant benchmark between the CIP-002 and the CIP-010 & CIP-011 standards will be the number of assets involved, and has that number increased in size and scope.

How should the industry be incentivize to implement the new CIP-010 & CIP-011 standards, but not the Medium or Low impact controls at the expense of first focusing on the High impact assets. Possibly a 'rolling' implementation of the standards is in order.
What is the impact categorization of a BES cyber system if it moves up or down an impact level? How should it be considered in the implementation plan?
The Implementation Plan subteam will also work with the nuclear folks to discuss policies and impacts vs. an implementation schedule. Two stakeholders from the nuclear industry will be part of the implementation plan subteam.

Some level of reporting to FERC on implementation plan development (including content and schedule) is encouraged. The reporting should be designed to provide review of justifications, milestones, and accountability while offering a degree of oversight.
One possible scenario for implementation plan development would be for the entities to quickly develop their lists of categorized assets, immediately followed by the establishment of their respective implementation plan. The responsible entities should then report their implementation plans to the respective regional entity for approval. Guidance documents will be prepared by the SDT to provide a level of consistency and assistance in the development of the implementation plans. Potential conflicts between compliance deadlines and audit schedules must also be considered.
Allow entities to be compliant early especially through implementation of system upgrades that will need to be compliant later. We'll need to recognize that some entities may need additional time to do the job right while maintaining appropriate levels of oversight. For example, larger organizations may have a larger portion of assets affected by the new standards.

b. Discussion of Transition and Migration

A transition plan from the existing CIP-002 to CIP-009 requirements to the new draft CIP-010 and CIP-011 requirements is needed. Some CIP-011 requirements are a direct replacement for those in CIP-003-009 and a migration plan should be developed for those, while other requirements are new and an implementation plan is needed. Plans to guide the entity may be helpful to both the entity and the auditors.

A roadmap for the transition/migration activities would help in the development of a schedule to accomplish these tasks.

The draft CIP-011 standard does not appear to provide a significant base level of protection for the low and medium impact controls. FERC expressed concern that the controls requirements for the "low" impact systems do not provide an adequate level of protection. The blank entries in the tables in CIP-011 might imply that there are no control requirements.

c. Discussion of Physical Controls

Physical items or locations may have protection but may not be auditable as a NERC standard, which focuses on cyber assets. For example, substations have physical protection, but how can an auditor be convinced that the physical fence or padlock was there thirty days ago.
The focus of the SDT is on cyber security. The team considered a separate SAR for physical security. The issue is not when the fence went up, but was it secured and was the lock actually locked – actually visiting remotes sites to prove this might be too much.
Too much energy goes into such audits without corresponding benefit of protecting the system. An auditor might randomly select a few remote sites – because selection is random, but an entity would need to protect them all.

d. Discussion of Immediate Revocation

It's questionable if the industry can meet targets for "immediate revocation of access". Do timeframes of 72 hours work?

May need a primary and secondary revocation applied to remote and/or physical access – this will also depend on the "cause" for revocation.

What does "immediate" really mean in these cases? For example, an entity may need to revoke access of an individual before letting the person go for cause.

"Immediate" is not auditable, even if we set a time period. "As soon as possible" would be a better phrase or a set time period would be sufficient. If it is a planned termination, then it can be immediate because it precedes the termination. If it is part of an emergency, revocation may need a reasonable time period.

e. Discussion of Security Systems Protection

FERC suggested adding a fourth column to the tables in CIP-011 that would list the physical/cyber security system protection required for each asset. The intent is to apply

the appropriate level of security. It was also suggested that a function be added to the table in Attachment I of CIP-010 for security/protection systems.
Security systems impact the BES

Passwords – maximize use without being prescriptive – suggested language – cut down on TFE's

f. Beyond CIP-010 and CIP-011

FERC Order 706 included some directives (e.g., defense in depth) that have not been addressed so far. There was too little time to accomplish these requirements and it might have derailed the process to this point.
Concern is that some of the items may have been part of the paradigm shift FERC was asking for in Order 706. How can some of these items in the order be defined, or implemented, or audited, etc.?
Implementation of an active vulnerability assessment (testing) can be contrary to reliability and security. Special care and guidelines are needed for this requirement.
The December 2010 date for filing of the new draft CIP standards for approval by FERC is not one of the Commission directives. It can become an informational filing, since it is not making law, and may be changed with FERC approval. Need to implement improvements sooner, but may not be able to resolve issues now.
The SDT is planning to file the new draft CIP-010 and CIP-011 standards by December 2010, and will start in January 2011 to look at the other remaining issues – may be a continuously moving target.
Think about how to telegraph the issue to the industry
The recent SDT Technical Workshop was aimed in part at telegraphing this schedule to the industry and thereby telling them the new standards are not a completed deal.
'Defense in depth' is implementation of guidance or guidelines for layered security, that is guidance for designing but not necessarily an auditable requirement.
The SDT would benefit from a shared dialogue with FERC Staff on this and other issues about what we are trying to achieve, the overall objective, and what is needed for the industry to reach it. This dialogue would go beyond just the standards, but could also cover how you approach audits and compliance.
NERC and the SDT still have to legally deal with the directives in FERC Order 706, and ask for clarification in the December 2010 filing. The SDT may ask for clarification of specific parking lot issues, or maybe a separate filing on those issues should be developed.

5. Closing

The dialogue and sharing of information during this meeting was constructive and has been very useful.

The FERC staff reminded us that they do not speak for the Commission. They may not agree with the statements or agreements reached. However, with continued dialogue and progress on the issues we may at least achieve a mutual understanding of the problems and concerns being addressed.

Gerry Adamski asked FERC staff about their general sense of acceptability of the body of work to date? Also, what needs more work?

> The approach is responsive, but as discussed earlier, there are many questions remaining, including how the impact levels will be applied. There is still a lot of work to be done to achieve the filing by the end of 2010. It is an ambitious schedule, but there is recognition of the quality and amount of effort involved.

Meeting adjourned.

Appendix #7 "Parking Lot Issues"

CIP VERSION 4 PARKING LOT (JUNE, 2010)

Issue (Reference)	Raised By	Date Raised	Sub-Team Assigned	Resolution (Date)
Review clarity of item 1.1, Attachment 2 – Generation Facilities and criteria for Contingency Reserve and Reserve Sharing	Rich Kinas	4/29	CIP-002	**AI:** Revise item 1.1 with input from the industry through the informal comments received.
Shouldn't there be delegations made by the Senior Manager for any exceptions (CIP-011 R2 & R3)	Jackie Collett	4/29	Governance	**Resolved** by the revised CIP-011 text that was posted.
User type access (R3) 3.2 Review the need for network device training (Operators, etc.)	Jim Brenton	4/29	Physical/Cyber & Access Control	Possibly regarding the level of access for outward facing and inward facing devices. What type of user training is required for each level? **Add role-based access (e.g., admin vs. application level access) – physical access & training requirements. Awareness training for everyone, and role-based training as required.**
Combine tables for electronic and physical access control systems (R6, R20, & R22)	Philip Huff	4/29	Physical and System Security	**AI:** Double-check that the proper requirements are incorporated in the respective tables.
Remove ~~Training~~ Termination for physical	Doug	4/29	Physical	

Issue (Reference)	Raised By	Date Raised	Sub-Team Assigned	Resolution (Date)
access to Low Impact (R9)	Johnson			
What do the blank cells mean in the tables in instances where a timeframe is given? (R9)	Jackie Collette	4/29	Howard Gugel	Do they mean there is no requirement at that particular level? **AI:** Double-check the table entries to ensure that the entries are indicative of the requirement. Possibly a statement should be added to the Guidance Document that describes what is meant by a blank entry in a table.
Monitoring the baseline configuration means monitoring the physical location as written. (R23)	Rob Antonishen	4/29	Change Management (Dave Revill)	**AI:** Is baseline the right term? What do we mean by changing physical location?
What timeframe for issuing alerts (Table entry 18.2)	Jackie Collett	4/29	System Security	**AI:** What is the response time requirement? In what timeframe should the alerts be issued?
Need to address what disciplinary actions are? Should physical or cyber access be revoked?	Jackie Collett	5/11	Disciplinary actions (physical/cyber access)	AI:
Combine the revocation of physical and electronic access requirements (including remote access) into one topical area of the standard	Phil Huff	5/11/2010	Personnel access (Sharon Edwards)	**AI:** Need to investigate possible alternatives. Have a requirement to develop a procedure for handling

Issue (Reference)	Raised By	Date Raised	Sub-Team Assigned	Resolution (Date)
				revocation of access.
Review "objective" statements to ensure they do not implicate requirements	FERC	5/27/2010	All	
Make requirements text consistent throughout the Standard	FERC	5/27/2010	All	
Global review of adjectives like "sufficient", "appropriate", etc.	FERC	5/27/2010	All	
Baseline for Low level of Impact	Drafting Teams	6/10/2010	ALL	**Completed on 6/10/2010**
Description of Timing (e.g., annual, months, etc.)	Howard	6/10/2010	NERC	
Protection requirements for electronic and physical access control systems	Doug/Phil	6/10/2010	ALL	
Broad Application of TFE Statement	SDT	6/9/2010	ALL	
Gantt Chart for Compliance Deadlines	Varnell	6/9/2010	Howard	
Exclusion for Entities that don't own cyber systems	Doug	6/10/2010	Full SDT	

Appendix #8 Overview of Format Comments

011 FORMAT TOPICS

9. **Do you prefer the currently proposed format for CIP-011-1, which contains a complete single set of requirements? Do you prefer the alternate format, where the requirements are grouped in separate standards? Or do you have no preference?**

CIP 011 Combined Requirements Format

CIP 011 Combined Requirements Format – Question 9	Count	Percent
Keep CIP 011-1 as one document	48	40.3
Break CIP 011-1	38	31.9
No preference	23	19.3
Not checked	10	8.4
Total:	**119**	**100**

A. BREAK UP CIP 011 INTO MULTIPLE STANDARDS

1. Retain 003-009 Format *(10 comments)*
2. Audit/Enforcement/Compliance and Negative Perceptions *(9 comments)*
3. Suggested Standard Format Combinations *(8 comments)*
4. Level of Effort and Cost of Changing Format *(6 comments)*
5. Use Functional Areas *(3 comments)*
6. Consistency with Other Industry Cyber Protection Standards *(2 comments)*
7. Makes Easier Ownership Assignment and Referencing *(1 comment)*
8. Monitoring Changes *(1 comment)*
9. Aids the Revision Process *(1 comment)*
10. Focus on Security *(1 comment)*
11. Approve as a Complete Set *(1 comment)*
12. CIP Standards Should Stand Alone *(1 comment)*

KEEP AS A SINGLE 011

1. Better Organization and Organizational Review *(8 comments)*
2. Auditing and Multiple Violations of Single Standard. *(6 comments)*
3. Format *(2 comments)*
4. Table Format *(1 comment)*
5. Revisions *(1comment)*
6. Alignment with Other Standards *(1comment)*

C. NO PREFERENCE

1. Implementation, Updates and Revisions *(4 comments)*
2. Focus on Defining Auditable Requirements. *(3 comments)*
3. Reporting at a Requirement Level *(2comments)*
4. Simpler Management *(2 comments)*
5. Table Format *(1comment)*

A. BREAK UP CIP 011 INTO MULTIPLE STANDARDS

1. Retain 003-009 Format (10)

- (18) simply the fourth iteration of Version 1. ii) SDT should lay FERC Order 706 side by side with CIP-003-3 through CIP-009-3 and make changes specifically attendant to 706 FERC directives - no more, no less. iii) Topical subjects addressed in CIP-003-3 through CIP-009-3 Standards respectively should remain the same, i.e., subject matter organization should not be moved under from under one Standard to another; iv) Concepts already well established and understood throughout the industry created under CIP V1, e.g., CA, CCA, ESP, PSP, etc., should be preserved intact
- (24) Keeping (as much as possible) the existing CIP Standards and Requirements in place, and augmenting each of the existing Standards with new and modified Requirements. This strategy will allow participating entities to transition to the new version 4 requirements in an easier fashion, while making better use of existing documentation and procedures.
- (26) For Responsible Entities, their Compliance Teams, their Employees, and their Contractors have all been indoctrinated with the terminology, standards and requirement numbering of CIP 002-009. One reason for continuing a similar number standard is to reduce the confusion for all those involved with compliance, and migration from CIP-002/009 to CIP-010/011.
- (33, 34, 35, 40, 48) It would be easier for entities to recognize and understand the similar or different requirements in version 4 if they were broken up in a manner similar to legacy CIP-003-009. Many organizations have made significant investments in training, policies, procedures, and document management systems that are based on the legacy CIP standard Requirement numbering structure. Staying with the legacy structure, to the degree that it is possible, may reduce stranded investment that needs to be recreated simply as a function of the name and numbering of the requirements
- (36) The revolutionary approach proposed will cause confusion, which may adversely affect the reliability of the BES. The version 4 standards should be built upon the existing standards to avoid the unnecessary confusion that will be introduced during the implementation of CIP-011. Rewrite CIP-011 and apply the requirements to existing CIP-003 thru CIP-009 standards.
- (43) The original setup seems indicated some logic on how cyber security should be addressed. Also, it has been there for several years. Most people probably have become used to the titles and subjects.

2. Audit/Enforcement/Compliance and Negative Perceptions (9)

- (10) Breaking CIP-011-1 into multiple standards lends itself very well to being audited.
- (18) From an enforcement perspective, using a single Standard document consisting of many Requirements is highly problematic. Per the current codified NERC Standards Development Process any Standard can be assigned only a single Violation Risk Factor (VRF).
- … it could well be that all Responsible Entities in the industry are found to be out of compliance with some aspect of a single large multi-Requirement Standard every year.
- (20) Because of the number of requirements involved, combining all into one document will make it more difficult for stakeholders to use, and make it more difficult to assess compliance.

- (23) …combining them all does not make it easier to comply. ..Has a decision yet been made how this would be audited as a single standard? Would we now have compliance violations reported on a requirement level instead of a standard level?
- (41, 40) The addition of sub-headings into CIP-011 is illustrative of the need to separate them. From a presentation perspective, e.g., most frequency violated standards, we would be faced with tough decision of either having one standard with a very large bar in a top 10 bar chart, or possibly having multiple CIP standards is the bar chart, until the Industry gets used to the new standards. Either way is politically difficult, so, the simpler approach is probably the preferable approach of multiple standards on different security topics.
- (45) The standard grouping in CIP11 will result in a negative perception as to the progress industry is making in improving cyber security of the BES.
- …Consider individual standards or a new approach to metrics reporting that focuses on the security domain versus the standard.

3. Suggested Standard Format Combinations (8)

- (23)Some standard combinations that do make sense are physical, electronic and information access (CIP-003 R4, CIP-005 R2-R3, and CIP-006 R2-R6). Also, combining incident response and recovery makes sense
- (26) …consider skipping CIP-010, and name it CIP-012. Then take the content related to CIP-003, and organize it into CIP-013. Effectively, putting the next evolution of the standards into the next "decade", whereby the second-digit is incremented.
- (28)break up the standard into three (3) standards, one (1) for low impact BES Cyber System, one (1) for medium impact BES Cyber System, and one (1) for high impact BES Cyber System.
- (30) In addition to breaking up the standards by grouping, they should be broken up by facility type and/or function.
- (31) Suggest adding a matrix of all the requirements by a major category showing all the requirements and impacts, not just the ones which differ. Having one standard would require the entire standard to be re-issued for any change.
- (31) Suggest multiple standards or using a numbering scheme such as CIP-011-1.1, CIP-011-1.2, CIP-011-1.3, etc to separate the requirements by major categories. If there is a change to a major category, the numbering would be CIP-011-1.2a, CIP-011-1.3c, etc.
- (32) It would be clearer if the requirements were organized based on their objectives: physical security, system security, boundary security, personnel management, access, etc
- (44) The section of standards that deal with controls should be divided into components that are grouped thematically. For instance, management of personnel may contain all requirements pertaining to training, background checks, etc., as one standard. Another standard should be used for governance functions such as policy making and management, audit documents, change management, etc. A third standard for Access Management can be used to list in detail end-to-end access controls for interactive access that is electronic, escorted and unescorted physical access and access to information. Boundary protections, physical and electronic, can be addressed as a family of security controls along with system security requirements as a fourth standard. A section that describes priority of controls within each requirement, in addition to a VRF/VSL document, should be provided so that RE's can implement controls at a granular level even within the High-Medium-Low framework. SCE supports the modification of the

CIP standards from a family of eight controls in the current version, and the reduction of the number of sub-levels within requirements.

4. Level of Effort and Cost of Changing Format (6)

- (19) many entities are now in the compliance phase of the current CIP Standards and have spent a great deal of effort in developing documentation and evidence gathering processes base on the CIP-002 through CIP-009 Standards. Concerned about the upheaval required to alter processes and procedures, currently tied to multiple Standards, to match a single Standard.
- (23) …combining them all creates an administrative mess by requiring everyone to change all their document references to conform to the new standards and requirements.
- (24) We've put a lot of time into the organization, layout, and design of our process and materials and it appears to be a daunting task to revamp all of this to comport with almost completely new Standards.
- … Transitioning to a comprehensive single document requires Entities to perform additional translation, communication, implementation and review across departments, organizational structures and systems owners, and increases the potential for communication and task errors, and the potential probability of introducing an operational or security concern.
- (27) Given the extensive work that has been done to establish monitoring and compliance tracking systems, the wholesale change in format will cause extensive rework to compliance programs (systems, procedures, governance models, etc...). One must ask how this re-work is intended to improve reliability.
- …Staying with the legacy structure, to the degree that it is possible, may reduce stranded investment that needs to be recreated simply as a function of the name and numbering of the requirements.

5. Use Functional Areas (3)

- (16,17)Establish new standards by functional areas- Ensure there is not a circular loop relating to other requirements/standards, each requirement/standard should be standalone
- (38) Most owners of BES equipment have multiple departments that manage different corporate functions. These departments include Information Resources, System Operations, Human Resources, Relay Protection, Engineering, etc. Organizing the CIP requirements into topic-specific standards (as was done for CIP-002 through CIP-009), will facilitate corporate management of compliance.

6. Consistency with Other Industry Cyber Protection Standards (2)

- (17)Cyber protection is not unique to the electric industry. generic set of Cyber protection standards that is applicable to all sectors that use Cyber Systems
- (118) *No preference.* We urge NERC and the electric industry to assess if indeed it needs to have its own cyber protection standards at all. Cyber protection is not unique to the electric industry. Other sectors - airline industry, national security/ defense, financial sector, banking system, etc. all employ a high level of cyber security to protect fraud and invasions.

7. Makes Easier Ownership Assignment and Referencing (1)

- (21) Multiple standards allows for easier ownership assignment and referencing (indexing) within policies and programs. The new format still provides multiple reference for the same item in multiple locations (e.g. Access), therefore this supports keeping multiple standards.

8. Monitoring Changes (1)

- (37) Monitoring changes to the requirements would be easier if they were separated into different standards.

9. Aids the Revision Process (1)

- (42) We also feel with multiple standards the revision process would be simplified. If only one section needs to be revised, then NERC could just post that particular section for industry comment.

10. Focus on Security (1)

- (46) Breaking up the requirements will allow emphasis to be placed on categories that may be more critical to security. Breaking up the requirements will also allow for much easier application.

11. Approve as a Complete Set (1)

- (39) Multiple standards that are logically separated is preferred. However, if separated the standards still should be approved as a complete set.

12. Stand Alone (1)

- (29) If NERC separates into multiple standards, need to make sure the CIP standards are stand alone.

KEEP AS A SINGLE 011

1. Better Organization and Organizational Review (8)

- (10)Keeping it as one single CIP-011-1 standard will ease discussions throughout organization when talking about CIP as there will only be one standard for all controls and it makes sense based on the previous versions repeated statement that the standards should be treated as one standard.
- (81) Having CIP-011-1 as one document makes it more streamlined and is easier to follow.
- (82) Having the requirements in a single standard significantly improves understanding and ease of reading.
- (83) It is much easier to find all the requirements when all contained is a single document and the chance of discrepancies between documents is greatly reduced.
- (86) One document makes it a lot cleaner for a smaller entity to deal with.
- (89) The previous CIP-003 through CIP-009 required cross-referencing between the standards and standard owners to get it right. CIP-011 is much easier to follow and understand.
- (90) The single document format clearly states the requirements unlike the current standards which link to one another but do not clearly link the requirements. Having

CIP-011-1 as one document rather than multiple standards is great. All of the requirements are in one place and easy to find.

- (95) With the requirements in a single document, it seems that it will be easier to arrange and consolidate requirements to alleviate the duplications and contradictions which have plagued the preceding CIP standards.

2. Auditing and Multiple Violations of Single Standard. (6)

- (81) The concern is how multiple violations of several different sub-requirements will be looked at by the compliance enforcement agencies. If an entity is found in violation of CIP-011-1 R4 for example and is later found in violation of CIP-011-1 R26 will this be considered a second violation? If so, FEUS would prefer CIP-011-1 to be grouped into separate standards.
- (83) However, the CMEP should be updated to monitor and report violations by standard and requirement not just standard. Otherwise, CIP-011 will always be in the list of Top 10 most violated standards and create a misleading impression that utilities cannot figure out how protect the reliability of the BES.
- (84) Keeping the controls in one document as proposed is preferable; provided that the intent is not that ALL requirements in CIP-011-1 have to be audited as a family of requirements.
- (93) We are concerned about the current compliance monitoring and enforcement structure where the magnitude of fines and sanctions are levied based on prior violations, and the violations are reported per standard. The proposed standard contains over one hundred requirements and sub-requirements, which increases an entity's exposure to multiple violations for a single standard, and increases the exposure of the industry to a large number of violations to a single standard.
- (94) However, by consolidating the current version 3 standards into one document, this new CIP-011 standard would become one of the NERC's standards with the largest number of requirements. This could potentially make it "the most violated" one as well consequently impact the amount of monetary sanctions. If the proposed format is adopted, special compliance consideration should be adopted when dealing with violations
- (111) *No preference* Having them in one document could prevent public documentation of specific areas of weakness for an organization as audit results are public information and published on the NERC website. It also eliminates the need for circular referencing that is in the current CIP-002 to CIP-009 (e.g., CIP-005 R1.5).

3. Format (2)

- (88) Keep CIP-011-1 as one document if: 1. Requirement number should be consistent with the Requirement table numbering. For example, currently requirement 3.1 Cyber Security Training does not relate to Table item 3.1 Electronic Access. The result is two items that would be referenced as CIP-011 3.1 on completely different topics.2. Every requirement should have a related table. Currently R1 & R2 do not have related tables for applicability. It is 'bad practice' to assume the interpretation that those requirements without a table apply to everything 3. The 'local definitions' should be gathered in a separate definitions section and numbered. Lacking a definitions section there is no convenient mechanism to refer to local definitions.4. While I understand the expressed opinion makes the standard easier to use, I don't agree with that opinion. The defined terms related to this standard should be listed in a separate section. My opinion is that

the current format of the local definitions is more confusing than clarifying.5. Based on the CIP Standards Workshop information, I would suggest the Requirement statement (R1, R2, R3, etc.) be a statement of the requirement objective, and the Table rows be implementing requirements for that objective. This approach should also resolve items 1 & 2 above.

- (92) Using a single standard for all requirements is preferred, however the format internal to the single standard appears to be inconsistent. For example, some requirements are in paragraph form while others are embedded in a requirements Table. All requirements should be contained within a requirements Table. Where possible, information preceding the table should be used only to state the context and establish the security objective or intent behind the requirements.

4. Table Format (1)

- (91) The tables holding the sub-requirements are a good feature that enhances readability. CIP-011 R3 and R4 have some requirements outside of the table and some in the table. Please move all sub-requirements to table format so each requirement would become a paragraph followed by a table with sub-requirements. This will help minimize confusion caused by having a requirement and a table entry with the same number.

5. Revisions (1)

- Future changes that do not impact the compliance documentation numbering should be considered

6. Alignment with Other Standards (1)

- (87) Alignment of CIP security controls with security controls based on NIST 800 series standards and implemented in NEI 08-09, Revision 6, for nuclear plant systems would prevent regulatory uncertainty and potential dual regulation of a single system.

C. NO PREFERENCE

1. Implementation, Updates and Revisions (4)

- (115) The SDT should consider the advantages of breaking the Standard into multiple standards, as far as implementation goes. Some requirements will require more time to implement than others. Having the standard broken apart may make distinguishing these timeframes easier.
- (112) The disadvantage is that more of the requirements will potentially be exposed to comments whenever the standard is being updated.
- (112) Additionally, multiple standards permit parallel modification efforts whereas a single standard may result in single-threaded modifications over a prolonged development and approval timeframe.
- (119)One document eliminates potential confusion about the use of the correct version. However, during the initial implementation phase, there may be multiple revisions for CIP-011 being issued each month/quarter.

2. Focus on Defining Auditable Requirements. (3)

- (109) Believe the SDT's time and effort are better spent on defining well-understood and auditable requirements that will enhance BES security & reliability than on trying to force-fit new/updated requirements into existing document structures.
- (112) Having all of the requirements in one document as opposed to many makes no difference to the compliance monitoring and enforcement process as long as Violation Severity Levels and Violation Risk Factors do not roll up higher than the main-level enumerated requirements.
- (113) Breaking CIP-011 into multiple documents facilitates certain compliance and accountability aspects

3. Reporting at a Requirement Level (2)

- (108) A personnel training issue can cause a violation of the whole standard that will be looked at as the same as a Cyber System boundary problem (Outsider Scanning). Until violations reporting and sanctions are reported at the requirement level only, then this could have a disproportionate impact on the entity relates to potential impact on the BES.
- (117) Violations are by requirement, so whether it is one standard or multiple standards makes no difference.

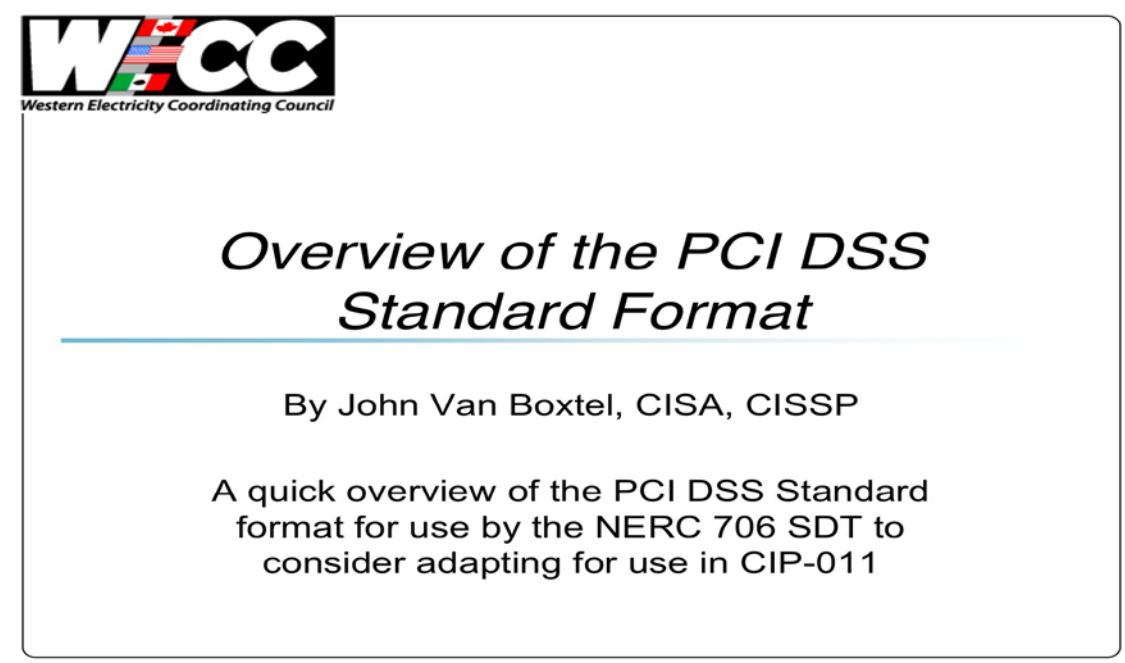
4. Simpler Management (2)

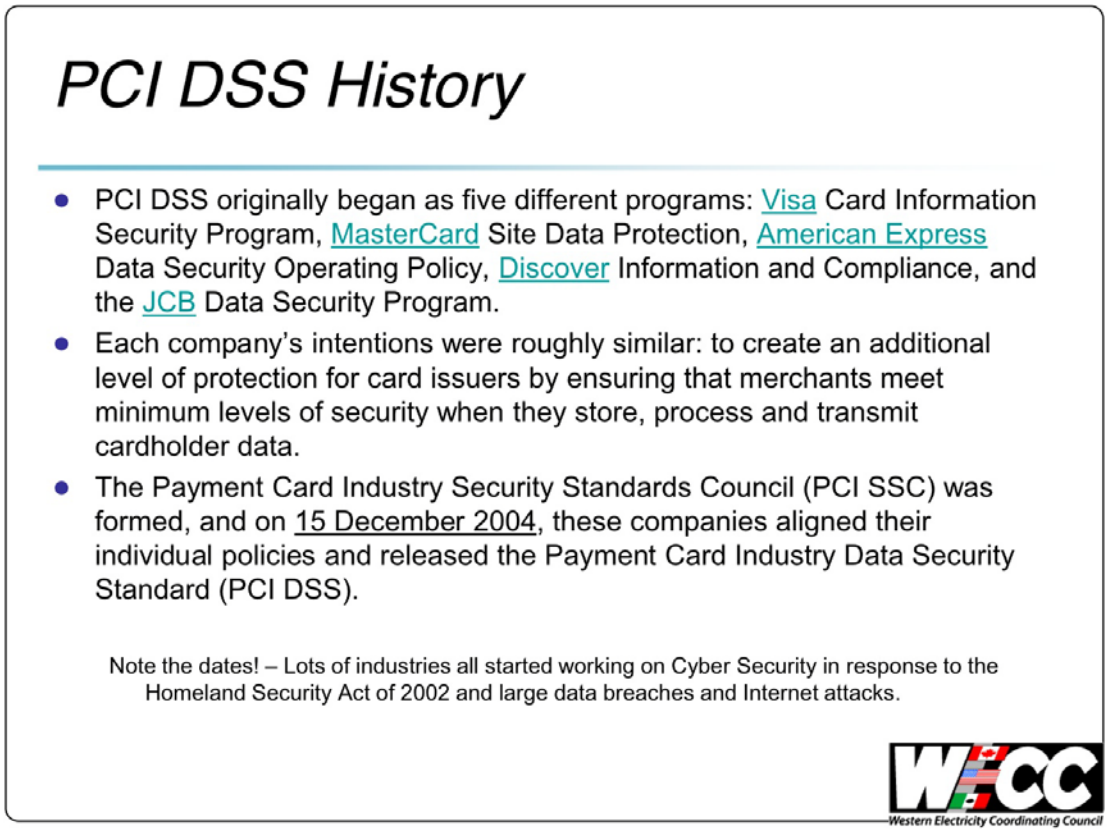
- (112)The advantage of keeping everything in one document is simpler version management and reducing the need for cross-standard references.
- (113) Keeping CIP-011 as one document reduces complexity and makes overall understanding easier.

5. Table Format (1)

- (116) The tabular format for the requirements section is an excellent vehicle to capture the individual requirements. This should be expanded to include all requirement items. The numbering in the tables should be made unique to match the associated requirements in the standards body. (i.e., R3.1 is related to security training while table entry 3.1 is related to electronic access.)Sections of the table which do not apply should be marked N/A.

Appendix # 9 Format Consideration- John Van Boxtel Presentation





Example Requirement

PCI Security Standards Council

Regularly Monitor and Test Networks

Requirement 10: Track and monitor all access to … d cardholder data.

Logging mechanisms and the ability t… preventing, detecting, or minimi… compromise. The presence of logs in all environments … ing, and analysis when … termining the cause of a compromise is very difficult without …

Requirement Details

Testing (measures)

PCI DSS Requirements	Testing Procedures	In Place	Not in Place	Target Date/ Comments
10.1 Establish a process for linking all access to system components (especially access done with administrative privileges such as root) to each individual user.	10.1 Verify through observation and interviewing the system administrator, that audit trails are enabled and active for system components.			
10.2 Implement automated audit trails for all system components to reconstruct the following events:	10.2 Through interviews, examination of audit logs, and examination of audit log settings, perform the following:			
10.2.1 All individual accesses to cardholder data	10.2.1 Verify all individual access to cardholder data is logged.			
10.2.2 All actions taken by any …	10.2.2 Verify actions taken by any individual with root or …			

Western Electricity Coordinating Council

Example Requirement

PCI Security Standards Council

Regularly Monitor and Test Networks

Requirement 10: Track and monitor all access to network resources and cardholder data.

Logging mechanisms and the ability to track user activities are critical in preventing, detecting, or minimizing the impact of a data compromise. The presence of logs in all environments allows thorough tracking, alerting, … d analysis when something does go wrong. Determining the cause of a compromise is very difficult without system activity logs.

Section Titles

Requirement (broad)

Justification and Guidance (objective)

PCI DSS Requirements	Test…	In Place	Not in Place	Target Date/ Comments
10.1 Establish a process for linking all access to system components (especially access done with administrative privileges such as root) to each individual user.	10.1 Verify through obs… system administrator, that … active for system components.			
10.2 Implement automated audit trails for all system components to reconstruct the following events:	10.2 Through interviews, examination of audit logs, and examination of audit log settings, perform the following:			
10.2.1 All individual accesses to cardholder data	10.2.1 Verify all individual access to cardholder data is logged.			
10.2.2 All actions taken by any …	10.2.2 Verify actions taken by any individual with root or …			

Western Electricity Coordinating Council

More Examples of Guidance

PCI Security Standards Council

Requirement 6: Develop and maintain secure systems and applications

Unscrupulous individuals use security vulnerabilities to gain privileged access to systems. Many of these vulnerabilities are fixed by vendor-provided security patches, which must be installed by the entities that manage the systems. All critical systems must have the most recently released, appropriate software patches to protect against exploitation and compromise of cardholder data by malicious individuals and malicious software.

Note: Appropriate software patches are those patches that have been evaluated and tested sufficiently to determine that the patches do not conflict with existing security configurations. For in-house developed applications, numerous vulnerabilities can be avoided by using standard system development processes and secure coding techniques.

PCI Security Standards Council

Implement Strong Access Control Measures

Requirement 7: Restrict access to cardholder data by business need to know

To ensure critical data can only be accessed by authorized personnel, systems and processes must be in place to limit access based on need to know and according to job responsibilities.

"Need to know" is when access rights are granted to only the least amount of data and privileges needed to perform a job.

WECC Western Electricity Coordinating Council

Examples of Guidance

PCI Security Standards Council

Protect Cardholder Data

Requirement 3: Protect stored cardholder data

Protection methods such as encryption, truncation, masking, and hashing are critical components of cardholder data protection. If an intruder circumvents other network security controls and gains access to encrypted data, without the proper cryptographic keys, the data is unreadable and unusable to that person. Other effective methods of protecting stored data should be considered as potential risk mitigation opportunities. For example, methods for minimizing risk include not storing cardholder data unless absolutely necessary, truncating cardholder data if full PAN is not needed, and not sending PAN in unencrypted e-mails.

Please refer to the *PCI DSS Glossary of Terms, Abbreviations, and Acronyms* for definitions of "strong cryptography" and other PCI DSS terms.

- Good example of complicated technical requirement referencing external document

WECC Western Electricity Coordinating Council

Inspiration from similar requirements?

- **Segmentation**
  - **Requirement**

    1.3.7 Place the database in an internal network zone, segregated from the DMZ.
  - **Measure**

    1.3.7 Verify that the database is on an internal network zone, segregated from the DMZ.

WECC Western Electricity Coordinating Council

Inspiration from similar requirements?

- **ESP**
  - **Here is one piece out of Requirement 1 which is their Electronic Perimeter Req.**

1.2 Build a firewall configuration that restricts connections between untrusted networks and any system components in the cardholder data environment.	**1.2** Examine firewall and router configurations to verify that connections are restricted between untrusted networks and system components in the cardholder data environment, as follows:
Note: An "untrusted network" is any network that is external to the networks belonging to the entity under review, and/or which is out of the entity's ability to control or manage.	

Guidance right next to the specific requirement

WECC Western Electricity Coordinating Council

Appendix A – Additional Requirements based on risks

- PCI DSS standard sets a "base level" of security that all card processors must meet.
- They layer additional requirements on with appendixes.
- This might work well for us:

  Appendix 1 - Routable, Dialup, Remotely Accessible Components
  Appendix 2 - Control Centers / Data Centers (2-layer ESP? forensics?)
  Appendix 3 - Data and Communications Integrity
  Appendix 4 - Virtualization
  Appendix 5 - Wireless

WECC Western Electricity Coordinating Council

Policy Requirement

PCI Security Standards Council

Maintain an Information Security Policy

Requirement 12: Maintain a policy that addresses information security for employees and contractors.

A strong security policy sets the security tone for the whole company and informs employees what is expected of them. All employees should be aware of the sensitivity of data and their responsibilities for protecting it. For the purposes of this requirement, "employees" refers to full-time and part-time employees, temporary employees and personnel, and contractors and consultants who are "resident" on the company's site.

PCI DSS Requirements	Testing Procedures	In Place	Not in Place	Target Date/ Comments
12.1 Establish, publish, maintain, and disseminate a security policy that accomplishes the following:	12.1 Examine the information security policy and verify that the policy is published and disseminated to all relevant system users (including vendors, contractors, and business partners).			
12.1.1 Addresses all PCI DSS requirements.	12.1.1 Verify that the policy addresses all PCI DSS requirements.			
12.1.2 Includes an annual process that identifies threats, and vulnerabilities, and results in a formal risk assessment.	12.1.2 Verify that the information security policy includes an annual risk assessment process that identifies threats, vulnerabilities, and results in a formal risk assessment.			
12.1.3 Includes a review at least once a year and updates when the environment changes.	12.1.3 Verify that the information security policy is reviewed at least annually and updated as needed to reflect changes to business objectives or the risk environment.			
12.2 Develop daily operational security procedures that are consistent with requirements in this specification (for example, user account maintenance procedures, and log review procedures).	12.2.a Examine the daily operational security procedures. Verify that they are consistent with this specification, and include administrative and technical procedures for each of the requirements.			

WECC Western Electricity Coordinating Council

Appendix B – Compensating Controls

- Appendix B "Compensating Controls" is basically what we would call TFEs. It starts with this phrase:

  Compensating controls may be considered for most PCI DSS requirements when an entity cannot meet a requirement explicitly as stated, due to legitimate technical or documented business constraints, but has sufficiently mitigated the risk associated with the requirement through implementation of other, or compensating, controls.

  1) Compensating controls must satisfy the following criteria:

  …

- This approach of a process for handling situations of not meeting the requirements INCLUDED inside the standard addresses industry feedback that the TFE process wasn't as open as the standard development process; however, it might be too late.

Western Electricity Coordinating Council

Appendix A – Additional Requirements Example

PCI Security Standards Council

Appendix A: Additional PCI DSS Requirements for Shared Hosting Providers

Requirement A.1: Shared hosting providers must protect the cardholder data environment

As referenced in Requirement 12.8, all service providers with access to cardholder data (including shared hosting providers) must adhere to the PCI DSS. In addition, Requirement 2.4 states that shared hosting providers must protect each entity's hosted environment and data. Therefore, shared hosting providers must additionally comply with the requirements in this Appendix.

Requirements	Testing Procedures	In Place	Not in Place	Target Date/ Comments
A.1 Protect each entity's (that is merchant, service provider, or other entity) hosted environment and data, per A.1.1 through A.1.4: A hosting provider must fulfill these requirements as well as all other relevant sections of the PCI DSS. *Note: Even though a hosting provider may meet these requirements, the compliance of the entity that uses the hosting provider is not guaranteed. Each entity must comply with the PCI DSS and validate compliance as applicable.*	**A.1** Specifically for a PCI DSS assessment of a shared hosting provider, to verify that shared hosting providers protect entities' (merchants and service providers) hosted environment and data, select a sample of servers (Microsoft Windows and Unix/Linux) across a representative sample of hosted merchants and service providers, and perform A.1.1 through A.1.4 below.			
A.1.1 Ensure that each entity only runs processes that have access to that entity's cardholder data environment.	**A.1.1** If a shared hosting provider allows entities (for example, merchants or service providers) to run their own applications, verify these application processes run using the unique ID of the entity. For example: • No entity on the system can use a shared web server user ID. • All CGI scripts used by an entity must be created and run as the entity's unique user ID.			

Supplemental Documents

- The PCI SSC has released several supplemental pieces of information to clarify various requirements. These documents include the following
  - Information Supplement: Requirement 11.3 Penetration Testing[5]
  - Information Supplement: Requirement 6.6 Code Reviews and Application Firewalls Clarified[6]
  - Navigating the PCI DSS - Understanding the Intent of the Requirements[7]
  - Information Supplement: PCI DSS Wireless Guidelines[8]
- These are NOT referenced inside the standard and updated independently (might not be work for us because of NERC standard procedures ?)

What are we already using?

- Requirements grouped by Sections
- Broad simple requirement sentence is similar to current approach of generic requirement statement “in Table X…” above the table of specifics
- Table below broad requirement statement with specifics on how to achieve the requirement.

What might we want to consider?

- Moving measures into the table immediately next to requirement.
  - Simplifies knowing what is necessary to prove compliance
  - Simplifies auditing
  - Perhaps since the measures are now in the table beneath the broad requirement sentence they are "part of the requirement"
  - Easy to argue "auditing to the requirement"

WECC Western Electricity Coordinating Council

What might we want to consider?

- Several comments about breaking out the "objective" phrasing contained in the requirement. This is exactly like the PCI standard does in italics above the tables.
- Can link to supplemental guidance documents in the area above the requirement table.
- Using Appendixes to "layer" on additional requirements for specific situations

WECC Western Electricity Coordinating Council

What would this potentially look like:

Requirement 9 - Revoke access to BES Cyber Systems when access is no longer required

Each Responsible Entity shall have processes or procedures to prevent malicious operation of BES Elements by maintaining control of access to its BES Cyber Systems. Personnel that no longer require access shall have the ability to access that equipment revoked at the time of termination (immediately). Accounts will be removed within reasonable time frames to prevent them from being accessed by unknown access methods, failure of primary access control methods, or misused by other personnel.

NERC CIP - Requirement 9			Applicability		
Requirement		Measurement	Low Impact BES Cyber System	Medium Impact BES Cyber System	High Impact BES Cyber System
9.1	Immediately revoke access for personnel terminated for cause.	Verify that a policy for immediate revocation of access exists and that procedure and process exists to prevent access to the BES Cyber System. Perform a random sample of the process to ensure that procedure is followed and prevents access.	Required	Required	Required
9.2	Remove or disable accounts on BES Cyber Systems within a Control Center within the following time periods.	Perform a sample validation of account removal from several systems inside the Control Center for personnel that had access revoked.	7 days	3 days	1 day (24 Hours)
9.3	Remove or disable accounts on BES Cyber Systems controlling Transmission within the following time periods.	Perform a sample validation of account removal from several systems inside the Control Center for personnel that had access revoked.	30 days	7 days	1 day (24 Hours)
9.4	Remove or disable accounts on BES Cyber Systems	Perform a sample validation of account removal from several	30 days	7 days	1 day

WECC Western Electricity Coordinating Council

Conclusion

- We have already adopted several of the formatting elements from PCI
- It would not take much to adopt our existing draft into this format
- Much easier to read, audit, and reach compliance by Responsible Entities
- Most likely fits existing NERC Rules of Procedures – minimal if any changes

WECC Western Electricity Coordinating Council

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Appendix #10

CS0706 Standards Drafting Team
OVERVIEW OF UNOFFICAL AVERAGE OF RESULTS OF INDUSTRY COMMENT FORM POLLING

(120 SETS) JUNE 3, 2010
(Color Legend: Agree Disagree)

COMBINED AVERAGE SUPPORT FOR ALL SECTIONS (14) =51%

1. **DEFINITIONS 41% AVERAGE SECTION SUPPORT**
2. **CIP-010-1 — CYBER SECURITY 54% AVERAGE SECTION SUPPORT**
3. **CIP-011-1 — CYBER SECURITY — BES CYBER SYSTEM PROTECTION: 55% AVERAGE SECTION SUPPORT**
4. **SECURITY GOVERNANCE AND POLICY (R1) 56% AVERAGE SECTION SUPPORT**
5. **PERSONNEL TRAINING, AWARENESS, AND RISK ASSESSMENT (R2 –R4) 43% AVERAGE SECTION SUPPORT**
6. **PHYSICAL SECURITY (R5 –R6) 40% AVERAGE SECTION SUPPORT**
7. **ELECTRONIC ACCESS CONTROL (R7 –R14) 51% AVERAGE SECTION SUPPORT**
8. **SYSTEM SECURITY (R15 –R19) 36% AVERAGE SECTION SUPPORT**
9. **BOUNDARY PROTECTION (R20 –R22) 44% AVERAGE SECTION SUPPORT**
10. **CONFIGURATION CHANGE MANAGEMENT (R23) 50% AVERAGE SECTION SUPPORT**
11. **INFORMATION PROTECTION AND MEDIA SANITIZATION (R24 –R25) 64% AVERAGE SECTION SUPPORT**
12. **BES CYBER SYSTEM MAINTENANCE (R26) 65% AVERAGE SECTION SUPPORT**
13. **CYBER SECURITY INCIDENT RESPONSE (R27 –R29) 61% AVERAGE SECTION SUPPORT**
14. **BES CYBER SYSTEM RECOVERY (R30 –R32) 56% AVERAGE SECTION SUPPORT**

DEFINITIONS 41% AVERAGE SECTION SUPPORT

1.a. BES Cyber System Component
34 (31%)= Agree with proposed definition
76 (69%)= Disagree with proposed definition
1.b. BES Cyber System
30 (29%)= Agree with proposed definition
80 (73%)= Disagree with proposed definition
1.c. Control Center
42 (40%)= Agree with proposed definition
63 (60%)= Disagree with proposed definition
2.
67 (63%)= Agree with proposed definition
40 (37%)= Disagree with proposed definition

CIP-010-1 — CYBER SECURITY 54% AVERAGE SECTION SUPPORT

3.
49 (45%)= Agree with proposed definition
59 (55%)= Disagree with proposed definition

4.
66 (63%)= Agree with proposed definition
40 (38%)= Disagree with proposed definition
5.
41 (39%)= Agree with proposed definition
64 (61%)= Disagree with proposed definition
6.
62 (58%)= Agree with proposed definition
45 (42%)= Disagree with proposed definition
7.
72 (67%)= Agree with proposed definition
35 (33%)= Disagree with proposed definition

CIP-011-1 — CYBER SECURITY — BES CYBER SYSTEM PROTECTION: 55% AVERAGE SECTION SUPPORT

9.
48 (44%)= Keep CIP 011-1 as one document
38 (35%)= Break CIP 011-1 up into multiple standards
23 (21%)= No Preference
10.
67(66%)= Agree with proposed definition
34(34%)= Disagree with proposed definition

SECURITY GOVERNANCE AND POLICY (R1) 56% AVERAGE SECTION SUPPORT

11.
58(56%)= Agree with proposed definition
46(44%)= Disagree with proposed definition

PERSONNEL TRAINING, AWARENESS, AND RISK ASSESSMENT (R2 –R4) 43% AVERAGE SECTION SUPPORT

12.
23(23%)= Agree with proposed definition
77(77%)= Disagree with proposed definition
13.
59(60%)= Agree with proposed definition
39(40%)= Disagree with proposed definition
14.
43(47%)= Agree with proposed definition
48(53%)= Disagree with proposed definition

PHYSICAL SECURITY (R5 –R6) 40% AVERAGE SECTION SUPPORT

15.
37(40%)= Agree with proposed definition
56(60%)= Disagree with proposed definition
16.
37(41%)= Agree with proposed definition
54(59%)= Disagree with proposed definition

ELECTRONIC ACCESS CONTROL (R7 –R14) 51% AVERAGE SECTION SUPPORT

17.

56 (58%)= Agree with proposed definition
40 (42%)= Disagree with proposed definition

18.
66 (69%)= Agree with proposed definition
30 (31%)= Disagree with proposed definition

19.
74(80%)= Agree with proposed definition
19(20%)= Disagree with proposed definition

20.
45 (48%)= Agree with proposed definition
48 (52%)= Disagree with proposed definition

21.
50 (55%)= Agree with proposed definition
41 (45%)= Disagree with proposed definition

22.
27 (29%)= Agree with proposed definition
67 (71%)= Disagree with proposed definition

23.
30 (33%)= Agree with proposed definition
62 (67%)= Disagree with proposed definition

24.
27 (28%)= Agree with proposed definition
68 (72%)= Disagree with proposed definition

25.
44 (46%)= Agree with proposed definition
51 (54%)= Disagree with proposed definition

26.
47 (50%)= Agree with proposed definition
47 (50%)= Disagree with proposed definition

27.
51 (55%)= Agree with proposed definition
41 (45%)= Disagree with proposed definition

28.
49 (54%)= Agree with proposed definition
42 (46%)= Disagree with proposed definition

29.
55 (60%)= Agree with proposed definition
37 (40%)= Disagree with proposed definition

30.
50 (55%)= Agree with proposed definition
41 (45%)= Disagree with proposed definition

31.
37 (40%)= Agree with proposed definition
55 (60%)= Disagree with proposed definition

32.
31 (34%)= Agree with proposed definition
60 (66%)= Disagree with proposed definition

33.
51 (58%)= Agree with proposed definition
37 (42%)= Disagree with proposed definition

34.
49 (57%)= Agree with proposed definition
37 (43%)= Disagree with proposed definition

SYSTEM SECURITY (R15 –R19) 36% AVERAGE SECTION SUPPORT

35.
25 (27%)= Agree with proposed definition
67 (73%)= Disagree with proposed definition
36.
40 (45%)= Agree with proposed definition
49 (55%)= Disagree with proposed definition

BOUNDARY PROTECTION (R20 –R22) 44% AVERAGE SECTION SUPPORT

37.
28 (31%)= Agree with proposed definition
62 (69%)= Disagree with proposed definition
38.
49 (56%)= Agree with proposed definition
38 (44%)= Disagree with proposed definition
39.
38 (46%)= Agree with proposed definition
44 (54%)= Disagree with proposed definition

CONFIGURATION CHANGE MANAGEMENT (R23) 50% AVERAGE SECTION SUPPORT

40.
36 (41%)= Agree with proposed definition
52 (59%)= Disagree with proposed definition

41.
48 (58%)= Agree with proposed definition
35 (42%)= Disagree with proposed definition

INFORMATION PROTECTION AND MEDIA SANITIZATION (R24 –R25) 64% AVERAGE SECTION SUPPORT
42.
54 (58%)= Agree with proposed definition
39 (42%)= Disagree with proposed definition
43.
65 (72%)= Agree with proposed definition
25 (28%)= Disagree with proposed definition
44.
43 (49%)= Agree with proposed definition
45 (51%)= Disagree with proposed definition
45.
62 (75%)= Agree with proposed definition
21 (25%)= Disagree with proposed definition

BES CYBER SYSTEM MAINTENANCE (R26) 65% AVERAGE SECTION SUPPORT
46.
64 (73%)= Agree with proposed definition
24 (27%)= Disagree with proposed definition
47.
41 (48%)= Agree with proposed definition

45 (52%)= Disagree with proposed definition

48.

61 (74%)= Agree with proposed definition
21 (26%)= Disagree with proposed definition

CYBER SECURITY INCIDENT RESPONSE (R27 –R29) 61% AVERAGE SECTION SUPPORT

49.

54 (61%)= Agree with proposed definition
34 (39%)= Disagree with proposed definition

50.

52 (60%)= Agree with proposed definition
34 (40%)= Disagree with proposed definition

BES CYBER SYSTEM RECOVERY (R30 –R32) 55.5% AVERAGE SECTION SUPPORT

51.

39 (46%)= Agree with proposed definition
46 (54%)= Disagree with proposed definition

52.

52 (65%)= Agree with proposed definition
28 (35%)= Disagree with proposed definition

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Agenda
Cyber Security Order 706 SDT — Project 2008-06

July 13, 2010 | 8:00 AM to 5:00 PM EDT
July 14, 2010 | 8:00 AM to 5:00 PM EDT
July 15, 2010 | 8:00 AM to 5:00 PM EDT
July 16, 2010 | 8:00 AM to 12:00 PM EDT
CERT Software Engineering Institute, Carnegie Mellon University
Pittsburgh, PA

Proposed Meeting Objectives/Outcomes:

- To review the CSO706 SDT 2010 Work Plan and Schedule for CIP-002-4
- To explore and clarify the Work Plan and Schedule for completing CIP-010 & 011
- To review, clarify and refine the strawman CIP-002-4 standard proposal
- To convene sub-teams to review the sub-team responses to Industry comments and proposed changes to CIP-010 and 011
- To provide SDT guidance so sub-teams can make further refinements to CIP 002-4, 010 & 011
- To agree on next steps and assignments

Tuesday, July 13, 2010 8:00 a.m. - 5:00 p.m.

- Introduction, welcome, and opening remarks -*(Morning)*
- Overview of CSO706 SDT Work plan and schedule for CIP 002-4 and Explore and Clarify CIP 010 & 011-*(Morning)*
- Review and seek agreement on proposal for refining the SDT Consensus Procedures -*(Morning)*
- Receive updates on other related cyber security initiatives- *NERC Staff and SDT Members (Morning)*
- Review and refine draft CIP 002-4 standard and related documents. *(Morning)*
- "Lunch and Learn"- Format Proposal*(Lunch)*
- Review and refine draft CIP 002-4 standard and related documents. *(Afternoon Plenary)*

Wednesday, July 14, 2010 8:00 a.m. - 5:00 p.m.

- Sub-teams present requirement changes and test SDT consensus on directions and changes *(Morning Plenary)*
- "Lunch and Learn"- NERC CIP SDT and the ASAP-SG Architecture Team
- Sub-teams present requirement changes and test SDT consensus on directions and changes *(Afternoon Plenary)*

Thursday, July 15, 2010, 8:00 a.m. - 5:00 p.m.

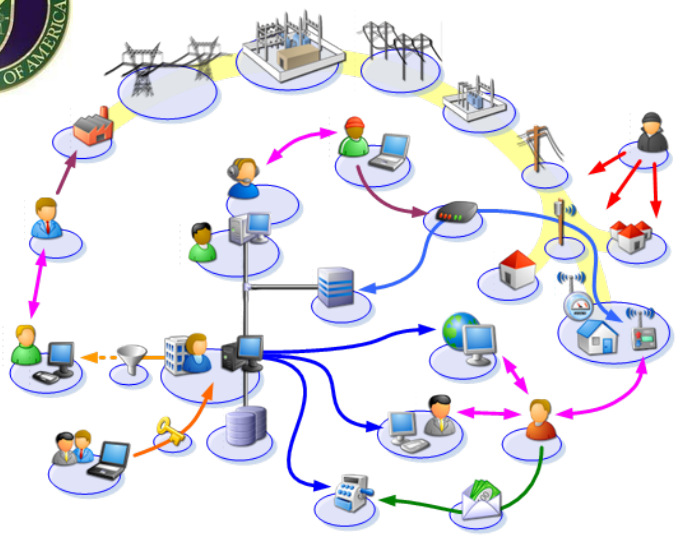
- Sub-teams present requirement changes and test SDT consensus on directions and changes *(Morning)*
- "Lunch and Learn"- Substation Networks (Varnell)
- CIP-010 and 011 Sub-Teams address changes in requirements in light of industry c*omments & i***n**puts from the SDT *(Afternoon)*
- Sub-teams present requirement changes and test SDT consensus on directions and changes *(Afternoon)*

Friday, July 16, 2010, 8:00 a.m. - 12:00 p.m.

- Review of CIP-002-4 Refinements (Morning)
- Review SDT Workplan Schedule to prepare new Draft CIP-010 and 011 Requirements documents. *(Morning)*

Review Next Steps and Sub-Team schedule and SDT Chicago Meeting Agenda (*Late Morning)*

ASAP-SG: Summary



- **Project Description:**
  - Utility-driven, public-private collaborative project to develop system-level security requirements for smart grid technology
- **Needs Addressed:**
  - **Utilities:** specification in RFP
  - **Vendors:** reference in build process
  - **Government:** assurance of infrastructure security
  - **Commissions:** protection of public interests
- **Approach:**
  - Architectural team → produce material
  - Usability Analysis team → assess effectiveness
  - NIST, SG Security → review
  - SG Security, UCAIug → approve
- **Deliverables:**
  - Strategy & Guiding Principles white paper
  - Security Profile Blueprint
  - 6 Security Profiles
  - Usability Analysis

Schedule: June 2009 – May 2011

Budget: $3M/year

($1.5M Utilities + $1.5M DOE)

Performers: Utilities, EnerNex, SEI, ORNL

Partners: DOE, EPRI

Release Path: UCAIug, NIST

Contacts:

Bobby Brown bobby@enernex.com

Darren Highfill darren@utilisec.org

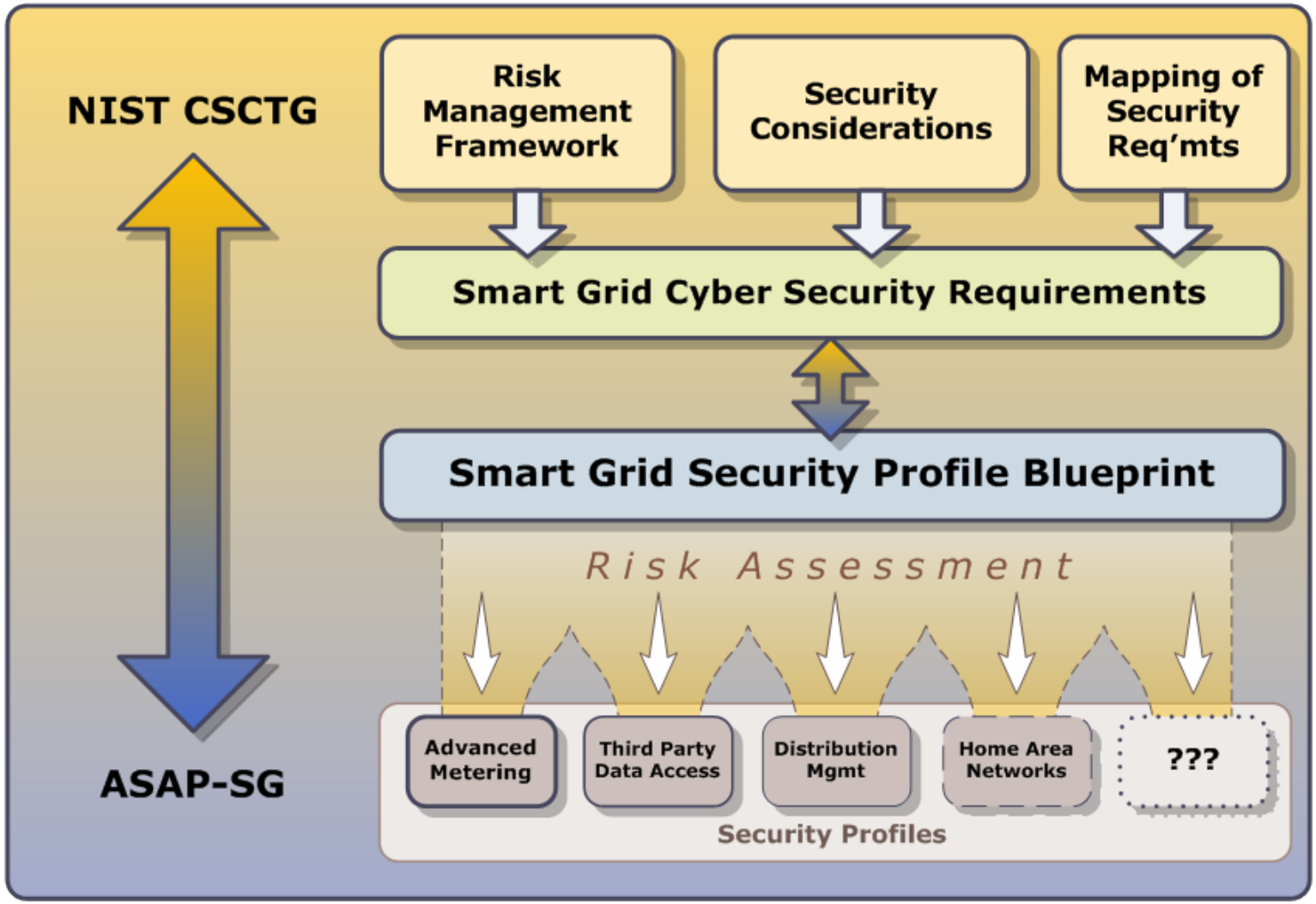
ASAP-SG Security Profiles

- Prescriptive, actionable guidance
  - How to build-in and implement security
- Tailored to a set of specific smart grid functions, such as
  - Advanced Metering Infrastructure  COMPLETE
  - Automated Data Exchange  COMPLETE
  - Distribution Management  UNDERWAY
  - Home Area Networks  PROPOSED
  - Wide Area Situational Awareness (Synchrophasors)  PROPOSED
  - Substation Automation  PROPOSED

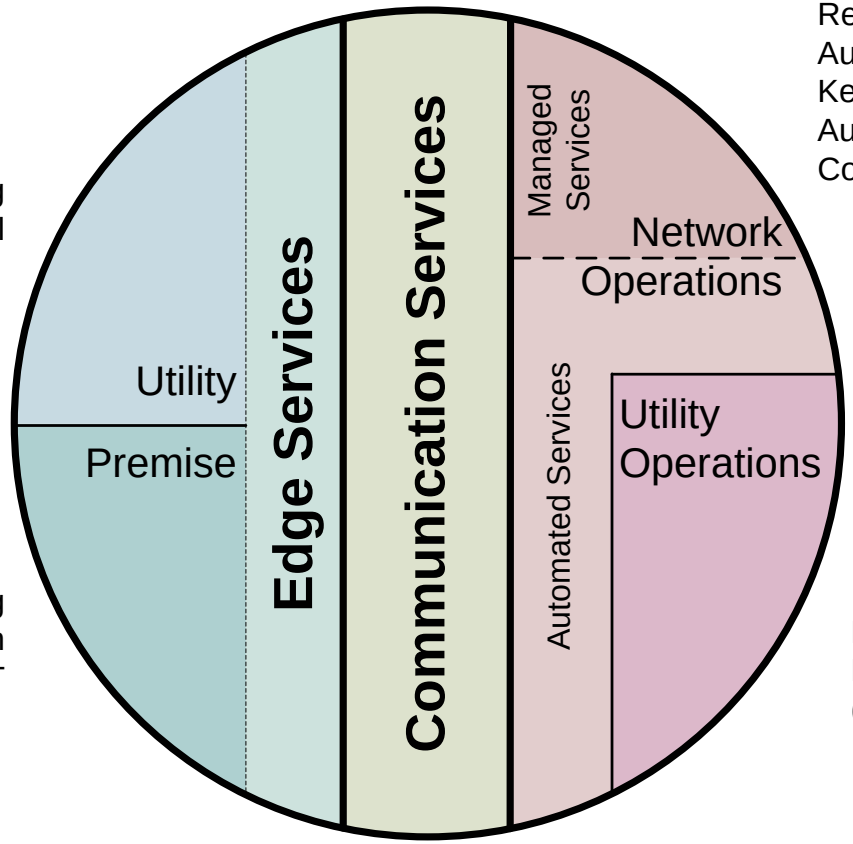
SG Security Working Group

- **Mission:** detailed requirements and best practices guidance for utilities procuring, implementing, and deploying smart grid technology
  - Technology-specific, but vendor-agnostic
  - Feed and accelerate SDO work (IEC, IEEE, etc.)
- **Status**
  - AMI Security Profile v2.0 ratified June, 2010
  - Third Party Data Access Security Profile under review
- **Participation**
  - 400+ Subscribers to various Listservs across 8 countries and 4 continents
  - Broad mix of utilities, vendors, government, and academia

Technical Coordination with NIST



AMI Security Services



Registration
Authentication
Key Management
Audit
Console Operations

Metering
Cap Bank Control

Routing
Filtering / Firewall Settings
Certificates

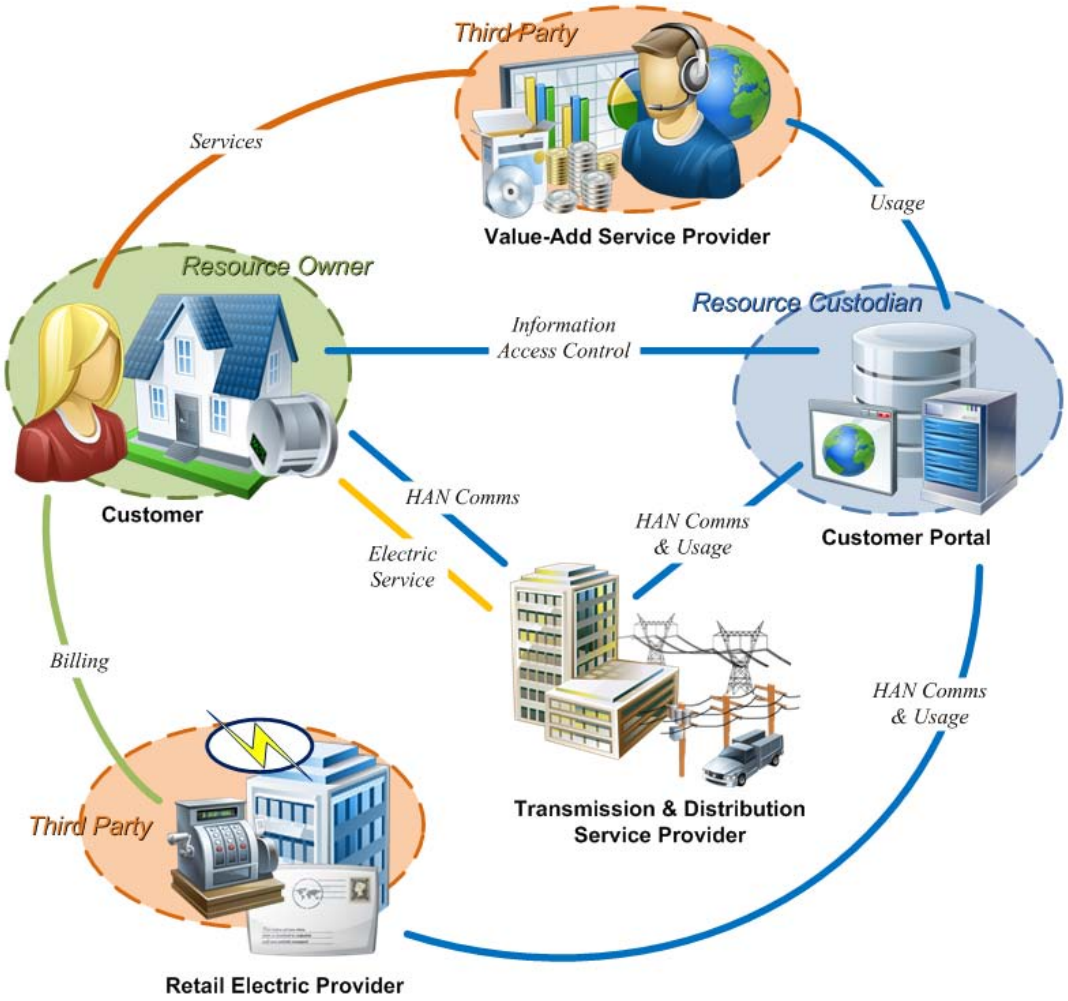
Submetering
Distributed Generation
PCT

Demand Response
Billing
(Business Applications)

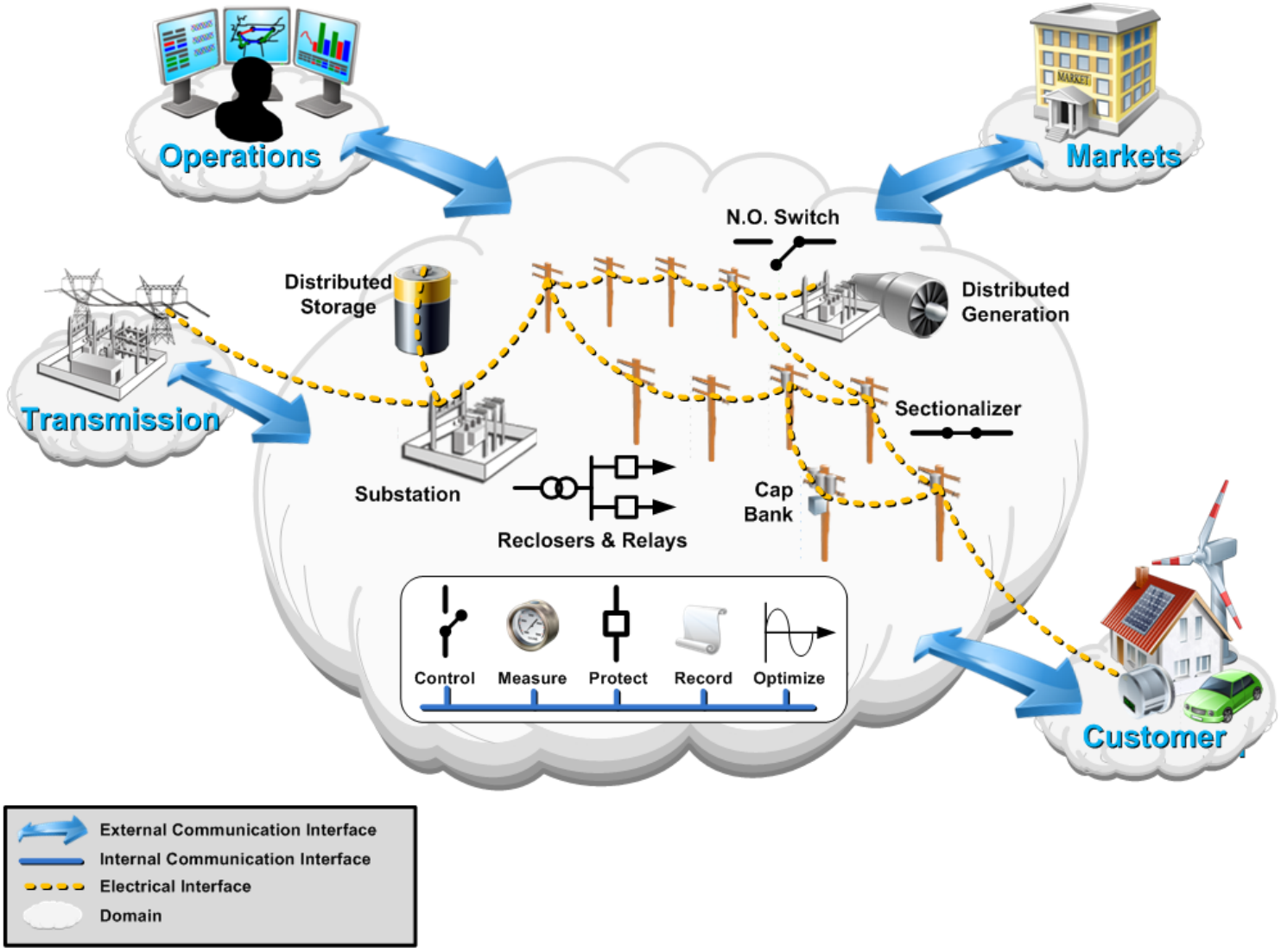
Aggregation
Transport

Text outside the circle represents example activity for service domains.

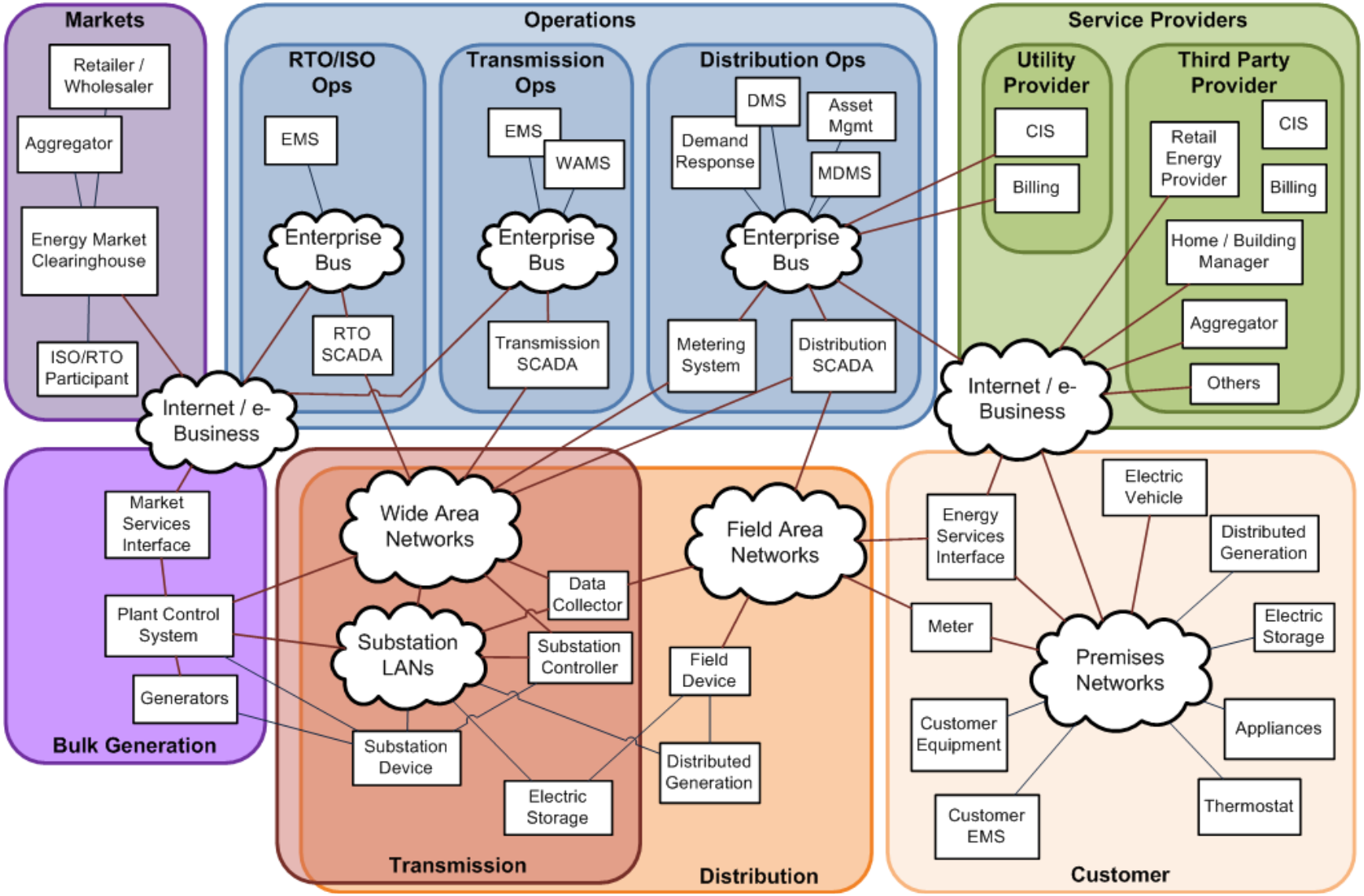
Third Party Data Access – REP



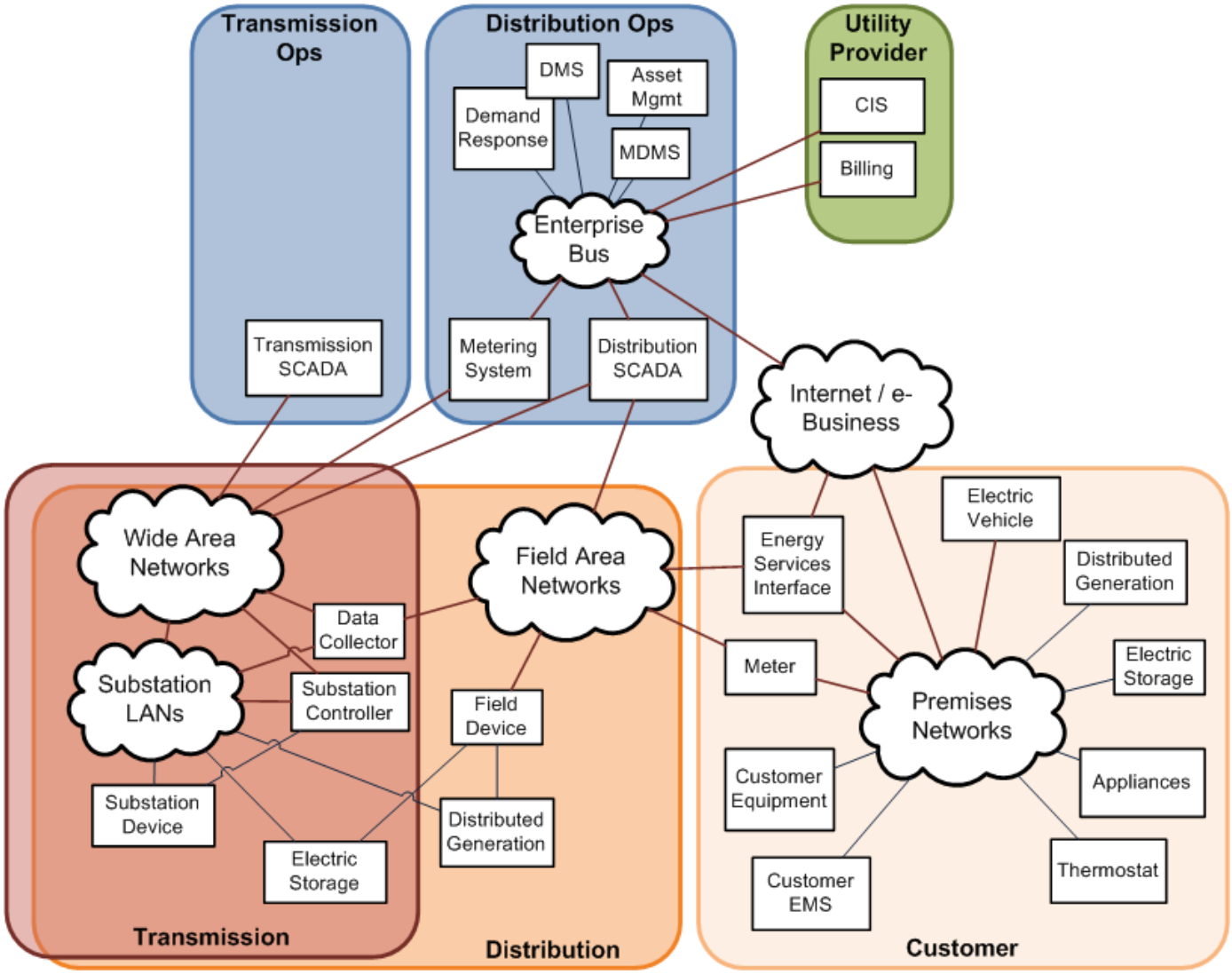
Distribution Management



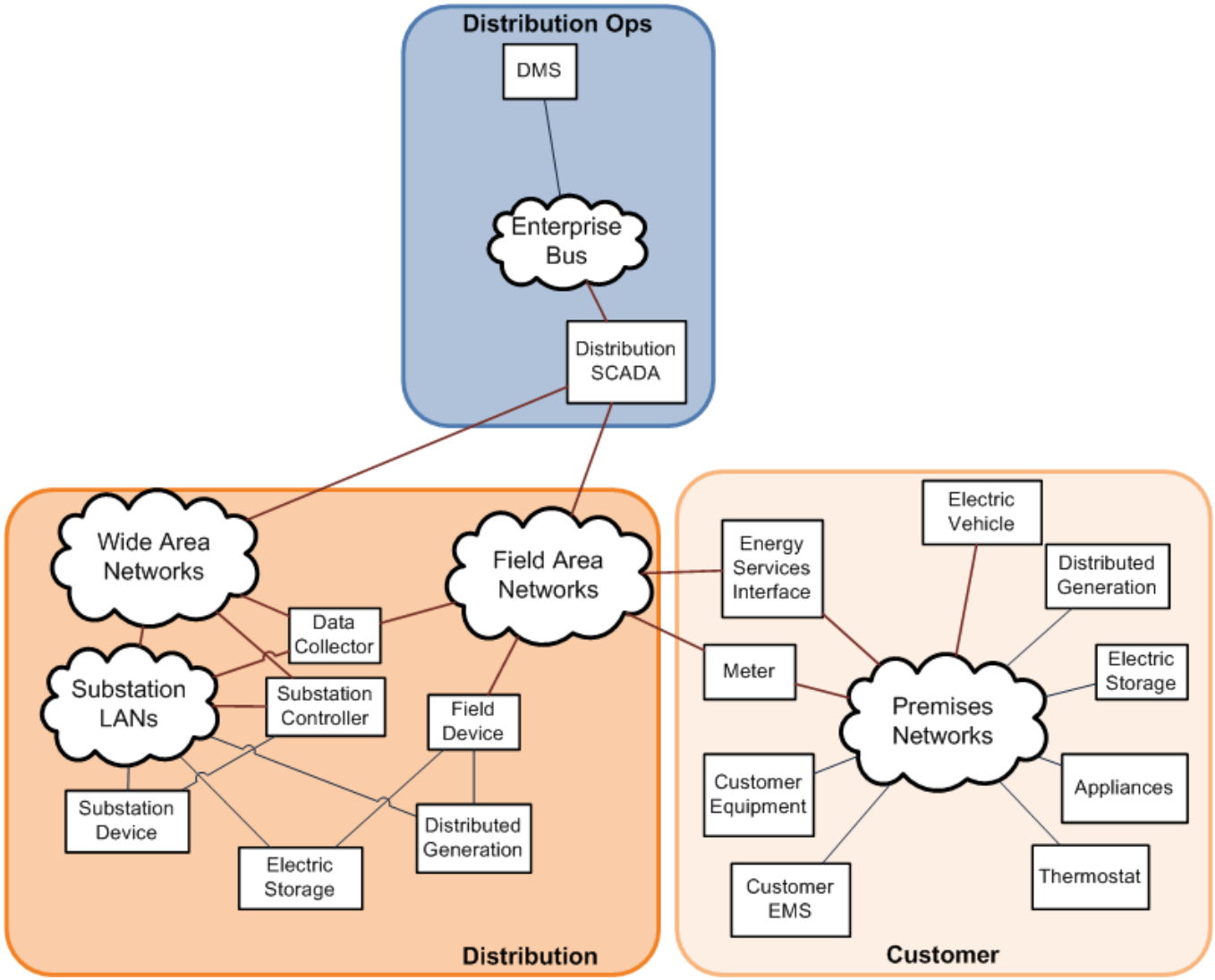
NIST High-Level SG Architecture



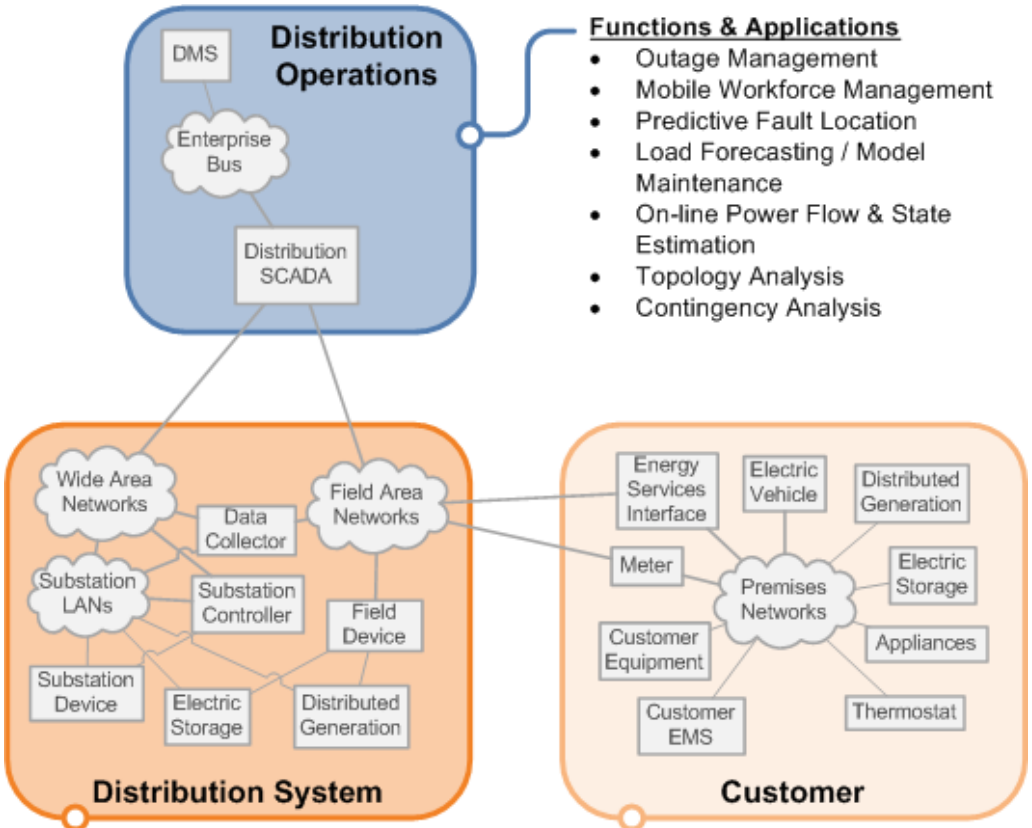
DM SP – In Consideration (Informative)



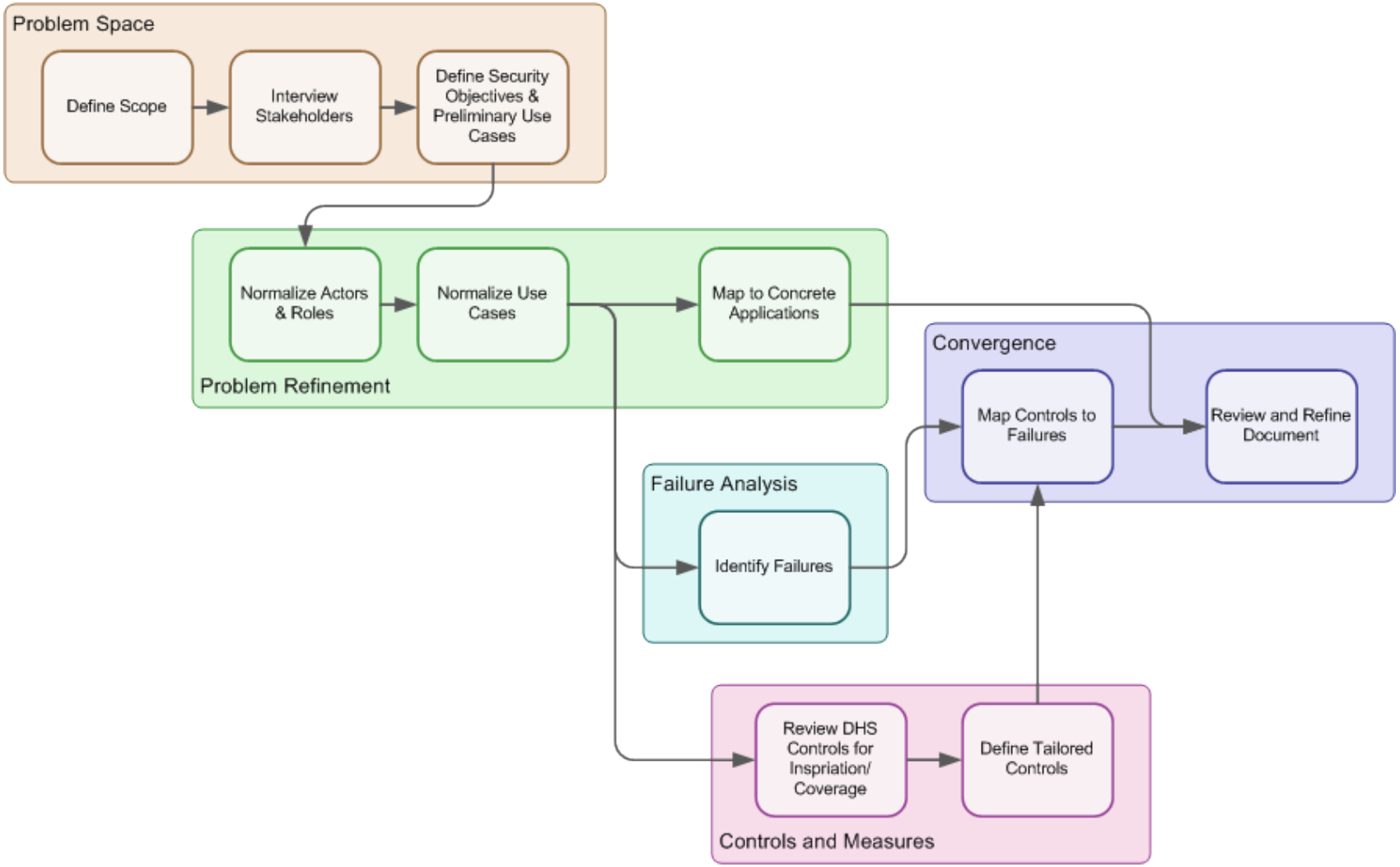
DM SP – In Scope (Normative)



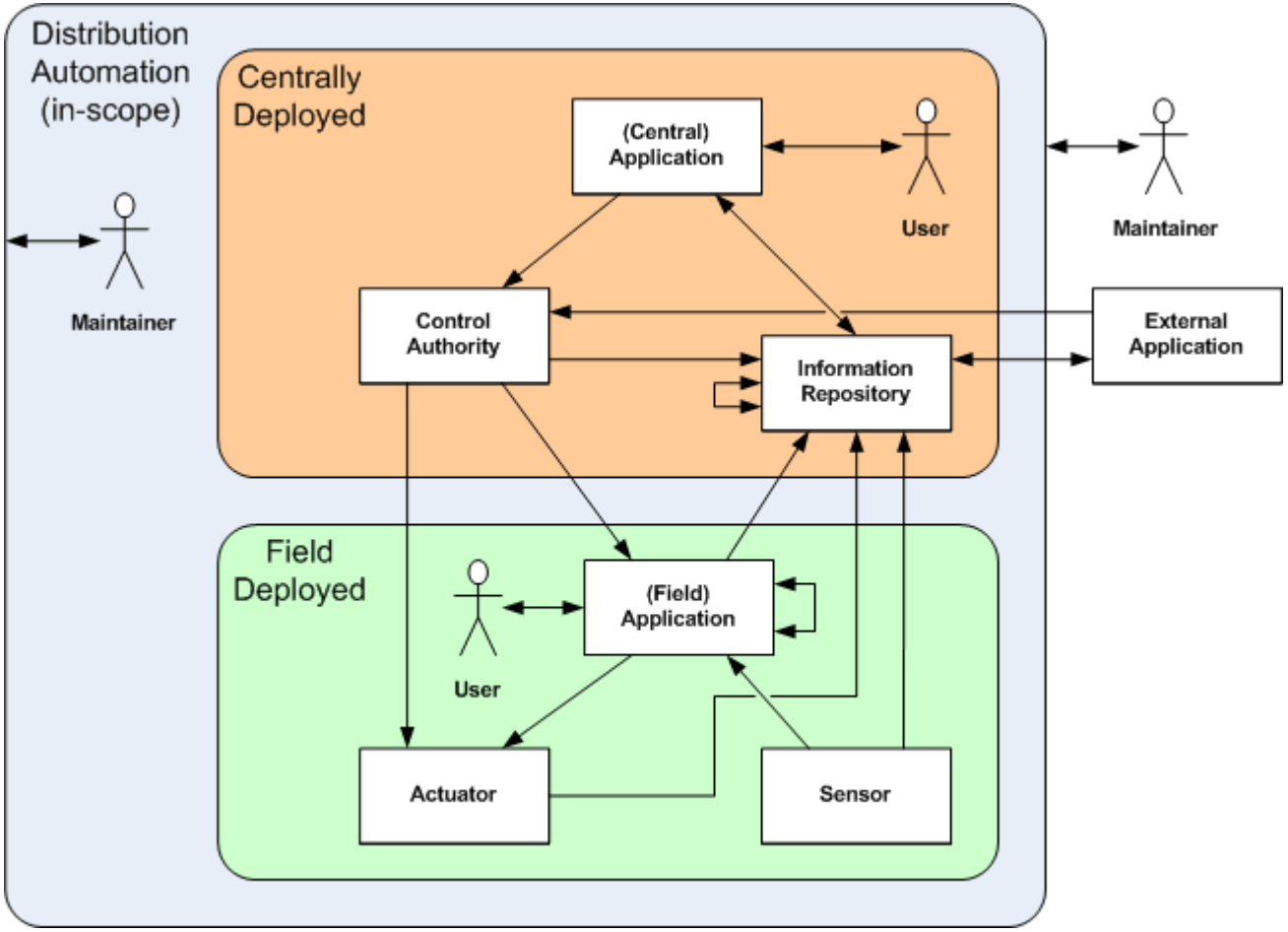
DM SP – Scoping Examples



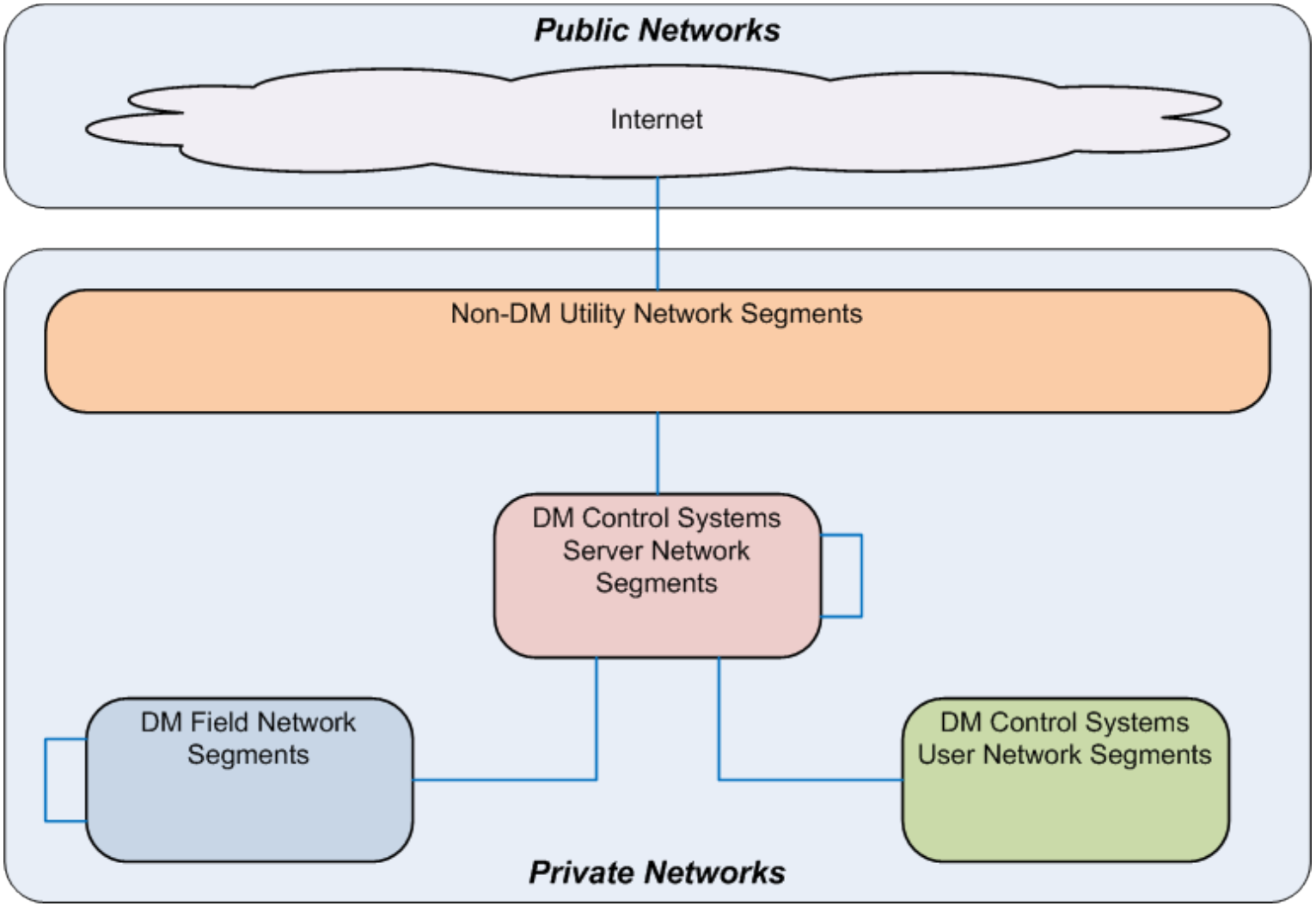
Technical Process



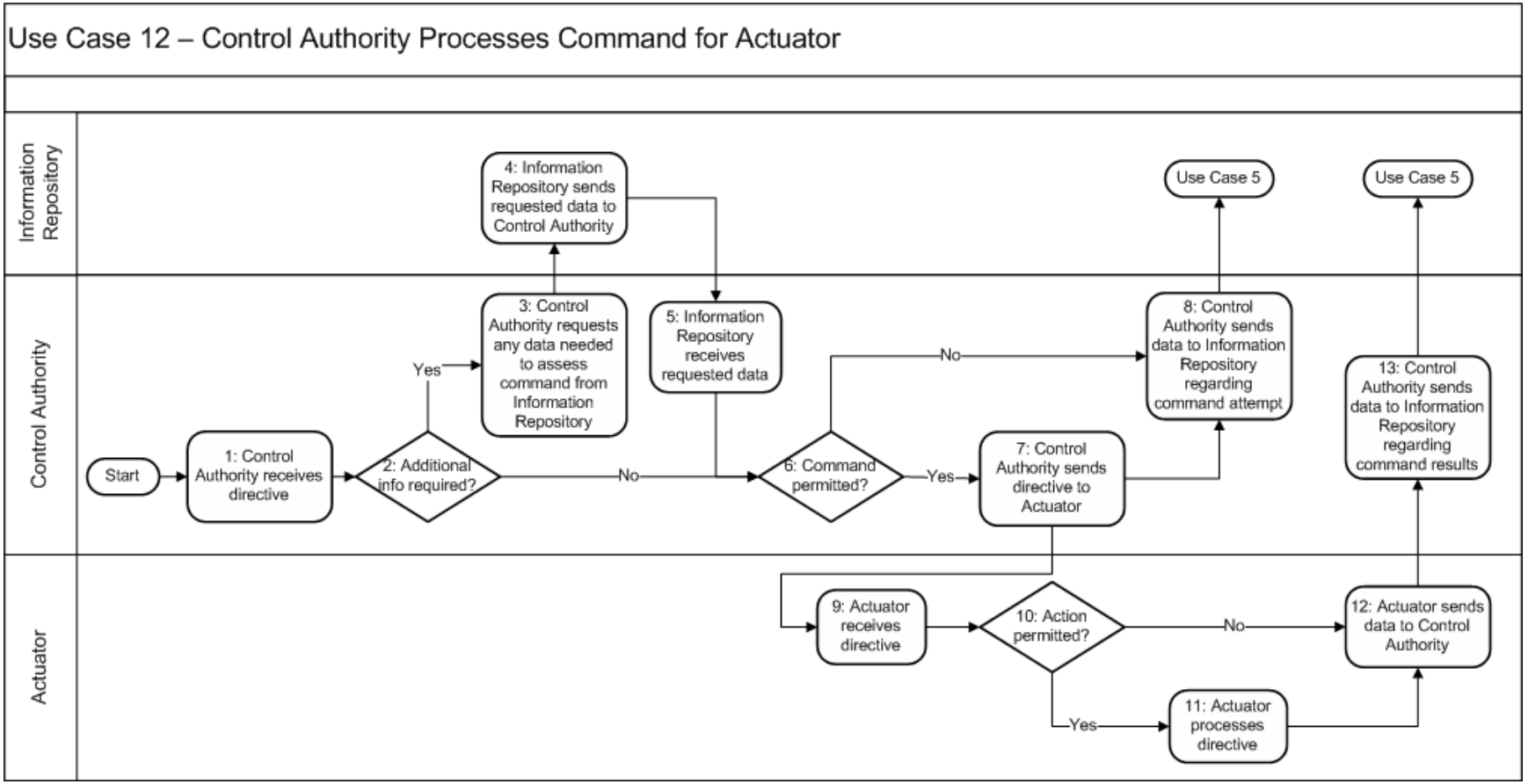
Abstract Architecture



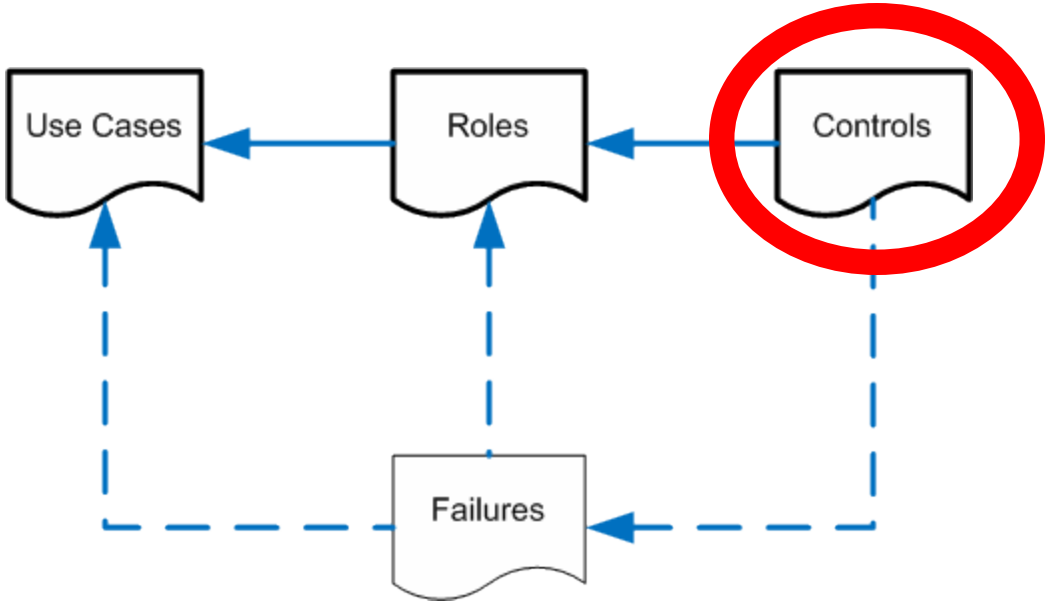
Network Segmentation



Use Cases

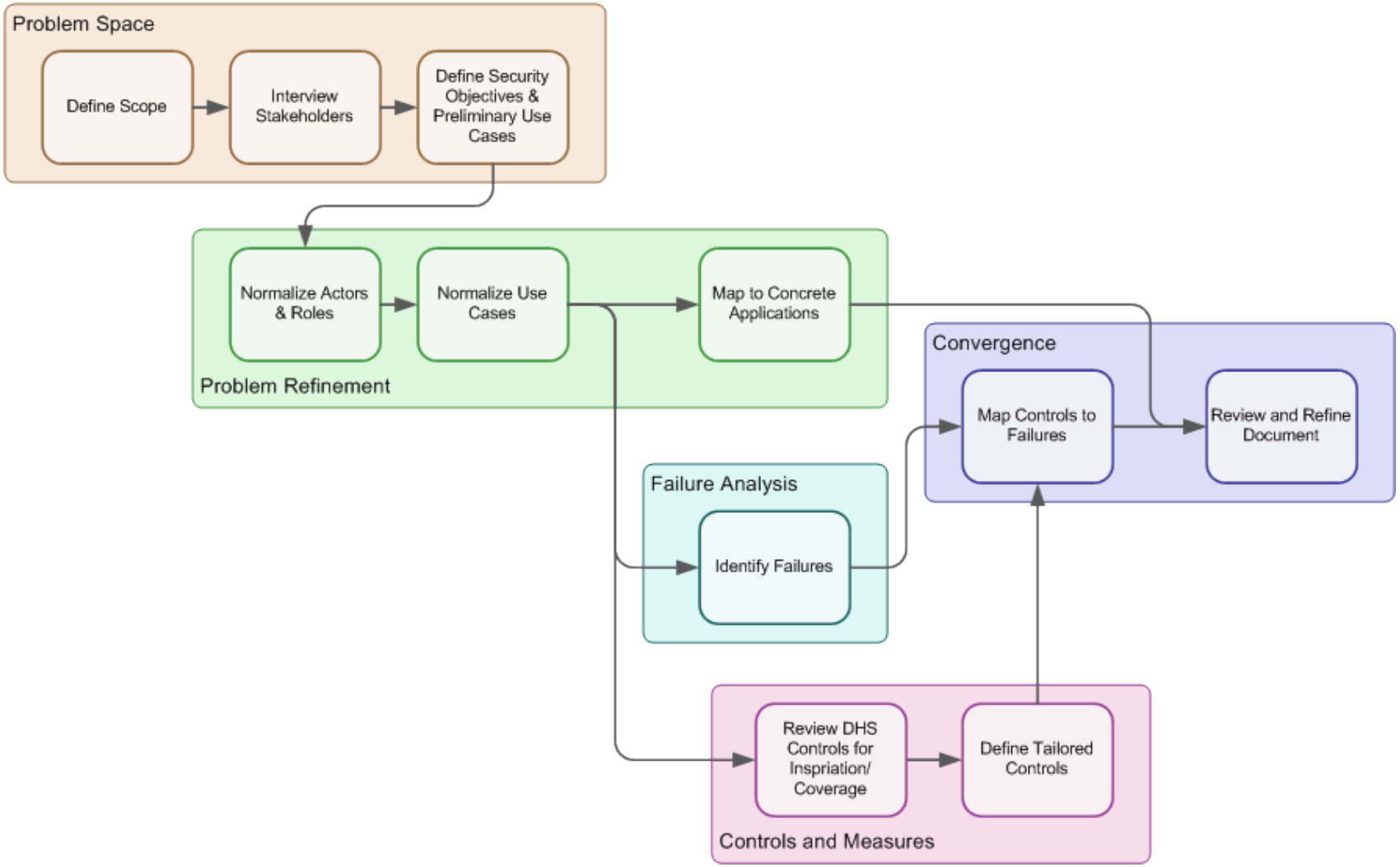

Use Case 12 – Control Authority Processes Command for Actuator
Information Repository
Control Authority
Actuator
4: Information Repository sends requested data to Control Authority
Use Case 5
Use Case 5
3: Control Authority requests any data needed to assess command from Information Repository
5: Information Repository receives requested data
8: Control Authority sends data to Information Repository regarding command attempt
13: Control Authority sends data to Information Repository regarding command results
Yes
No
Start
1: Control Authority receives directive
2: Additional info required?
No
6: Command permitted?
Yes
7: Control Authority sends directive to Actuator
9: Actuator receives directive
10: Action permitted?
No
12: Actuator sends data to Control Authority
Yes
11: Actuator processes directive

The Bottom Line



Actionable results for utilities and vendors

Technical Process



NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Notes
Cyber Security Order 706 SDT — Project 2008-06

July 13, 2010 | 8 AM to 5 PM PST
July 14, 2010 | 8 AM to 5 PM PST
July 15, 2010 | 8 AM to 5:00 PM PST
July 16, 2010 | 8 AM to 12:00 PM PST

Adopted Unanimously August 12, 2010

Robert Jones, Stuart Langton, and Hal Beardall
Facilitation and Meeting Design
FCRC Consensus Center, Florida State University

Joe Bucciero, Bucciero Consulting, LLC

http://www.nerc.com/filez/standards/Project_2008-06_Cyber_Security.html

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

CSO706 SDT July 13-16, 2010 Meeting Summary Contents

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

CSO706 SDT JULY 13-16, 2010 MEETING
CERT Software Engineering Institute, Carnegie Mellon University
Pittsburgh, PA

EXECUTIVE SUMMARY

On Tuesday morning, the Chair, John Lim and Vice Chair Phil Huff welcomed the members and participants to the SDT's 24th meeting. Joe Bucciero conducted a roll call of members and participants in the room and on the conference call. The host Sam Merrill, a participant in the SDT sub-team process, welcomed everyone to the facilities and covered logistics. Bob Jones, facilitator, reviewed the proposed meeting agenda. On Wednesday afternoon the SDT approved without objection the meeting summary for the June 8-11, 2010 SDT session in Sacramento, California. Mr. Bucciero reviewed the need to comply with NERC's Antitrust Guidelines each day of the meeting.

The Chair noted that the Team had met by conference call/ready talk three times since the Sacramento meeting to review and adopt a revised schedule to produce, ballot and send on to FERC a narrowly framed CIP 002-4 by the end of 2010. He also pointed out that the draft agenda sent out the week before has been revised based on member feedback so that the Team will be meeting together in a plenary format until at least Thursday.

The Vice Chair, Phil Huff noted the inclusion of "lunch and learn" sessions that are intended to present helpful additional information and briefings as requested by the Team.

The Chair and Vice Chair introduced the challenge of functioning with 26 members and an 18-member quorum to conduct business. After discussing the pros and cons a straw poll was taken of those members in favor of changing quorum in which 4 were in favor and 16 opposed. Following the straw poll the motion was withdrawn. A second proposal was offered for changing 75% decision rule to 2/3's. After discussing the pros and cons a motion was made to change the 2/3 decision voting rule for the SDT to 2/3s from the current ¾ and 17 members voted in favor with 3 opposed (85%) which passed.

This SDT reviewed information on the CIP 005 SAR presented by Scott Mix of NERC staff. Joe Bucciero reported that the NISTIR report released for internal review by NIST.

The Vice Chair and Chair introduced the concept of lunch briefings on key issues or efforts that have been discussed or requested by Team members. They noted that a "forensics" lunch and learn presented by SERT originally planned for this meeting will be scheduled for the Chicago meeting. At this Pittsburgh meeting three sessions were organized and presented:

1. Standard Format Concepts- Proposed New Approach to Scoping Controls Presentation - John Von Boxtel on Tuesday

2. A joint meeting with Darren Highfill and the Advanced Security Acceleration Project for the Smart Grid (ASAP-SG) Team meeting at SERT on Wednesday.
3. Substation Networks Presentation- John Varnell

The Chair summarized the SDT agreement reached on the July 2 teleconference to finish CIP 002-4 and ballot it and submit to FERC by the end of the year mean that the Team needs to finish CIP 002-4 by August in Chicago so that NERC staff can review and then the Team will refine and adopt it at the September using initial results of industry survey. The Team will continue working but will have to adjust the CIP 010 and 011 schedule for the industry review and response to after the completion of the CIP 002-4. The SDT explored working simultaneously and separately on survey and CIP-002-4 vs. releasing both at same time. At the conclusion of the schedule and survey discussion on Tuesday, the Chair asked Howard Gugel to develop and present some schedule options for the SDT to consider on Thursday. On Thursday afternoon Howard Gugel reviewed and the SDT conducted two straw polls on the following two options:

Option 1 – Release 002-4 after survey results, provide two days for the SDT to analyze survey results before approving for NERC staff review and send to Standards Committee for approval – only one ballot with possible re-circulation ballot for 10 days. (***Acceptable: 12 Not Acceptable: 0 Abstain: 4)***

Option 2 – Approve 002-4 and all related documents by end of July to post by August 6, release 002-4 concurrently with survey and have a 45 informal comment period without ballot, refine based on comments and another 30 day period leading to the ballot. (***Acceptable: 8 Not Acceptable: 5 Abstain: 3)***

Howard Gugel, NERC staff, outlined the NERC effort draft and conduct an Industry Survey on information that the SDT could utilize in the CIP 002-4 drafting effort. He reviewed the schedule which required industry comments on the draft, BOT approval of the survey and NERC conducting the survey in August with the results due back on September 7, which would be during the SDT's meeting in Winnipeg. The SDT discussed the survey covering the following areas:

- Mandatory information request.
- Justification for Thresholds.
- Focus on Completing CIP 002-4 first.
- Industry Ability to Respond.
- NERC Survey vs. SDT Survey.

The facilitator summarized the conversation noting Team concerns over: the "mandatory" nature of the request, the appearance that the request coming from the team and not NERC; concerns and assurances about how will information be used by NERC; and balancing whether there is any way to accelerate the survey process to have results in time to review in September, yet enough time to respond accurately if "mandatory."

The Chair noted that NERC has already posted a survey document for comment and date for responses to the draft survey cannot be changed. Thirty days for industry response seems to be minimum time we can allow for response to the survey. At the conclusion of the discussed the following motion was adopted:

- The SDT requests that NERC modify the survey language and transmittal letter to state that NERC is requesting the survey and correct the reference that states that the CSO706 SDT drafting team requested the survey. ***(18, in favor, 1 opposed)***

Following the motion, Howard Gugel presented draft survey revisions to the SDT consistent with the motion to address the concerns. On Friday, Howard Gugel asked for SDT feedback on the survey for the following concept regarding "at-large" generation facilities: "Generation Units as CAs that are at-large facilities (i.e. plants whose combined output is greater than the contingency reserve). CCA to be narrowly defined as the shared systems (requires changes to R2)." ***Members favoring concept: 10; oppose 0; abstain 1***

The Team reviewed and discussed a draft CIP 002-4 objective statement drawn from materials provided at the July 2 conference call meeting and suggested taking a few minutes to be sure the SDT agrees on the objective or outcomes we are hoping to produce with the development of CIP 002-4.

John Lim then presented the CIP 002-4 strawman for the SDT's consideration and input. He walked the SDT through the sections of the draft. The CIP 010 sub-team worked on producing this initial draft. The sub-team started with CIP 002-3 and developed a redline of proposed changes. The SDT discussed the draft CIP 002-4purpose statement including whether functions will be referenced.

4.3 exemption from 002-4 and Facilities

Straw Poll In favor removing 4.2? 15 members favor of removal of 4.2, 3 opposed. (83% support)

Requirements

Straw Poll on R2 examples

- How many favor including a list of functions as attachment – *5 in favor*
- How many favor the original R2 with examples? *6 in favor.*
- How many favor the original R2 without examples? *12 in Favor.*

Motion: to remove examples and keep remaining language R2 in first paragraph 14 in favor, 4 opposed. (Passes 78%)

Motion: The SDT objective for CIP 002-4 is to leverage the work already completed by the SDT for CIP 010 in developing a revised CIP 002-4 version that is narrowly scoped to identify

the Critical Assets in the Bulk Electric System through the use of bright line criteria as currently under development in CIP 010. 15 in favor; 3 opposed. Passes (83%)

The SDT reviewed and discussed and polled the proposed revisions to Attachment #1. The following are the Straw Poll results:

- Support for dropping 1.1: 15 in favor; 3 opposed. (83%)
- Support for Revised 1.2 language (a-d). Support for – Support 0 Oppose 19
- Support proposed changes to 1.3 - 13 oppose 0 support ; abstain 7
- Support section 1.4 as changed: 14 support; 5 oppose (74%)
- Support 1.5 as revised – 18 in favor 0 opposed, 1 abstain (100%)
- Support 1.6 as revised – 19 in favor 0 opposed (100%)
- Support including 1.7: 18 in favor; 0 oppose; 1 abstain. (100%)
- Substitute in 345kV –5 in favor; 14 oppose. (26%)
- Support 1.9 original language with FACTS and IROLs: Support 12; Oppose 0; Abstain 6 (100%)
- Delete the second sentence in 1.9 –14 in favor: 0 oppose: abstain 3 (100%)
- Proposal to use “control center” – Support 17, Oppose 2. (89%)
- Proposed language without limits for 1.14-1.16: 10 in support; Opposed 10 (50%)
- Support for: “Any control center or systems that are or could be used by a NERC registered RC or its delegate to perform RC functions. Support 13; Oppose 1; Abstain 8 (93%)
- Support for: “Any control center or systems and backup control center or systems performing RC functions.” 17 in support; 0 Opposed Abstain: 1 (100%)
- Support for Approach: Appropriate to incorporate bright line criteria from attachment 1 into the risk based methodology. Support 8 Oppose 12 (40%)
- Support for Thresholds on 1.18- 9 in Favor; 8 Oppose ; 1 Abstain (53%)
- Support for Thresholds on 1.19 10 in Favor; 8 Oppose ; 1 Abstain (56%)
- Support for Thresholds on 1.20. -12 in Favor; 6 Oppose; 1 Abstain (67%)
- Support for taking out distribution provider in 1.15: Support 14; Oppose 1; Abstain 1 (93%)
- Support for Wording in 1.14 and 1.15 from 002-3 R1.25 – “System and facilities critical to automatic load shedding under a common control system capable of shedding 300 MW or more.” Support 14; oppose 0 (100%)

On Friday morning the Vice Chair asked each Sub-team lead to give a report on progress since the Sacramento meeting. He suggested that as a minimum, each sub-team should complete its summary of industry informal comments received as well as the Dallas workshop input so a response document can be developed and be prepared for posting. Each of the following Sub-teams presented updates:

1. Systems Security and Boundary Protection (Jay Cribb, Lead)
2. Recovery Management Scott Rosenberger (Lead)
3. Personnel and Physical Security Doug Johnson (Lead),
4. Change Management, System Lifecycle, Information Protection, Maintenance, and Governance. Dave Revill (Lead)\
5. Access Control Sharon Edwards (Lead)
6. Implementation Plan Sub-Team Scott Mix (Lead)

The Vice Chair thanked the sub-teams for the significant work done by sub-teams despite the political sideshow. He noted he had underestimated when the SDT could get back to CIP 010 and CIP 011which may not be until December. Many in industry will want to know what was said and done at the Dallas workshop as well as the industry's informal comments. We need to decide soon how we want to address and respond to those in the future, but for now we need some closure on summarizing the comments we have received. WE may need a conference call or a webinar to explain why we are moving 002-4 and putting the 010 and 011 on hold. He urged each sub team to hold at least another call in order to create a response summary to industry comment by the Chicago meeting.

The SDT then conducted an initial discussion of CIP 010 and 011 Schedule. The Vice Chair noted the Team will review and adopt a proposed schedule in Chicago to send to the Standards Committee.

Phil Huff noted the 002-4 team will continue working. He discussed developing a revised schedule with 3 full days of meeting after September. Finally, the Vice Chair, on behalf of the SDT, thanked Sam Merrill and the CERT for their excellent hosting and facilities. He noted Doug Johnson will be our host in Chicago in August and urged members to register for the session.

Meeting adjourned at 11:30 a.m.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

24TH MEETING SUMMARY
Cyber Security Order 706 SDT- Project 2008-06
July 13-16, 2010
CERT Software Engineering Institute, Carnegie Mellon University
Pittsburgh PA

I. AGENDA REVIEW, WORKPLAN, SCHEDULE AND REVIEW OF NERC SURVEY

A. Agenda Review

On Tuesday morning, the Chair, John Lim and Vice Chair Phil Huff welcomed the members to the SDT's 24th meeting. Joe Bucciero conducted a roll call of members and participants in the room and on the conference call *(See Appendix #2*). The host, Sam Merrill a participant in the SDT sub-team process, welcomed everyone to Pittsburgh and Carnegie Mellon University and the meeting facilities and he reviewed the history and role of SEI in cyber security and covered logistics.

Mr. Bucciero reviewed the need to comply with NERC's Antitrust Guidelines *(See Appendix #3).* He urged the team and other participants in the process to carefully review the guidelines as they would cover all participants and observers. He urged all to avoid behaviors or appearance that would be anti-competitive nature and also reminded the group of the sensitive nature of the information under discussion.

The Chair noted that the Team had met by conference call/ready talk three times since the Sacramento meeting to review and adopt a revised schedule to produce, ballot and send on to FERC a narrowly framed CIP 002-4 by the end of 2010. He also pointed out that the draft agenda sent out the week before has been revised based on member feedback so that the Team will be meeting together in a plenary format until at least Thursday. He then reviewed the following proposed meeting objectives:

- To review the CSO706 SDT 2010 Work Plan and Schedule for CIP-002-4
- To explore and clarify the Work Plan and Schedule for completing CIP-010 & 011
- To review, clarify and refine the strawman CIP-002-4 standard proposal
- To receive presentations on forensics, sub-station networks and advanced persistent threats
- To convene sub-teams to review the sub-team responses to Industry comments and proposed changes to CIP-010 and 011
- To provide SDT guidance so sub-teams can make further refinements to CIP 002-4, 010 & 011

- To agree on next steps and assignments

The Vice Chair, Phil Huff noted the inclusion of "lunch and learn" sessions that are intended to present helpful additional information and briefings as requested by the Team. Bob Jones, facilitator, reviewed the proposed timed meeting agenda *(See Appendix #1*). The Team agreed to proceed with the agenda and on Thursday morning the SDT approved without objection the meeting summary for the June 8-11, 2010 SDT session in Sacramento, California.

B. SDT Consensus Procedures

The SDT were sent, as part of the agenda packet, some changes being suggested by the Chair and Vice Chair. (See Appendix #). Phil noted the challenge of maintaining a quorum in meetings when the Team has grown to 26 members. The current rule requires at least 2/3s of the members (18) present to establish a quorum. The proposal is to ask standards committee to allow 50% +1 rule for the SDT which would mean we would need 14 members present to establish a quorum. Phil Huff moved to and John Lim seconded the motion to change the quorum rule.

Discussion Comments

- Have we ever not had quorum at in person meeting? (Yes) Problem is with decisions on conference calls that we cannot participate on. May not be aware of the meeting and decisions will be made without members knowledge.
- Two conference call meetings in June to discuss and adopt a revised schedule had to be rescheduled due to lack of quorum.
- The is a quorum, not decision rule
- Could have two votes on two days and have different results?
- Why has the SDT gotten larger? A: Two new members were appointed by the Standards Committee to help the SDT with nuclear issues.
- Did not know that. Not happy about increasing size of group – why do we schedule decisions for Friday mornings instead of Tuesdays – Is this a scheduling issue?
- Concerned that we need to look at both rules together. So if we drop to 50% +1 quorum and down to 2/3's to make a decision, then it would be possible to make a decision with 2/3 or 10 of 14 or can make decisions with only 38% of the members.
- May also need to address issue of members who do not regularly participate but require a larger quorum.
- Not all of the SDT's business, considering the amount of work we need to do, can be done in person and requires phone review and votes. Yes, we need to address the issue of regular participation too – may need rules about participation in person and

by phone. Ready talk counts as participation to in-person meetings – when members agreed to join the SDT there was an expectation you could meet the obligation to participate. It would help for member to notify leaders if you can not make calls. When we send a notice of a call, the assumption is everyone can participate.

- We do try to participate on calls and we do have a real jobs. I commit to make the whole meeting as schedules. There should be no excuse to leave early. Friday votes may be necessary to follow on discussion and review at in person meetings – have to make the effort to be here, that is the commitment .
- I think that is a good point – commitment is to be available, even if team meets more often and longer than most – this team does not determine the standard, the ballot body does – you need to get something to the ballot body.
- Suggest that if the expectation is for more SDT conference calls, then we should schedule ahead of time on regular basis in order to allow us to reserve time in our schedule – one week notice is not enough time to set aside time for calls.
- Is the 2/3's vote for approval 2/3's of those present where there is a quorum? Yes.
- Need to understand in order to make judgment on quorum. It would mean that less than half the team could make decisions.
- Most standards teams are smaller and do not even have votes.
- This is a new subject, thus the larger team and more difficulty in making decisions

A straw poll was taken of those members in favor of changing quorum: 4 in favor: 16 opposed. (20%)

Following the straw poll the motion was withdrawn.

The second proposal was for changing 75% decision rule to 2/3's. Phil Huff made the motion and John Lim seconded.

Member Discussion

- This change might assist the SDT in making decisions more quickly and moving team forward and it follows the 2/3 quorum.
- 2/3 is the standards process default – team used 75% when it was smaller and to achieve higher approval level. This has proven difficult with the quorum at 2/3 (i.e. 18 members) 75% may be even more difficult to achieve and move the team forward.
- We need to be able to move forward with certainty. This is a brand new area, and in order to effectively convince industry we need to be sure team is fully on board. On any vote we have had, we have 1/3 on each side with the middle third going one way or the other – we need a substantial margin to ensure even members disagreeing on

particular issues can support decision on the package once made. WE need to hold ourselves to a higher level

- Do we need a quorum at time of the vote? A: yes. SM – quorum must be present at time of vote according to NERC's legal counsel.
- Need to be able to bring some of the dissenting third on board into the decision if we then want to sell it to the industry. In the end we have to do a better job of selling issue to the industry and that starts with building consensus in the room.
- We also have to be willing to compromise and some individuals in this room have found it hard to compromise – taking hard positions and refuse to move – too many on the team

Motion: To change the 2/3 decision voting rule for the SDT to 2/3's from the current ¾ 's (75%).

17 in favor 3 opposed Passes (85%)

Comments after the Vote

- We need to promote member participation and schedule votes well in advance – need to bring the dissenting side along as much as possible – need to work together, collaborate on decisions
- It is easier to schedule early and cancel than to schedule late.
- We will try to schedule votes ahead of time as much as possible – members need to reply if they cannot make it so we can have an idea if we will have quorum – if you do not respond, assume you will be able to make it.
- Is a proxy vote or vote *in-abstentia* possible? A: not allowed under NERC's standards rules.
- May not have an hour for long discussion but can jump on for quick review and vote in 5 to 10 minutes – also need subject of the vote to determine importance of participation.
- We will clarify if a call involves a vote and what subject of the vote will be.
- Can we use an on-line voting tool that allows us to read it and cast vote over a period of time? The SDT approved an email voting provision but it is very limited in its use.
- We also need to allocate enough time for calls in which votes will be taken.
- Set regular schedule of time blocks for possible calls such as every two weeks.
- Voting in the interim between meetings has been used twice due to time and schedules – also, note the last month was sloppy due to requests from the Standards Committee – not a good precedent – hopefully used only in emergencies – blocking off time is a good idea, but use only if needed.
- The consensus process provides that the SDT strive first for unanimous agreement based on thorough discussion but that depends on willingness of some not to oppose after thorough vetting of issues and concerns – have to be willing to listen to others as well as argue your own point – broader effort to get quality product from the collective knowledge you bring to the table.

C. Related Cyber Initiatives

1. CIP 005 SAR.

- Scott Mix provided an update on urgent action process for reviewing CIP 5 - SAR is done and the standard is 80% complete – deals with support and maintenance from vendors and the devices used for remote access – wholly impractical to have critical assets located at vendors. Jim Brenton noted he was involved and it was a good team. They are clarifying terms including the use of laptops for system maintenance and vendor access – look at advisory and it sets out the valid reasons for the vendor access and need for control and oversight of the laptops.

Member Discussion

- How can I get involved?
- What is the relationship between the CAN information, Jim's team, and our effort? A: CAN and urgent action process relationship? None – for this team, need to be sure later work on 011 matches up with work done by the CAN and Jim's team.
- Do this replace this teams work? –The process is very unclear
- No, but need to be sure they match up
- Almost all support can access the system and test operations – the CAN missed the mark, puts the grid at risk by limiting our efforts to make process and access more efficient – reduces reliability rather than enhances
- Urgent action is a new version? When is it due out? May cause confusion
- All hits about the same time
- Seems like it will slide in well with the draft maintenance section in 011
- Six wall perimeter and how you handle it – careful if we are changing ESP's
- Reviewed the people working on the urgent action team

2. NISTIR Report

Joe Bucciero reported that the NISTIR report released for internal review by NIST – three volumes – to be released soon to outside review – will not go through a FERC process before release to industry and is not subject to formal FERC approval.

Member Comments

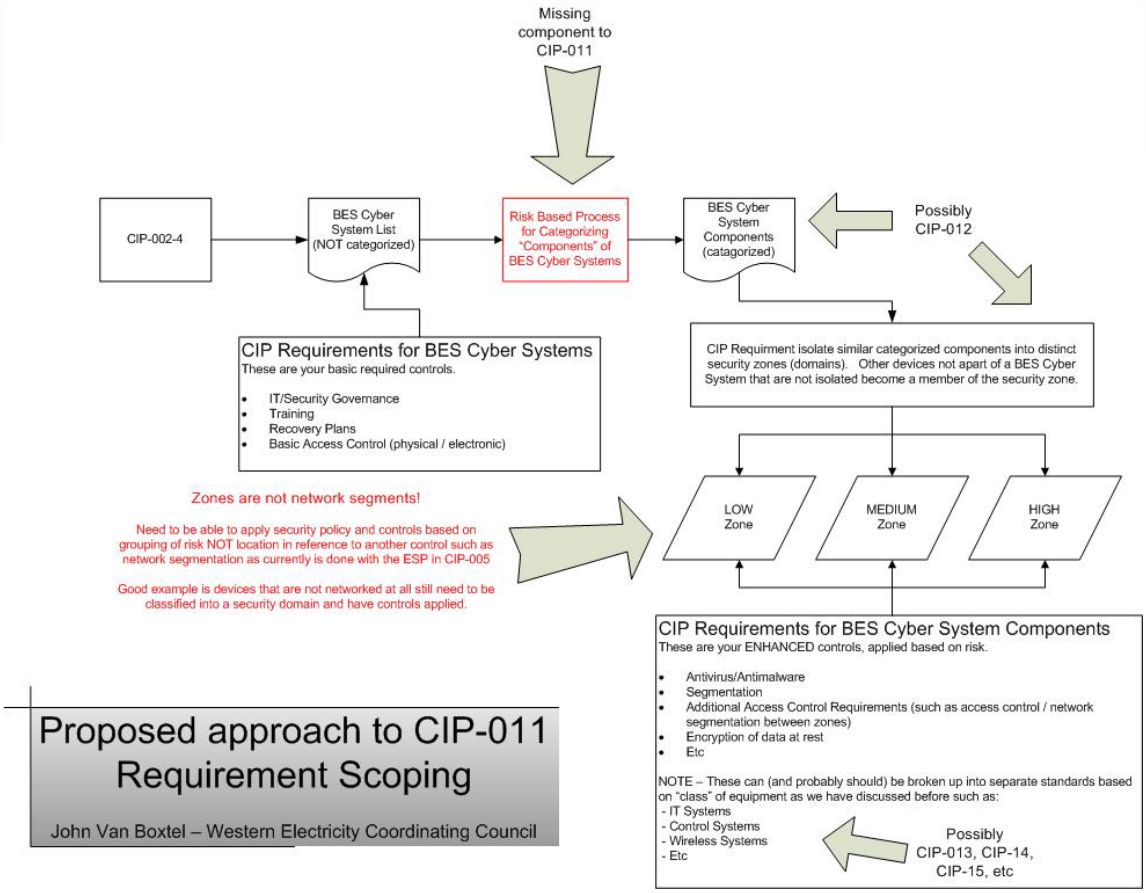
- FERC is providing input if not formal approval
- CCI guidelines completed and now official
- Cyber security group formed by NASBE too – still high level at this point
- Has anyone discussed Senator Collins Bill? It includes a requirement to report cyber incidents to new Homeland Security director position.

D. Lunch and Learn Sessions

The Vice Chair and Chair introduced the concept of lunch briefings on key issues or efforts that have been discussed or requested by Team members. They noted that a "forensics" lunch and learn presented by SERT originally planned for this meeting will be scheduled for the Chicago meeting. At this Pittsburgh meeting three sessions were organized and presented.

1. Standard Format Concepts- Proposed New Approach to Scoping Controls Presentation - John Von Boxtel

John Van Boxtel presented a proposed different format approach to scoping and tailoring controls to risk. This would be an approach that would leverage the work on CIP-010 while solving some of the problems with trying to apply controls only based on the impact level of BES Cyber Systems. The main proposed difference is to apply a base level of controls at a BES Cyber System Level and to apply additional controls to the BES Cyber System Components based on grouping into different security zones based on risk for the SDT to consider. During and following the presentation the SDT informally discussed some of the ideas presented.



Member Discussion

- Changing words to zone or segment is not effective – now we have high, medium and low – should have different boundaries – if not connected then just a physical boundary.
- You can have protection around h-m-l and have further system segregation for high assets
- If you have one high connected to low – the attack will come through the low to get to the high.
- We need to break things up based on risk, not as part of systems.
- Separating those that are at risk from those that are not is the "crux of the biscuit" (Frank Zappa – apostrophe album) Further segmentation is the concern. "Domain" means different things in different contexts.
- What about calling them "zones"?
- How do you segment zones
- Initial requirement in 011, then additional requirements in subsequent standards to further layer on additional controls for specific zones.

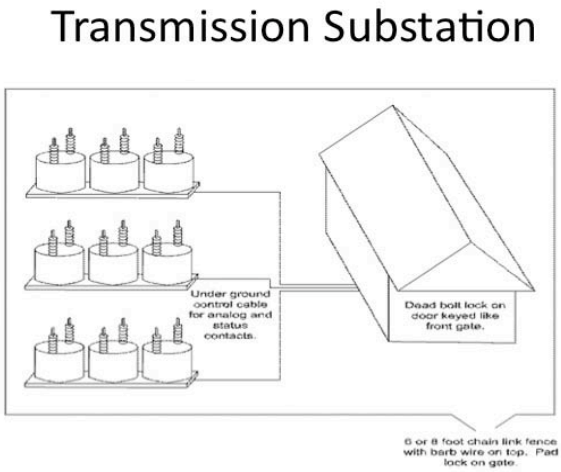
- How would you determine high-medium-low?
- Still have to establish the criteria.
- Is this biased toward the controller? Problematic if bringing in broader ring of corporate assets.
- This may be the "three by three" matrix creeping back – zone classifications come out of that matrix.
- This is similar but a little more broken out.
- The red box pulls the multiple matrix back in and we do not have time or understanding to pull that together.
- This is a separate standard from 010
- The multiple matrix was only in the concept paper and the industry gave strong feed back not to do that because it was too complicated.
- Might be more receptive if you give industry their own risk based methodology for figuring out the h-m-l –
- Problem with the "red" box is that it moved away from "acceptance of risk" to meet FERC concerns – if identify as critical then you have to be prescriptive.
- Also, how do multiple zones work within one interconnected system?
- It will depend on how they are connected to determine the vulnerability of a component – two separate sets of risk assessment.
- This might work with IT but not in the power industry.
- This is where the smart grid is headed.
- This will give too much leeway to a few to screw it up for the rest of the industry – need to universally apply standards to be fair. Could create a competitive disadvantage for fully identifying critical assets.
- This works if the team can come up with something reasonable for the red box.
- Previous teams wrestled with this issue. You can use categories, classes or zones, but Mike Peters at FERC consistently says that everything needs something – you have the production and the distribution – baseline is and ought to be different for a control center and a substation – give thought to differences in the physical location. We have been thinking about big, medium and little iron. The Team should think more about the connection to the system.
- Zones allow for baseline for everything and additional protection for a control center – have to address the issue or will be wasting time on 011.
- Taking something from routable to serial should not be considered gaming the system – instead it is a business decision.

- Is the SDT getting away from 706 – take what is in the order and fix 003-009. (*participant)*
- 4.2.1? FERC asked for clarification – should cabling be exempt if within the physical boundary (*participant)*
- Use base level of protection on all assets and a cyber risk assessment above and beyond the base.
- Also tired of hearing about gaming – it is business decisions – we do not have a well defined problem statement – clarifying what are we trying to accomplish will be key to project management.

2. **A joint meeting with the ASAP-SG Architecture Team meeting at SERT on Wednesday.**
   Darren Highfill and the Advanced Security Acceleration Project for the Smart Grid (ASAP-SG) Team met with at SERT with the SDT and discussed possible opportunities for coordination.

3. **Substation Networks Presentation- John Varnell**

John Varnell presented information on Sub-station Networks for the SDT to consider. During and following the presentation the SDT informally discussed some of the ideas presented.



II. CIP 002-4 REVIEW AND REFINEMENT

A. CIP 002-4 Schedule

1. Initial CIP 002-4 Schedule Issues Discussion

The Chair summarized the SDT agreement reached on the July 2 teleconference to finish CIP 002-4 and ballot it and submit to FERC by the end of the year mean that the Team needs to finish CIP 002-4 by August in Chicago so that NERC staff can review and then the Team will refine and adopt it at the September using initial results of industry survey. The Team will continue working but will have to adjust the CIP 010 and 011 schedule for the industry review and response to after the completion of the CIP 002-4.

Member Comments

- Results will be essential to setting metrics – however there is a scheduling disconnect that will not allow the Team to review, analyze and incorporate the learning from the survey results into CIP 002-4 that same week.
- The facilitator noted that the Team had tried to change SDT meeting to the following week but that would conflict with CIPSE meeting which a number of Team members and NERC staff directly participate in.
- Can we cut some red tape and streamline the survey process? Looked carefully at this but there is very little flexibility in the notice times etc.
- Critical path for the SDT is through the survey. We need to find a way to accelerate the survey to get the info back sooner – no one looking at it yet because the date is too far off in the queue of work. NERC President, Gerry Cauley, may be the only one who can light a fire and get it done
- We need a schedule we can all live with. Concerned about the confusion this might create in the industry. Looking at the overall 010 and 011 schedule, it looks like industry voting in February while 002-4 moving through approval with FERC?
- The schedule only provides for 2 CIP 002-4 ballots with the 2nd in December.
- The Motion adopted on July 2 by the SDT call does not include balloting beyond 002-4. The CIP 010 and 011revised schedule has not been discussed and approved by team yet.
- A draft of the survey was briefly reviewed by Howard Gugel with the SDT at the July 2 conference call meeting on schedule. There is an appendix of the draft in the July 2 meeting summary.
- The SDT agreement was to complete CIP 002-4 without impacting the CIP 010 and 011 effort. However that is not realistic. We need to continue to work on these simultaneously, however we should focus on completing 002-4 first.

- Is the comment period required under the NERC rules of procedure? Yes, and it is being expedited.
- **Working Simultaneously and Separately on Survey and CIP-002-4 vs. Releasing both at same time.**
- Why can't the survey be part of the info requested during the posting of CIP 002-4? Try to fold into the comment period?
- NERC is under pressure to get numbers to share for Congress.
- NERC is proposing not folding the two together but rather conducting simultaneously and separately with CIP 002-4 for comment at same time the mandatory survey request is out.
- What about finishing CIP 002-4 complete by end of the Chicago meeting and put out simultaneously with the survey?
- If we try to finish by end of the SDT August meeting and post at same time as the survey, we might buy some time for a third ballot but we would have to complete our work at this meeting so NERC staff could review between now and Chicago.
- Are we severely underestimating amount of work needed for 002-4? The Team should consider dividing up to work on 002-4 and the rest of the Team could continue to work on 010 and 011. Bringing this up now because it impacts any proposed schedule.
- The NERC survey is intended to help the Team to understand if we have the line for heavy/medium drawn in the right place –Question 1 and 2 are quick, 3 may take a little more time – if compress it, industry will express concerns about the validity of result.

2. Review and Testing Consensus on CIP 002-4 Schedule Options

At the conclusion of the schedule and survey discussion on Tuesday, the Chair asked Howard Gugel to develop some schedule options for the SDT to consider on Thursday.

a. Option 1- Conduct Survey in August, Post CIP 002-4 in September

On Thursday afternoon Howard Gugel reviewed with the SDT the Option 1 schedule which called for release of the NERC survey in August, the SDT analyzing survey results at their September meeting before approving for NERC staff review CIP 002-4 and send to Standards Committee for approval. It would provide for only one ballot with possible re-circulation ballot.

Member Comments

- Line 53 – what criteria will be posted in the survey?

- Date actual survey will go out – include the teams output – may be additional data points that NERC staff will include such as 1.1 – not painted as a request from the team, only from NERC – very quick turn around – may add an arbitrary line for "medium" to get additional level of data.
- May cut "high" in half for "medium" as a data point.
- Line 56 – challenging to get results and make decisions by that next Friday
- Two days is for team to analyze – survey closes in thirty days during the SDT Winnipeg meeting.
- Survey finalized by 7/26? Good chance "high" as we have it will not identify enough – think in Chicago about "what if" scenario responses to possible survey results – wait until September and results in hand may be difficult.
- This approach takes away from getting other work done.
- May need to organize discussion to test potential responses.
- May be better to let a sub group of 2-3 create straw man without putting too much full team time into speculative responses.
- Trying to back everything into same time period – May need to schedule a team call for the Sept. 15th? Same day as CIPC meeting.
- Will NERC put in request for information on nuclear even if not in the current version? A: Yes.
- Will gain assets, stay the same or will lose assets – industry fears impact of increased number and cost impact and decrease on political optics - any space for narrative responses we have to respond to? A: No, data only.
- Comment period is on now for survey structure – this schedule is very tight.
- How can we work on this, on 010 and 011 and our real jobs too?
- NERC staff will prepare draft responses to the first posting of 002-4 as starting points for the team to work on.
- Will we work on the other documents related to 002-4 in Chicago in August – comment form, VSLs, etc.?
- Might be of value for each of us to fill out survey as a subset of the survey and use as an example to think about responses at the Chicago August SDT meeting.
- What about the implementation plan for 002-4? A: 24 months as planned for 002-3.
- We should consider splitting into separate teams to make progress on 010-011 and the 002-4 in the time given
- Even if initially review, we still need full team review for approval and adoption.

- Should we consider going to the Standards Committee to split the team into two separate teams to work on the two tracks?
- Schedule needs to reflect the implementation plan and other related documents for 002-4 and factor in the time needed.
- We will need to focus full group time to review and discuss – small sub group could bring a product forward.
- It will be folly to think much progress will be made on 010-011 until end of the year and work on 002-4 completed – given a new directive.

Straw Poll
Option 1 – Release 002-4 after survey results, provide two days for the SDT to analyze survey results before approving for NERC staff review and send to Standards Committee for approval – only one ballot with possible re-circulation ballot for 10 days.

Acceptable: 12 ***Not Acceptable: 0*** ***Abstain: 4***

b. Option 2: Post CIP 002-4 along with Survey

Howard Gugel reviewed with the SDT the Option 2 schedule which would allow for two comment periods, issuing the first version of 002-4 along with the survey. The SDT will have to respond to two comment periods and need an approval by end of July for CIP 002-4 – not a ballot – but includes implementation plan.

Member Comments
- May get the same result from option 1 by putting content into the survey.
- The thought here is that people prepare comments along with survey and gives team two shots at explaining rationale – providing the pros and cons to both approaches.
- Which option offers most time to evaluate data – only two days in the first option and seven days in option two?
- Favor second option – still don't see us making progress on 010-011 until end of the year with either option.
- Hopefully the survey will inform our understanding and rationale.
- The survey will inform the second posting in this option
- The work products due with posting means the SDT will have only two weeks time to review and develop the implementation plan under this option
- With option 2, how much harder will it be to make changes based on survey input?

- May be easier with two comment periods in option 2. The first comment period does not include a ballot.
- Explanation of the criteria may not be enough – balance realities of what has to happen with what industry may say if there is a big increase in assets identified.
- In terms of the implementation plan, if you don't have to recreate critical asset plan then that will greatly reduces the amount of work
- The first option allows us to make changes and justify using the survey results.
- May be a lot of association pressure to pass whatever version we put out regardless of grousing.
- An implementation plan requiring changes would not be justified at this point. It should be a relatively simple plan – probably able to prepare in three days.
- CIP 003-009 changes are just conforming? Yes
- Yes, except for the other group on CIP 005 which may only confuse the industry more
- Survey going out independently might mean the data is less skewed.
- Delivery of CIP 002-4 by the end of July is the major problem with Option 2
- Possible exception for additional documents with the posting? A: probably not.
- Much of the comments last time related to the lack of related documentation – people want to know the rationales.

Straw Poll

Option 2 – Approve 002-4 and all related documents by end of July to post by August 6, release 002-4 concurrently with survey and have a 45 informal comment period without ballot, refine based on comments and another 30 day period leading to the ballot.

Acceptable: 8 **Not Acceptable: 5** **Abstain: 3**

B. NERC Industry Survey and CIP 002-4

Howard Gugel, NERC staff, outlined the NERC effort draft and conduct an Industry Survey on information that the SDT could utilize in the CIP 002-4 drafting effort. He reviewed the schedule which required industry comments on the draft, BOT approval of the survey and NERC conducting the survey in August with the results due back on September 7, which would be during the SDT's meeting in Winnipeg.

Member Comments on Survey

Mandatory information request.

- Is this a mandatory request? Yes, industry must respond. However there is a statement that the data will not be used to monitor compliance.
- NERC is using a "mandatory" request to insure timely responses that can be used by the SDT. There was a request at the Dallas workshop for a voluntary response which was met with total silence. However the mandatory 1600 process brings with it a slower bureaucratic process.
- People concerned are at one level above those who have to respond – yes, you probably need to go mandatory.
- It would be possible, but perhaps not advisable, to post CIP 002-4 during the survey, but we cannot delay the survey to look at final version and meet the December deadline. We would have a scheduling nightmare, the proposed schedule is the only way to physically meet the deadline.
- NERC realizes Congress and Senate up for reelection and under pressure to do something – Gerry Cauley needs hard numbers to fend off pressure. I misunderstood and told my folks it would not be mandatory and would be anonymous.
- Of mandatory then it may raise flags of concern in the industry that it will be used against us.
- Uneasy feeling that this is about FERC and Congress asking if this is enough critical assets – what are we going to do with the data, nothing – what if the the former says it is not enough assets?
- Comfortable with an informal survey but mandatory response will put team in position we do not want to be – this may mean the list will have to be the same as the final list we will be requiring – if it is not the same, what happens to the company – if numbers don't match, companies may find themselves in hot water? A: The survey instructions say the survey is to only inform the team and guide development of the standard. We are looking for a reasonable response, not an exhaustive one. The survey also states how the data will be used, and that is will not be used for any future compliance action or monitoring.
- This will still be seen by industry as a legal requirement.

Justification for Thresholds.

- 002-4 uses same bright line criteria, sort of, as 010 – told we need to provide clear basis for bright line – industry feels they are arbitrary – the questionnaire just moves the arbitrary line – we tweak the lines to get the number we or someone else wants? Difficult to establish the basis for the threshold, boat load of work
- The industry perceives little difference between team and NERC. Why put the times together? Industry is confused why going back to 002-4 from 010 – conflicting message, survey just adds to the confusion.

- Concerned that we have roughly same set of criteria on three different development tracks – 002-4, 010 and survey – survey may not be in sync with team's work on 002-4?
- The team must provide comment saying this is what we want to include in the survey
- NERC and team are not seen as the same in the industry – industry understands the difference – also, is NERC management going to push back if we change 002-4? That is why it is important to ask industry based on the changes to 002-4
- Still not really getting a bright line
- People appear more concerned about the political perception of "high" than actual number
- We will not have any more assets identified than before?
- Some confusion in industry but to try and resolve the confusion may cause more confusion through industry as a whole.
- Similar concerns are that we are not resolving the correct issue and just stopping to identify assets, not identifying the correct critical assets – the survey doesn't get at the latter.

Focus on Completing CIP 002-4 first.

- Need to focus on getting 002-4 done first
- Depending on when schedule is needed for the 010 and 011 – we need to push that off and focus on getting 002-4 done.
- How much time do we spend on 010 and 011 sub team reports versus focusing on 002-4?
- We have three days, we could get 002-4 done by Friday – just proposing a few days delay on 010 and 011?

SDT to Summarize CIP 010 & 011 Informal Comments and Workshop Input in August.

- We should not suspend 010 work. Indeed the work on 002-4 should inform 010
- We had an informal comment period and teams have addressed those comments for 010 and 011 – we should not stop, but provide comments – have to balance tasks
- Need to get 002-4 out – also need a schedule that reflects reality about getting 010 and 011 out.
- Since there was not unanimity among the SDT about going forward with 002-4. Consider the possibility of splitting our resources to make progress on both tracks –

also allows those who don't support 002-4 approach to distance themselves from that process.

Industry Ability to Respond.

- Will industry be able to provide this information in a such a short interval? The survey was designed to be relatively straightforward to complete with existing CIP data.
- The chair noted that the Team will have to wait and see results before we can evaluate – will do what we can in September and hold additional calls, if needed, to finish work.

NERC Survey vs. SDT Survey.

- This language needs to be clarified that request is from NERC, not from this Team.
- Howard Gugel agreed to take the SDT's suggestion into account in finalizing the survey.
- The team did not ask for the survey, do not present that way – request is from NERC – don't like the politics affecting technical questions, but that is the reality – there is no identified number of critical assets just a politic perception – not thrilled with approach but that is what we have to do to get the job done.
- Seems to be too much red tape here – team had nothing to do with this and should not be presented as requesting the information
- Appears NERC is asking for a lot of data in just two weeks? A: Only asking for comment on the survey in two weeks before getting BOT sign off, then there will be 30 days.
- Even thirty days requires legal and management review – question why we are requesting – remove our name and say NERC wants to know.

The facilitator summarized the conversation noting Team concerns over: the "mandatory" nature of the request, the appearance that the request coming from the team and not NERC; concerns and assurances about how will information be used by NERC; and balancing whether there is any way to accelerate the survey process to have results in time to review in September, yet enough time to respond accurately if "mandatory." The Chair noted that NERC has already posted a survey document for comment and date for responses to the draft survey cannot be changed. Thirty days for industry response seems to be minimum time we can allow for response to the survey. NERC should look to whether it might be possible to shave a week to post survey sooner than the August 6th date. Request NERC look at end of comment period and posting of the survey. Howard Gugel noted that NERC staff need time to analyze and comment on industry comments

and make possible changes to survey and produce a recommendation for review by the Board of Trustees as urgent action on August 5, in only nine days.

After additional facilitated discussion which highlighted that the SDT could use any resulting information to inform and modify their standards drafting going forward, Sharon Edwards made and Jim Brenton seconded the following motion:

- **The SDT requests that NERC modify the survey language and transmittal letter to state that NERC is requesting the survey and correct the reference that states that the CSO706 SDT drafting team requested the survey.**

Having confirmed a quorum, the Team adopted this statement *(18, in favor, 1 opposed)*

Following the motion, Howard Gugel presented draft survey revisions to the SDT to address the concerns. Howard noted that he had replaced "team" with "NERC" – also bolded the language that data not used as basis for determining compliance.

Member Comments

- What does "currently enforceable" mean? Could be used for 002-4? Add the phrase "and any future standards"? By saying one and not the other, it leaves open the question.
- NERC would be using the data cumulatively to determine compliance in the future
- Does the data assists and validate the standards, not compliance? Yes. This is not meant to apply to any individual
- NERC should modify to include that clarification.
- Not used for compliance of individual entity but cumulative for determining compliance standard.
- Worried it flags issues for auditors to look at going forward – "currently" cannot be used here – put in the specific language.
- Regions need to clarify the auditors cannot use the information for future audits
- Roger Lampila noted the information is only going to NERC not the regions. I would hope you would say no if the region came and asked for the info. That list for the survey should have no basis for the audit.
- Clarify that it won't be used for compliance and you will publish a cumulative compilation, not individual data.
- In addition, note that Section 1600 mandatory request provisions do not apply to compliance actions. This should be put that into the statement

On Friday, Howard Gugel asked for SDT feedback on the survey for a concept regarding "at-large" generation facilities. He noted the need to know what attachment will look like for CIP 002-4 since the survey will key off of that. The SDT discussed the need to draw lines for control centers and the characterization of high and medium- "darts", noting that we should try to find points that industry can easily fill out and that also helps the team draw some lines in CIP 002-4. He then asked the SDT to give him feedback on the following:

Concept: Generation Units as CAs that are at-large facilities (i.e. plants whose combined output is greater than the contingency reserve). CCA to be narrowly defined as the shared systems (requires changes to R2)

Discussion of Concept

- Targeting reliability factor
- Do assessment for CA then go back to CCA?
- Looking at aggregate impact
- Before it was the sum of the reserve
- Attempting to use the balloted language
- Generator would know if they exceed the minimum requirement of shared system
- Headed in the right direction – but point out "plant" is ill defined term much like difficulty we have had in defining control center.

Favor concept: support 10; oppose 0; abstain 1

C. Discussion of CIP 002-4 Overall Objectives

The Team reviewed and discussed the draft CIP 002-4 objective statement. Bob Jones reviewed the statement which was drawn from materials provided at the July 2 conference call meeting and suggested taking a few minutes to be sure the SDT agrees on the objective or outcomes we are hoping to produce with the development of CIP 002-4. The strikethrough and underlined reflect the discussion comments below but not effort was made to test for SDT support for the statement.

> ~~"Both NERC and the Standards Committee, with concurrence from major stakeholders and trade associations, believe there is a need for the SDT to develop a CIP 002-4 consistent with its approach to CIP 010 and 011 in order to demonstrate industry responsiveness with very high stakes in play. The SDT's revised work plan and schedule will provide additional time for the SDT to~~

~~produce a quality product for the next formal posting of a very substantial package of CIP-010 and CIP-011 with associated required documents.~~

The SDT ~~agrees to~~ will work to accomplish the following ~~objectives to~~ in developing a CIP-002-4 in 2010:

1. To provide an incremental step forward towards developing a CIP 010, CIP 011,etc. as new CIP standards for industry review and acceptance in 2011.
2. To leverage the work already completed by the SDT for CIP-010 in developing a revised CIP-002-4 version that is narrowly scoped to ~~more fully~~ identify the Critical Assets in the Bulk Electric System through the use of bright line criteria as currently under development in CIP-010 in place of the risk-based methodology in CIP-002-
3. ~~To ensure that we have covered all of the nuclear facilities and 500kV transmission facilities in the CIP-002-4 bright line definitions.~~
4. To meet the goal for a successful industry standards ballot and filing to FERC of the revised CIP-002-4 before the end of 2010."

Member Comments

- Objective 4? All we can do is put proposal out and respond to comments but we cannot be sure it will get to FERC by December
- Objective #1? Agree that we want to be responsive to industry but question what NERC supports and what the team is doing.
- Not sure the opening it is a true statement – portions of the industry not on board
- Seems disjointed as to the trade associations
- Representatives from trade associations on the July 2 call seemed to suggest they support this support. Allen Mosher addressed the team on this.
- The executive committee of the Standards Committee expressed support for this approach.
- Objective 3 – problem with including nuclear facilities and 500Kv facilities as bright line specifically in the criteria. Suggest deleting here and addressing in CIP 002-4 as appropriate. It might be better to address these in next CIP 010 and 011 and not a bright line assessment.
- It is confusing as to who is speaking at different points in this statement – first part seems to be a call to action from NERC and the 2nd sentence a response of team – may need to clarify into the first paragraph as the call and 2nd paragraph as response.
- Suggest deleting the opening paragraph.
- Concerned with the phrasing "more fully" Suggest removing the phrase – identify critical assets using the bright line criteria.

- What is the purpose of this exercise? How will this statement be used? We are off of our focus if we are dealing with critical cyber assets.
- SDT still needs to clarify what are we trying to protect and from whom with the CIP?
- The point is being sure we have a common basis for this effort moving forward.
- If we want the statement to guide us, we would need more team time refining it. We do not need this for the SDT to move forward on 002-4.
- The facilitator clarified that there is no need to refine and test the acceptability of the statement and it will be reflected in the meeting summary as a set of discussion point.

D. Review of CIP-002-4 Strawman

John Lim presented the CIP 002-4 strawman for the SDT's consideration and input. He walked the SDT through the sections of the draft. The CIP 010 sub-team worked on producing this initial draft. They started with CIP 002-3 and did a redline of changes.

1. Purpose and Appliability

- In the purpose statement, it says we are not changing CIP 003-009. Does that require a separate purpose statement for those and would that cause confusion?
- There is intended to be no changes to the CIP 003-009 requirements
- Are we changing the purpose statement for all of the standards
- Are the changes considered local to 002 or across the standards as we always did before?
- The Sub-team is just conforming changes to 003-009, not changes to the requirements.
- Only substantive changes will be in 002 – let others worry about conforming changes.
- We will have to change version numbering for 003-009 to show conforming changes.
- First word of third paragraph – "business"?
- That was already there in the earlier versions

Functions

- Are functions folded into this? If not, do we need to add something to the end of the sentence? How are we attacking the drafting? not a substance question.

- At the last sub-team's meeting they agreed to remove all reference to functions. Not all members were on and some expressed concerns regarding the treatment of functions
- There are also outstanding issues when we get to applicability if we remove nuclear. The current CIP 003-009- 3 says not applicable to nuclear and to include it would be an applicability change, not just a conforming change.
- Can follow a later schedule for the conforming changes?
- Because we include the nuclear industry we may need to put out for 45 day comment period – can be posted as a package
- We will have to have a detailed technical team meeting to review –SE – the purpose statement has changed – need consistency for applicability
- No one is proposing changing the purpose statements for 003-009 – each will stand on their own with version changes only because of applicability to nuclear – also included in R2 examples of control centers – other things we need to capture and add to the sentence.
- These are not examples – industry wants us to tell them what we need to do – allow industry to do risk based assessment but with clear guidelines, tell them what to put into the risk based assessment – industry would accept that as a slight adjustment and clarification.
- First concern is time – can we make December time if we have to revise whole set of 003-009?
- We are trying to keep within scope to get it to the industry and on to FERC by December. We are not trying to include all of the work in CIP 010 in CIP 002-4.
- We are really trying to tweak 002 and not bring all of the work on CIP 010 into the CIP 002-4
- We will have the purpose statement for 002-4 but new language in the purpose statements in CIP 003-009

Applicability- Distribution provider

- The draft suggests adding distribution provider.
- Need to be clear on the reason for adding distribution provider.
- How much heartburn from industry did we get on adding distribution provider? No much attention paid to it.

Bright lines for load shedding.

- Should we be drawing a bright line for the amount of load to be shed? (HG – yes) but make sure the number is clear, that it is the right number and the steps involved
- This only applies to the portion of assets under NERC scope and nothing else. There are other standards that address load shed
- Are we beginning to address issue not addressed before – should be a primary cranking path
- There is not one and is not in the scope of this group
- "initial cranking path" may be the key term – NERC functional model should determine this.

- An example of physical security as an alternative method of protection – here we were trying to address cabling between separate entities – the Progress Energy RFI was addressing a cable that ran outside the physical security but connected the same location
- Involved six wall perimeters –this is an example of a general protection with added layers of security as required
- This could take the scale of assets to be protected from hundreds to thousands
- If only addressing CIP 002-4 here then do not add

Applicability 4.3 exemption from 002-4 and Facilities

- Eliminate exemption statement of 4.3.1?
- Facilities can mean many different things.
- Does the need for exemption goes away under 4.2.1?
- Systems of facilities within?
- "facilities" refers to those with terminals – careful how we use "facilities" – the capitalized glossary term does not mean just a building.
- For example, nuclear considers everything inside the outer fence as part of the facility – this allows them to include those as "facilities."
- Does this clarify what is in NERC's jurisdiction? Does not seem to add anything. Jurisdiction is determined outside the standard.

Straw Poll

In favor removing 4.2?

15 members favor removal of 4.2, 3 opposed. Passes 83%

- Is FERC okay with that? A: not sure what you are doing with 4.3.1
- That stays out as an exception

2. Requirements section

R1

- Creating a new attachment 1? (Yes)
- There is a request for interpretation on this language already *(participant)* – cable between units in the same perimeter?
- Have separate ESP's
- If one ESP then you have to have physical six wall protection? A: yes

R2

- Should examples be in the requirement? John Lim proposes taking them out
- Support taking examples out and place in guidelines
- Agree to remove, as they do not add to the requirement
- Reviewed the alternative – takes current list of functions and include as attachment #2.
- Breaks R2 down into three parts - each piece is different set of assets to be identified
- Are we re-introducing function based assessment? Given short time frame for posting, not sure we can fully develop this.
- "situation awareness" was a big concern in the industry comments – we need to be able to clearly define it.
- We should include and be able to define – "situational awareness" as a component of every outage
- Trying to get industry to think more about computer connected systems – the industry rejected the Maureen edit of "functions", not what we originally wrote – network computing is what this is all about.
- Concerned about the time this will take in completing our task on CIP 002-4
- Don't add attachment #2 to CIP 002-4 – there is not enough time to develop both attachments and address the push back on both.

- We don't define situational awareness from whose point of view –
- Cyber assets with dial up? We may need to clarify intent and modernize if necessary to include any remote access.
- Without examples of functions, I question the effectiveness of R2

Straw Poll

- How many favor Rich's alternative to includes list of functions as attachment – 5 in favor
- How many favor the original R2 with examples? 6 in favor.
- How many favor the original R2 without examples? 12 in Favor.

- How is entity and auditors going to determine what is essential without examples or an attachment?
- That is what they do today
- R1 is the reason we are doing it
- Keep wording like it is today but in the new world for 010 and 011 we need examples
- May need guidance with examples or attachment 2
- Are we giving the industry an opportunity to shoot itself again – leave in a loop hole here then have an empty critical cyber asset list
- Need to make clear the essential cyber system functions, and we need a bright line
- Agree for more clarity on what CCA's are supposed to be but there is a risk that introducing it here is too big an initial step. We are dealing now with 002, then go back to 003-009 – trying to get industry acceptance.
- Ff it is not routable it is not in scope
- We have been asked to do a minimal scope then return to what we were doing with 010 and 011
- R1 is an eighteen page guideline from a different standards process –
- If a guideline exists, then we should use it
- Even if it is just guidance and auditors can not use it or enforce it
- **Motion (Lim/Brenton) to remove examples and keep remaining language R2 in first paragraph – 14 in favor, 4 opposed. Passes (78%)**

- Separate discussion of 2.1, 2.2 ad 2.3:

- R2.2 –need to expand
- That is a good idea but not for this round as it brings in a whole new set of assets.
- FERC had indicated that the SDT will need to justify why you are removing requirements.
- Without this change we will not head off the politics surrounding us
- It is the right thing to do, it is an update.
- It amounts to replacing all three with "if connected by routable protocols" – may turn into critical assets without any outside connectivity
- Industry may have to unplug assets
- Better than letting outside threats bang on it
- The industry needs to be defending at the host level and on interior systems too
- This is the problem with the 002-4 process – we are balancing what can get past industry and what Congress will accept.
- We still have not determined what we can afford to protect or we will have scope creep
- If advanced persistent threat is what we are after and we remove ability to communicate outside, then why cover routable within the same cabinet?
- Miss list of those authorized to access, also miss out on recovery plans, testing, etc. too – those are the things we need to determine the full threat – all these devices need to be included in a minimum protection scheme.
- Dave's proposal goes in the wrong discussion. Doing something fast is important now – we were on the right path and were told to stop and do something quick, then go back to the right path – cannot deviate and make everything right at this point – true we could make it better but have to get this job done first.
- Need a better update on risk assessment – need a clear cut set of risks to address
- Jim (phone) – agree we need to be more encompassing – note many sticks used to attack routable protocols through introducing viruses without being connected.
- Support moving forward quickly in order to get back to the right path
- For each requirement we need to ask what is the right thing to do, not just expand critical assets by the end of the year.
- We should always ask if this is the last time we get to discuss, what should we do because it may get yanked out of our hands – need to educate industry

- Important to do the right thing and need to secure the system – the next version will be more tailored to the equipment we are using – we need this now to allow industry to regulate itself
- If we use what the threats really are, would require massive education of congress, auditors, industry and others – now we are checking boxes for compliance.
- We can get something acceptable to industry short term in order to get time to do the right thing for the industry
- Cannot be yanked away from us without Standards Committee based on motion of author – the SDT should focus on solving the problem and less on Congress
- Need to play game and find medium to get us there – suggest addressing the dial-up language too.
- This will pass industry – EEI CEO's are whipped up and concerned they will lose authority to regulate themselves – this will not be rejected by industry
- If we put in those changes and it will be rejected
- If we make further tweaks here then need to make tweaks in 003-009 – cannot support change here.
- Would it be suicidal for the industry to ask you to stop and change direction then vote it down?
- The fundamental difference here is we are not just addressing critical assets but trying to improve standards as we go. We will continue to butt into this difference in approach
- Limited scope to change – now changing more – where is the line? Need to work on the bright lines.
- We all want a material impact on identifying critical assets – we need real security, not just paper security.
- Already made changes to R2 which is part of 010 – trying to make it better but not addressing everything you already changed.
- We never reached consensus on what our objective was. We did not change R1 but did start to change R2?
- Way too far to go to change everything and file by December – but changes here go to informing people where you are headed – need to include a list of cyber assets that need protection.
- Changes in R2 to remove functionality impacts in the definition of CCA's – may have removed some and weakened it.
- The issue of list not having enough on it – started with Mike Assante's letter – if we do not fix the CCA list then still have empty list?

- Note that "cyber" does not even appear in survey – it only asks about CAs
- Midwest organization ran the survey and had fewer CAs on the list
- Motion to focus discussion – suggest #2 on the purpose statement list captures what we need to do
- Scott Rosenberger's motion (John Lim second):

The SDT objective for CIP 002-4 is to leverage the work already completed by the SDT for CIP 010 in developing a revised CIP 002-4 version that is narrowly scoped to identify the Critical Assets in the Bulk Electric System through the use of bright line criteria as currently under development in CIP 010 ~~in place of the risk based methodology in CIP 002-3~~

Discussion of the Motion

- Clarifying question? Earlier changes discussed would be negated? Yes
- This represents a principle to help us move through and get CIP 002-4 done
- Friendly amendment to shorten and remove reference to CIP 010? No leave as is.
- The less we say the better – say what needs to be said and no more
- This acknowledges leveraging work done to date
- Should we make entities use bright line within their current process? There should be no need to replace current risk based assessment if we provide bright line
- This motion is trying to make sure we fix CA discussion. We can then consider a separate proposal to refine direction
- Suggest adding CCA? No.
- In Dallas one company said approach then cut their legs out from under them
- Scott is comfortable putting in period after CIP 010 and drop last clause:
- Need to make clear they are inclusive, not options
- Need to replace risk based with bright line?
- SR – that is not covered here – did not want to leave in risk based to keep assets from falling of the list.
- Does this rescind earlier discussion on R2, including deleting the examples?
- Does this include "engineering studies"? (No)
- Very concerned that some at entities who tried to do the right thing will now lose their jobs

- CIP 010 and 011 will bring those back in scope when we get done

Motion above: 15 in favor; 3 opposed. Passes (83%)

- R1, R2 and R3 will remain the same

3. Attachment #1

Below is an overview of the straw polls taken on various provisions of the draft Attachment #1 for CIP 002-4. Following are discussions points on the sections.

The SDT reviewed and discussed and polled the proposed revisions to Attachment #1.
The following are the Straw Poll results:

- Support for dropping 1.1: 15 in favor; 3 opposed. (83%)
- Support for Revised 1.2 language (a-d). Support for – Support 0 Oppose 19
- Support proposed changes to 1.3 - 13 oppose 0 support ; abstain 7
- Support section 1.4 as changed: 14 support; 5 oppose (74%)
- Support 1.5 as revised – 18 in favor 0 opposed, 1 abstain (100%)
- Support 1.6 as revised – 19 in favor 0 opposed (100%)
- Support including 1.7: 18 in favor; 0 oppose; 1 abstain. (100%)
- Substitute in 345kV –5 in favor; 14 oppose. (26%)
- Support 1.9 original language with FACTS and IROLs: Support 12; Oppose 0; Abstain 6 (100%)
- Delete the second sentence in 1.9 –14 in favor: 0 oppose: abstain 3 (100%)
- Proposal to use “control center” – Support 17, Oppose 2. (89%)
- Proposed language without limits for 1.14-1.16: 10 in support; Opposed 10 (50%)
- Support for: “Any control center or systems that are or could be used by a NERC registered RC or its delegate to perform RC functions. Support 13; Oppose 1; Abstain 8 (93%)
- Support for: “Any control center or systems and backup control center or systems performing RC functions.” 17 in support; 0 Opposed Abstain: 1 (100%)

- Support for Approach: Appropriate to incorporate bright line criteria from attachment 1 into the risk based methodology. Support 8 Oppose 12 (40%)
- Support for Thresholds on 1.18- 9 in Favor; 8 Oppose ; 1 Abstain (53%)
- Support for Thresholds on 1.19 10 in Favor; 8 Oppose ; 1 Abstain (56%)
- Support for Thresholds on 1.20. -12 in Favor; 6 Oppose; 1 Abstain (67%)
- Support for taking out distribution provider in 1.15: Support 14; Oppose 1; Abstain 1 (93%)
- Support for Wording in 1.14 and 1.15 from 002-3 R1.25 – "System and facilities critical to automatic load shedding under a common control system capable of shedding 300 MW or more." Support 14; oppose 0 (100%)

"Nuclear generation facilities"

- It should not matter how we boil water – the fuel source has no impact on reliability – addressed that nuclear facilities have to comply by removing them as an exception – should not say all nuclear facilities, regardless of size, are included
- Nuclear units take twenty-four hours to come back on line – no need to call them out just because they are nuclear.
- Some fossil fuel plants can take up to eight hours to come back on – NRC controls safety aspect of nuclear fuel
- Agree with comments – There is no engineering basis to call out nuclear separately as to reliability – Might include them in 1.2 criteria in some manner.
- We should be forward looking to changes in nuclear and new technologies.
- No technical justification for including nuclear separately – it is all electricity regardless of how it is produced – this is politically driven.
- Some agreement with NRC to include nuclear as critical assets – do nuclear facilities already have standards for their facilities?
- Nuclear safety is covered by NRC – more risk to the plant by the system than to the system by nuclear plants.
- Thought we were handling by saying "a generating unit, including a nuclear generation, …" in 1.2
- This is not in to address any agreement with NRC, rather it is in for political optics – even including in 1.2 appears to give an out for including a nuclear plant as not critical
- We did not make any distinction for any other fuels through the whole standard – from reliability stand point it does not matter – putting into 1.2 says we are listening but not actually recognizing any difference in reliability – that is the purpose of the standards

- Agree with comments – does not matter what fuel is used – may explain optics by changes in the applicability section, but if in the attachment, better in 1.2.
- Prefer putting in the applicability section but may not be obvious enough
- Nuclear is beginning to require cyber security measures in their licensing process – they have a defense in depth methodology in place – may miss on the optic side if only four out of over 100 units are identified as CAs
- Lots of talk about optics – NERC communications director can communicate – let industry know the justification – no technical basis, only political optics – NERC needs to do a better job handling the optics
- 1.11 addresses interface with nuclear that is reliability based.
- The threshold of 2000 for high will not capture most nuclear units that operate in pairs to create 1800.
- Consider naming them in 1.1 subject to criteria listed below.
- Agree to remove 1.1? If so, do we need additional criteria for nuclear?
- Motion to drop 1.1, with removal of exception for nuclear
- If the SDT removes 1.1 we will get comments back on the record from NERC to put it back in
- **Support for dropping 1.1: 15 in favor; 3 opposed. (83%)**

1.2

- Confused – "a group of units" relies on common control system – language is confusing, the concept is right
- Is it the lowest of the three or the highest of the three? Should be the lowest
- There is a contingency reserve or a shared contingency reserve – same thing – matter of total reserve.
- If 2000 mw or lowest value – then drop c.
- A and B are the same thing – combine with an "or"
- 1.2 needs to be more succinct and plain language – also is 2000 MW enough?
- Not the most productive to wordsmith as a group – Jason Marshall offered the Chair agreed to let him take a shot at redrafting and bring back tomorrow for review
- Intent is to capture the cyber systems that are part of the aggregate
- Is 2000 mw the right value?
- There is a logic issue between a, b and c.

- Support creating a proposal – do not forget we may need criteria for covering nuclear
- Needs to be based on reliability
- You have to have contingency reserve in nuclear
- Mike – no single units of nuclear exceed 2000 mw – and no mediums identified here
- Still looking at common or aggregating control systems
- Talking about big iron, share concern about 2000mw
- Those units do not share common control systems – might need to discuss aggregate bus as was described
- What are we protecting against – do not care why I lose unit, just about getting the supply back on line
- Generators themselves may not have common control – but other GCS systems may be in common .
- Comment may be covered by 1.17 which addresses generation control, not generator control
- Generation control is not within the generator control room
- We should be careful we invest in the units that we need to.

At the request of the Chair, Jason Marshall brought back some revised 1.2 language for the SDT's consideration which includes four options a-d

1.1. A generating unit, or a group of generating units that share or are reliant (dependent) upon a common cyber asset (e.g., control system) that has/have an aggregate highest rated net Real Power capability exceeding:

a. the Contingency Reserve of the associated Balancing Authority, or
b. the Contingency Reserve for the Reserve Sharing Group,
c. the associated Balancing Authority's obligation or share of the Reserve Sharing Group's Contingency Reserve or
d. 2000 MW.

Member and Participant Comments

- The 12 months was in there to cover seasonal ratings to keep units form going on and off the list.
- Makes sense at first blush but once on the list you will apply cyber security controls.
- It would allow gaming and the 12 months would limit potential gaming
- Can add it back; just trying to make it simpler

- 12 months limits fluctuation of value – need to set a definite value
- If move things in and out may only be in the interpretation phase and never get to implementation
- I think it adds confusion between 12-month sliding period within the three years
- The preceding 12 months sets the time period
- But compliance period is over three years – this is overly complicated, if any time in the three years then it must comply
- Look at R1 and R2 – words say on that day of annual review
- Sets an anchor – propose keeping the 12 month language to anchor the value
- All assets get roped in as critical assets even those not interconnected
- Suggest putting "that would have an impact on the reliable operation of the group o units within 15 minutes"
- How do we audit time compliance? How do we provide evidence to auditor?
- We can take an asset down and document that event
- Cannot provide evidence you can audit to it
- We are both a balancing authority and in a shared group – looking at "b" we could hit that – "c" is a different value for the same entity, how do I pick the appropriate one
- Says "or" – can choose the lower one
- Does that mean everything over my minimum obligation in "c" must be covered as a high?
- If balancing authority loses your share does that put the system in danger?
- I cannot defend that we have to cover everything over our minimum share if we also have the ability to cover the full reserve on our own
- Concerned about the addition of "c". How does c relate to a? Also concerned that our share under c is but a sliver of the pie. Compliance impacts that could come back and bite us
- Instances of "a" few and far between – "b" more likely – "c" may be lower as your portion of the shared group's reserve
- Still concerned about adding "c"
- Also concerned about "c" expanding obligation beyond obligation under "b'
- Concerned this addresses the reliability of individual entities rather than the bulk electric system – disproportion impact on PA's?
- Concerned about the actual grammar used – the "(e.g. control system)", and also the 15 minutes as equal to "real time"

- Jackie Collett noted she was willing to volunteer to rework the language
- This is confusing as to which direction it is going – for our organization it would bring in about 75% or more of our assets
- Propose b and c are exclusive of each other – either use full groups number or your portion – go with either b or c – your share under c is always lower – suggest dropping "c"
- We would have to go to "d" – for us "c" would be arbitrary

Support for including "c" – No Members

No changes to 1.3 and 1.4

1.5

- Added "primary" to 1.5 – though there is no definition for "primary"
- Last call we discussed the term "primary" and suggested using the term "designated" instead – neither word is officially defined – what wording should we use?
- Blackstart is not about reliability but recovery
- Instead of "primary" –since there are different stages of restoration, focus on initial stage of restoration as the critical moment
- Primary and designated are not the same thing
- Need to be sure designation plans are the right source – hundreds of units included in our area to cover multiple contingencies
- R1.3 – coordination between individual transmission operator restoration plans
- But R1.5 has the assets
- We have to be careful to avoid unintended consequences
- Question about contingency requirement and not meet a or b? Ever not meet contingency reserve in a or b and have to fall under d
- Concern about 12 months – consider prior calendar year rather then preceding 12 months? Variability in what this captures by entity – how do we know what it captures; does it capture the appropriate assets? This is too obscure for oversight as an entity by entity threshold.
- There are three or four ways to say the same thing – needs to be one number to meet whether as a single unit or in combination – propose one value for 12 months – conversation should be on the right number, not how you get there.

- Comfortable with removing “b”
- If we remove “b” we need “d”
- Concerned about removing “b” – confusing if we are left only with “a” – who is the associated balancing authority?
- Agree cyber system needs to be protected but do we mean that the small pieces that add up to the whole are each in themselves critical? The generators themselves are not critical.
- Nuclear – it is the control system we are trying to protect.
- May not be the right approach for the generating units.
- Trying not to lose control system by looking at individual units.
- This says the individual units are critical if they aggregate up to a critical level.
- Have to take the units as a group and look at the system critical for running that group – not the individual units.
- Does the wording here say that? May inadvertently be focusing on the individual units rather than the control system of the group.
- Bringing in every system for each unit which may not be critical.
- May need to look back at possible link to R2 as well.
- Remove the part discussing the combination of units, go down to 1.17 and add any system controlling the aggregate of units – possibly added as 1.18?
- This list is trying to identify which generators are critical to maintaining the reliability of the grid –
- Delete “a generating unit for” to be sure not looking at individual units and focusing on group. Also make the subject “common cyber asset” though that may not help with political optics of identifying more assets as critical.
- Phone? – adding language in “a’ drops the threshold to a low number bringing too many units into play?
- Goal is to protect the common asset – strike first sentence up to “upon.”
- Can you have a reserve less than the unit?
- Think about what we want for the outcome – do you want the group rather than individual units – focus needs to be on protecting cyber systems not the generation units.
- Talking about the bulk electric system reliability and the cyber systems that are connected to them.

1.3

Member and Participant Comments

- Why 1,000? What is the rationale?
- Best number we could agree on using our professional experience, expertise and judgment.
- 1,000 seems arbitrary – need to reword to tie to RC and not tie to a number – add "any reactive resource listed with in a mitigation plan approved by the reliability coordinator."
- The RC does not decide what equipment should be installed – also need to substitute NERC glossary term for the mitigation plan – need to be an operating procedure and process rather than mitigation plan.
- How hard or would it be possible to write up the reasoning behind the number? Bright lines are arbitrary with some rationale behind them – is this a work product for later?
- Documenting the rationale helps flesh out the petition to oversight authority.
- Trying to understand the impact of the proposed language – how much stuff would be coming in?
- Will it be clear which operating procedures will apply? Which ones belong to the RC's? Test new 1.3 language?
- Provides more of a rationale than the arbitrary number.
- Like to add "required" operating procedures.
- Are plans "approved" by the RC – change "approved" to "required."
- How does the owner find out what is in the RC operating procedure?
- RC has to communicate those procedures.
- Concerned about how logistics would work – bright line was easier to determine what this applies to.
- Add "Operating Procedure, Operating Plan and Operating Process"
- Will have many requesting plans that may not be related to this issue.

Straw Poll

- **Favor changes to 1.3 - 13 oppose 0 support ; abstain 7**

1.4

Member and Participant Comments

- Concerned about impact – not understanding or it is not worded correctly – looks like everything would be medium – also "Wide Area"
- "Must run" is a market concept and should be deleted
- As used here reliability is not a glossary term – reliability "must run" is distinguished from market concept – put back in in response to comments, need to clarify it is there for reliability purposes – need to keep track of the rationale
- Will Maureen let us get away with the quotes?
- Longer than the implementation schedule?
- May be there until a transmission or generation unit can be built
- Appropriate to say "pre-designated by the reliability coordinator as …"
- Still concerned about using "Wide Area"
- It is not always the planning coordinator – pre-designated covers both if not as clear as adding reliability coordinator
- Planning coordinator is responsible for coordinating with the asset manager – replace reliability coordinator with the planning coordinator
- What does pre-designate mean? Strike in favor of "identified by the Planning Coordinator."
- Can we eliminate "Wide Area reliability impacts"?
- Keep developing in passive voice – planning coordinator identifies as…

Straw Poll

- **In favor of section as changed: 14 support; 5 oppose (74% Passes)**

1.5

Member and Participant Comments

- Delete "primary"
- Could be unintended consequence of reducing the blackstart units covered
- Agree – another suggestion – no basis for primary, and language is redundant –
- Alternative – Blackstart Resource and the Facilities comprising Cranking Paths contained in the transmission Operator's restoration plan
- Can also use tie line to restore – not covered here
- Cranking paths include tie lines?
- Facilities as capitalized is defined – do we need a more specific level?

- The language here covers each of the issues discussed
- I read it differently because of the "and" means 1.5 does not apply at all – suggest two items
- Blackstart resources is well defined – let stand alone
- Any Blackstart Resources contained in the Transmission Operator's restoration plan.
- The Facilities comprising Cranking Paths contained in the Transmission Operator's restoration plan

Straw Poll

- **Support 1.5 as revised – 18 in favor 0 opposed, 1 abstain**
- **Support 1.6 as revised – 19 in favor 0 opposed**

1.7 – New

Member and Participant Comments

- Optics type criteria added
- No problem with the requirement but question the optics –
- Regional issue to define
- How do we handle the fact that NYC is not covered – bad optics
- Need to have a technical reason – if just adding for optics, we will get called on it
- Not every criteria has a technical reason or justification
- Many industry comments asked for technical reliability based reason for various criteria – need to be able to say why this was put here beyond perception
- Rationale: to protect the back bone of the system
- Do we have anything in writing to put this in here? If we pull it out, will we get a response or directive to put it in with a rationale?
- In CIP 010 we said had to have "four lines" – how do we do that later with 010 if we put this in here?
- With some research could create some rationale – critical to us in Florida – need something to support putting it in
- Team did not include this, but NERC staff did in response to informal directive – I do not have an issue with including it – clearly critical at this level
- This may be arbitrary but it does not hurt us and should be included, just with some justification beyond political optics

- Support including, goes with 1.8 – if you take 1.7 out then would need major rewrite of 1.8
- Including is a good idea – engineering analysis may not justify but collective experience of this group does
- No problem with 500kV, but need more than political optics to hang our hat on

Straw Poll

- **Support including 1.7: 18 in favor; 0 oppose; 1 abstain.**
- **Substitute in 345kV –5 in favor; 14 oppose.**

1.3 and 1.4

- 1.3 – "reliability coordinator" – RC does not require anything, not part of his job, just enacts guidelines passed to him – and, "mitigation plan" is a compliance term
- We know how to operate the system but may not have the language to properly explain it – "require" may not be the right word
- Majority of plans are for coordination – if trying to identify assets, then need to look at other documents, not to the RC
- Look to responsible entity's
- Look to the definition of "operating procedure"
- Put in "owned by a registered entity" and "submitted to a reliability coordinator"
- Doesn't add anything
- Some RC have copies just in case not because it is critical – "invoked by the RC"?
- Way it reads now it includes any reactive resource
- Only those submitted to RC to address and issue
- Will take back to his RC

1.8

Member and Participant Comments

- Syncer phaser requirement?
- Many – nothing to do with it
- Texas interconnection but run by ERCOT
- Needs to say "Texas Inter-connection"
- Same for Eastern Interconnection and Western Interconnection

1.9

Member and Participant Comments

- Strike FACTS
- But that is how you define an acronym in a document by spelling it out followed by parenthetical
- FACTS is well defined – question removing it – serve a real purpose where they are located
- Make it a line item for just FACTS
- Used to have a separate item for FACTS and IROLS
- Do we need to delineate into separate items
- Not sure if we need to delineate, but recognize to avoid unnecessary comments
- Reason for choosing IROLs instead of SOLs
- Is there a critical link between FACTS and IROLs? If not, then separate

1.9 original language with FACTS and IROLs: Support 12; Oppose 0; Abstain 6

Member and Participant Comments

- Why include Cascading – seems like the line is not bright here
- Because of the definition and inclusion of IROLs here
- Define FACTS
- We define only if it is different from commonly accepted definition or need for clarification in the industry
- Do not capitalize items unless they are part of the glossary
- Agree this looks sort of like a study – not many studies look at misuse of devices – support including FACTS devices but consider as a separate item
- By tying to IROLs it raise key devices without putting in more than needed if FACTS devices are separate out as a stand alone item
- We can simplify this and clarify coverage
- We could drop the whole second half of the sentence
- Need some delineation because not all of the FACTs devices are critical – they are local area things, not critical to BES reliability
- Add “outages” after Cascading
- Not needed

- Transmission Facilities, including Flexible AC Transmission Systems (FACTS), that , if destroyed, degraded, misused or otherwise rendered unavailable, would violate one or more Interconnection Reliability Operating limits (IROLs) – simply drops the second sentence
- But some areas do not have IROLs
- Recommend keeping the second sentence in
- Same concern – keep it in
- Need to change the second sentence if it remains
- Not available or not identified?
- Do both sentences say the same thing – does anything fall out if we drop the second sentence?

Straw Poll

Delete the second sentence –14 in favor: 0 oppose: abstain 3

- May be a compliance issue in areas without IROLs.
- Have to have studies to show they do not have cascading problem.
- For compliance, you need the second sentence.
- End of first sentence add comma and "would result in instability, uncontrolled separation or Cascading."
- Looking at different definitions and comparing the language.

1.10

- This is similar to 1.2 which we changed and are still revising
- Do we need to wait and see what we get there?
- Jackie Collett will edit 1.10 to include or conform to changes in 1.2
- Bus tie breaker? Do we need to include the breakers?
- But it is the transmission facility
- If interconnection occurs at the breakers, then include – it is for the utility to decide where the connection is.
- Suggest we capitalize Facilities and add "and Elements" which by definition includes breakers
- Do we need to add "Elements" to other areas we have "Facilities"?
- Facilities is a collection of Elements – add here but not above in 1.2
- Do we need "Transmission" at the start of the sentence

- Looking at transmission substations – just say “Facilities”
- A collector bus is a “Facility”
- Call out generation too – begin sentence with “Transmission Facilities and generation Facilities”
- Identified in the generation interconnection agreement

1.11

Member and Participant Comments

- Does it need to be called out? Can we reference another standard in the standard?
- Best not to reference another standard, put period after “Requirements” since NPIR is a defined term.
- Consider moving this up to the other nuclear item
- The other item was deleted and also we were trying to keep generation items together.

1.12

Member and Participant Comments

- Does local area create problems?
- Put language in due to the lack of a clear definition
- But what does it mean?
- Don’t think NERC definition will help
- We had a great deal of discussion before landing on the existing language as a compromise
- What about using RROs?
- Not everyone has an RRO
- Concept of local area is important to capture

1.13

Member and Participant Comments

- Does this change the meaning under CIP 2-3? Does it bring in the smart grid? What is the source of the 300 MW bright line?
- Bright line written for 010 – may need to rewrite here – as for smart grid, intent was to capture it going forward as it involves dropping a block of load to protect the reliability of the BES – we say automatic aggregate load shedding but not how or why

- 300 MW came from DOE 417 – also, what ever system can initiate the dump is critical, not the individual units that shed the load (unless it can unload 300 MW by itself)
- Grammatically say automatic load shedding in the aggregate?
- Will review language
- Would collection of small loads constitute high impact?
- Need to determine if system controls 300 MW
- Do we need to also cover a BES element that could draw 300 MW?
- Any BES element that can result in over 300 MW loss is covered
- Any control center that is capable of controlling more than 300 MW of load?
- Control system, yes – not just control center which also would be covered
- Operator versus automatic – the former is not covered, only the latter

1.14-1.17 were combined and have now been separated out

Member and Participant Comments

- The way this reads and auditor could read everything inside your fence is critical asset
- Need to change the word center to system
- For RC need to say situational awareness
- We have not adequately defined situational awareness
- As it stands you will greatly increase the devices covered –
- Term control center is vague – guidelines help but are not applicable here
- Primary system or backup system
- We are still in the old original paradigm – we are protecting the cyber asset – what is essential to the control center to ensure reliability of the BES? It is the control system – the issue is resolved in the next version of 011
- Have to include 1.14-1.17 to be sure central control centers are included
- Concerned we have added many assets we do not need to
- Leave as is, most will understand what is included in the control center
- Backup center in large building but sequestered – this is not a problem
- Assuming the next set, 010 and 011, will follow soon after this version but understand this version may be in place for awhile

- We are describing things by physicality rather than function here
- FERC needs to understand entities expense in time and resources to meet current standards, this new interim one and then subsequent 010 and 011
- Where does the control center begin? It is not the building or outer fence – need to identify where the BES assets that control the system are located
- Control center is a different issue for critical asset while control system is critical cyber system – each entity must determine where the control center is
- If you can define your control center – we had to use systems to define criticality because we could not define by physicality – not acceptable to determine how we have to define our control center
- The building is not the critical asset
- For CCA's in subcabinets – how controlling the cabinets
- Have a physical perimeter around cabinets
- Proposal to change center to system? I have not heard any concerns
- Many expressed concerns about changing
- We have many control systems – they do not perform the function of the control center – control systems do not capture the intent of this section
- Identifying critical assets not critical cyber assets
- Proposal to change from one undefined term to another undefined term
- Critical assets is a defined term – includes systems

Proposal to use "control center" – Support 17, Oppose 2. (89%)

Comments after Straw Poll

- Concerned about stripping out base for control centers – if remove BAs then no impact
- But need to account for misuse, malicious or not
- We need a bar, a bright line
- We stripped out those limits, bars, etc. – need some limit on identifying "critical"
- "Performing"? Are they registered? Or responsible entity?
- The language here brings in too many small entities and may exclude large entities controlling several small
- If you want a bar, you need to state what that bar should be
- Go back to high language we had before

- Remember 911 attack came through Bal Harbor to get to Boston
- If we keep this language then we keep in medium when we move back to 010.
- The control system is the key asset we are protecting – sophisticated level of attacks means we need to do more and have more robust protection even at small or remote sites – need to add "registered" in front of each entity identified in each of these – need to be sure people performing the high risk functions are asked to do more
- Jay – recognize were we are in the time line – we have to do a little optical maintenance at this stage
- In 011 we should force protection for all iccp's across the board
- Now telling those who used systems go back to big iron approach only to be told to go back to systems approach with 011
- Suggest striking 15-17 here and address using systems in 011
- Need to accelerate protections while meeting political expedience – get people moving in the right direction with the first step
- Control centers are covered in 1.2.1 – cannot take it out at this point
- FERC position – if new version removes requirements then it needs strong justification
- Current 010 identified high, medium – if make everything high, then cannot go back
- Size with control systems does not matter – only matters for big iron
- Propose adding back in language for 1.15 and 1.16 – to preserve option for high and medium in the next phase developing 010 and 011
- Not okay to use system to scope down but can for size of asset?
- If include language used in Dallas workshop, we need to include justification for the commission
- Talking about critical infrastructure – this is not a new thing
- Is there any tweaks from the workshop or comments we need for preserving the high and medium as we move to 010
- Still need to document justification
- When we did 010 we separated high and medium, in 011 we moved much of medium up to high
- When we get to 011 we will add more to high than are currently in 003-009
- Should we have a level? If so, maybe we need to determine the bar or line for each level

- What would we not do for medium level control center that we do not already do for a high control center
- FERC has said cost is not a justification for not doing it – propose we test language as offered here without going back to previous language

Straw Poll- Language as offered without limits for 1.14-1.16: 10 in support; Opposed 10

- Proposal to start fresh tomorrow?
- Concerned about having to cover as critical units that are not connected to outside units that collectively have less than 200 mw impact should be classified as critical and require high levels of protection
- Small cities with limited connection do not have a high impact on the BES
- Are they a BA or a generation control center?
- Can we ask John Lim if there were any additional edits to incorporate to limits from comments at the workshop or responses to industry comments
- Legal also concerned about the language in the survey – agree with the changes proposed by the team but make the change for the posting of the survey and the cover letter
- Does the team have to make a formal comment to make the changes happen
- Comment on the survey is open but not the data collection – board will approve the survey and will have the final version of 002-4 to base the survey language on – better to let staff make changes to survey language without the formal comment

Control Centers

- Should we look at Jackie's updates first
- Joe has the changes to present
- This is a criteria for figuring out what is needed for reliability of the BES not cyber security – then figure out what cyber security system is attached
- Then we should change the title to "Big Iron with computers attached to it"
- Reviewed suggested revisions – also change cyber system to critical asset – highlighted changes with blue – Word changed the numbers.
- Last time we posted it had the clarifiers on the thresholds, what comments did we get back?

- In 1.18 at the end is an “and” that needs to be an “or”

New 1.17

Member and Participant Comments

- What are we trying to solve, what does this do for us – we would fall out as a balancing authority – this would drop us out for a short time until we revise 011 – may not be as a big a deal not to have the qualifying criteria as we discussed yesterday.
- We have small systems that does not impact anything – not all control centers are the same – this becomes the high going forward and will remain so in the next version – many other small entities will have the same problem.
- Stay focused on what we are doing in 002-4 – not necessarily the case we will be stuck with the change – we may need to scope the controls at the component level instead – focus on this for now and not try to predict the future by looking into the crystal ball
- Are we implying there are other control centers not included? Even if a control center currently is or could be used to control the system it should be covered.
- Agree with RC – not putting any limits in 1.17.
- Current language in 003 causes problems – title of this is critical cyber assets – it is not about control centers.
- Backup control centers are not captured here.
- What about backup control centers – backup has baggage to it.
- Change to any control center that is or could perform RC functions – capability to perform.
- How big an issue is it for entities to identify primary and backup control centers
- Backup center is passive, it does not control anything, but watches – we declared control systems as critical assets used to run the iron.
- Multitude of control centers that do not run reliability of the system
- But should be if it performs any reliability coordinator function
- What does RC actually do – only 17 in the country – seems obvious that what they do is essential.
- We have no skin in the RC game – makes sense if registered as a RC or through delegation – Entergy used to be an RC but not now. Should they be covered?
- Any of the members could be an RC – should remove ‘with capability’ and change to ‘which.’

- Capability could be an avenue to attack whether you are actively using the capability currently or not.
- Concerned that we do need "capability" – narrow down from capability but need more than just active current ability.
- Most RC's have smaller staffs.
- But RCs are powerful in that they give directives to others – consider "host RC. functions" – trying to get at those who can give directives – or "designated" – also, can we get away from concept of it being a place or room by saying "equipment"?
- Concerned about removing "centers" – may be able to add "systems" but cannot remove "centers"
- What about systems that support the control centers such as fire suppression systems – are we trying to include them.
- "Any control center and its systems that are designated to perform the RC functions"
- Many have capability – trying to capture those who are doing it or have backup to do it – designated covers that with too broad "capability"
- "Designated" better but still not sure right word – not sure we "designate" a system, but do use them for that function
- Who and how RC functions are done varies between regions – designated may be vague in our area – prefer "capability" as capturing the essential functions.
- Functional model is not clear in the overlay of the system – say the "computers used"
- "That are used by a registered RC or its delegate to perform Reliability Coordinator functions.
- Control center or its system – you get the choice to choose which one, not required to do both
- "Or"? Systems needed to perform RC functions include the air conditioning system?
- Not a reliability function.
- Scoped out when looking at critical cyber assets.
- "used by…" is inclusive but could be simplified to say "used to perform."
- SM – need the additional language to capture everyone
- JM – instead of registered should it say NERC registered – who registers RCs? Say a "NERC registered entity"
- Suggest we use "used to perform"

Poll language: Any control center or systems that are or could be used by a NERC registered RC or its delegate to perform RC functions

Straw Poll

Support 13; Oppose 1; Abstain 8

Comments on the Poll

- Concerned about "could be used" – sounds too vague
- reliability coordination is not a glossary term, change to Reliability Coordinator functions
- "or could be used" is not needed.
- Every entity needs a plan.
- Do we need to add RC emergency plan.
- "Could be used" opens it up too much
- How about adding "including backup control…"
- Raises concerns
- Include "emergency plan" instead of "could be used"
- "identified in the emergency plan"
- "reliability coordinator plan"
- That is a different plan
- "that are identified in an emergency plan"
- Need to simplify to used by
- Need to captured what they plan to use – protect the stuff they need to use in an emergency
- "Or systems that are or could be used by a NERC registered RC or its delegate to perform RC functions, as identified in their operational or emergency plan"
- Why include "or could be used."
- Not required otherwise to include them.
- This is still about RC functions – drop the "operational or emergency plans" – adding words that will confuse
- Agree may limit confusion
- Test again without last phrase: or systems that are or could be used by a NERC registered RC or its delegate to perform RC functions?
- We figured out that once system comes on it must be compliant

- Requirement for RC to have emergency or backup is already covered elsewhere – "that are used by."
- Any control center or backup control center that performs a RC function – that is simpler and clearer.
- Have to add "or control systems"
- Control systems do not perform functions

Any control center or systems and backup control center or systems performing RC functions

17 in support 0 Opposed Abstain: 1

1.18 as rewritten with the language above

- If we use this criteria we are dropping out up to 25% of critical assets related to BAs and that makes for bad optics – many munis who are doing the right thing would not be covered
- NERC registry has 139 BAs including Homestead, New Smyrna Beach, Reedy Creek and several other little cities around the country – do we intend to include them as critical – supports having criteria, but are these the right ones
- Thresholds are okay, but we need to discuss the thresholds and not just the words that go in here
- Some drop off, but are some others added in? This keeps anyone form simply saying they are too small and do not need to respond
- Existing standards allow someone to put more on that they think is important than is required
- No one would do that – they would not accept the risk – also related to the BA function, think we should not have any qualifications
- This is why in the original effort we allowed to identify as important but at a lower level – should we have limiting factors, if so, then decide where the bar should be
- Whatever limits you set needs support of justification.
- Put in bright lines and we may take many out – we should wait and put bright lines in the next version
- Current system lists a lot more entities than BA, RC, and TO
- We are changing from a risk based system to setting bright lines
- But many more entities currently have to determine whether they are in – IA, Transmission Providers, others, fall off the list – need some justification for the change

- Difference here we are talking about functions not entities
- With limited scope we are trying to set maybe the bright line is not the way to go
- Justification is short hand for explaining why this is better, especially if the appearance is to drop assets off – simply a rational for the change
- Drop all of these and simply say any control center or backup or systems used to perform reliability functions
- We have never done a sufficiency analysis on any of these items – protecting bulk power rather than protecting the grid – need sufficiency analysis on any bright lines
- I would vote against the limiters in the proposed language – not in favor of removing mandatory control only because entity is small –
- FERC is looking to industry expertise to set rational levels and the reason for them
- Working under order to have more CCAs and CAs – wait for 010 and 011 to help reset levels
- Goals to have more CAs, though more CCAs may have been implied – need to see survey results to know if 002-4 gets there
- Who has cyber asset that if compromised would have the highest impact on the reliability of the BES – those are who we need to target and set criteria to include
- With limits we were trying to match the bright lines set above to identify CA – control two or more of the critical assets identified above
- This is not about size but attack vectors – doesn't matter how big they are
- CIP has always been backwards – working from figuring out what is in or out then setting criteria – here we are trying to work backward from 010 and 011 – need to determine the risk first
- Would it be possible to still include risk based and add bright lines to augment the list of those already covered under risk based
- This is set up as CA but trying to get to critical cyber assets – small control center that is not connected, then out, but if interconnected then does not matter how big you are – may want to put in additional language to cover
- Test simple concept: check on whether limitations should be included, if so, then discuss what the limitations should be
- Are we going to look at telling entities they conduct risk based assessment with the limitations as a minimum
- Modifying the current risk based assessment with these minimums – have to include these at a minimum

- The charge was to replace the risk based criteria with bright line – that is a deviation from the request that would need to be justified – request came from the call with Mosher and Adamsky.
- There is nothing in writing – we are working off the agreement we voted on in the July 2 call
- Perception of NERC executives direction was to replace with bright lines
- Long discussion on these sub requirements – ultimate goal of this group is a standard that adds critical assets to the list, if we don't, it will not be accepted – focus on adding more assets.
- My company was okay with keeping risk based and adding bright lines
- Given direction but were not told alternatives for achieving the outcome should not be considered – this meets the same goal in a way acceptable to the industry
- This method would increase the number of assets which is the goal.
- The associations asked for bright line criteria – we have brighter but still fuzzy lines – careful we do not end up decreasing the number of critical assets – our job is to accomplish the intent to increase the number
- The request may not have considered that some might use the new criteria to reduce the number of critical assets identified – the option here is a good compromise to accomplish the intent of the request
- Using bright line does not make sense – either have to use a methodology or a set of bright line criteria – one or the other, not both
- Data survey request structured to help us make this decision later – it will give us the data to determine which method ends up with which assets
- We were asked to create bright lines, let's finish it – the methodology will require months to prepare
- Not sure survey will clearly establish which assets are identified by bright line versus the methodology
- We can take a high cut at it, without identifying individual entities, by looking at the gross numbers
- Suggest taking R1 from 002-3 and adding "and at a minimum contains the bright line criteria contained in Attachment 1."
- Considers and includes other things – "and as a minimum…."
- Concerned about how this is applied in the real world
- The "bright line" is just additional criteria for you to apply in addition to their existing evaluation methodology – a methodology + process

- Most entities may rewrite their methodology to include the bright lines –
- The difference is that it gets additional message that criteria they were using in the methodology was not tight enough
- Concerned about mixing methods – telling them this is the answer we want you to get whatever methodology is that you use – you may go down if the bright line is in the wrong place – will we get enough granular data to know if number is going down
- "and as a minimum applies (or satisfies) the criteria."
- This does not work for me.
- You have criteria as minimum to include in risk based methodology.
- Keep R1 the same and add bright line augmentation in R2.
- Concerned we will confuse entities – asking them the keep existing methodology and add minimum criteria – if asking them to keep what they have then ask them to use the same criteria without adjusting the methodology
- In NIST had language to use risk based criteria and basic criteria – treat the latter as the only thing they can concretely identify
- We are working on 002-4 because the risk based methodology is not handle properly or has been insufficient at identifying critical assets – we are not fixing the problem but only putting on a patch
- Auditors only identify you have a methodology not its sufficiency – this would allow them to do so
- List bright line criteria in R2 and put the proposed language in as R3
- Presumption that methodology doesn't change from year to year – add "any previously identified assets" to keep entities from changing their methodology
- This is important tool but don't even know if we need to do this until we get the data – focus on getting the right data first
- Risk based methodology is not frozen as risk shifts.
- R1 stays the same
- R1.1 stays the same
- R1.2 Or, create a new sub-requirement in parallel here to speak to attachment as minimum that must be captured by entities risk based system.
- R1.3 The risk based assessment shall consider the following assets: (with list)

Approach statement – appropriate to incorporate bright line criteria from attachment 1 into the risk based methodology

- **Support 8 Oppose 12**

- Important to understand why people opposed
- Need to spend time more constructively
- We either have limitation language or not for all of them
- But we have not even looked at 1.20 yet
- Take them one at a time
- Check on whether limitations language should be included (if so, then discuss what the limitations should be)
- **On 1.18- Support 9; Oppose 8; Abstain 1**
- **On 1.19- Support 10; Oppose 8; Abstain 1**
- Willing to accept limitations if entities could continue to use risk based methodology
- Instead of methodology – another line item saying "any other assets essential to reliability…"
- We want a process that includes CA identified today, anything else you want to add and the minimums of the bright lines – we need ideas to accomplish the goal
- Request poll on twenty (1.20) too?
- Abstained – recognize need levels in identifying CA – trying to narrowly scope and fix in the next version – can we come up with good thresholds at this point in time – reluctantly willing to stick closer to what is in the existing standard
- That may be where we end up but need limits in the survey to give us information what falls above or below
- Political optics of rising and falling numbers
- The Vice-Chair proposed a team of John Van Boxtel, Doug Johnson, Scott Rosenberger, Jim Brenton and Jackie Collett to review and prepare an alternative proposal.

1.20

Member and Participant Comments

- Suggest changing language – Automatic Generation Control is a glossary term
- Changing that term in another committee
- AGC also include operator doing generation control?
- No, definition says equipment

- It is the system that is controlling from a distance
- AGC is becoming cloudy as entities shift how the handle this – some may control in their control room
- Everything else in this area is a functional model – "used to perform the Generator Operator function" to make consisted with the others
- Where does ACE control fall in this –
- It is covered under Balancing Authority in earlier section
- Threshold as written is very low

Straw Polls

Thresholds on 1.18- 9 in Favor; 8 Oppose ; 1 Abstain

Thresholds on 1.19 10 in Favor; 8 Oppose ; 1 Abstain

Thresholds on 1.20. -12 in Favor; 6 Oppose 6; 1 Abstain

Jackie Collett brought back some revisions for the SDT's consideration on Thursday afternoon.

Revision to 1.2

Member and Participant Comments

- 1.2a and b?
- talking about two different time periods
- Contingency reserve different? Should both be Balancing Authority?
- That's where we ended yesterday
- Difference between what it is rated to do and what we actually do – never try to get to capability level
- Think they are talking about net dependable capability – gross minus axillaries
- Make as a recommendation without input or explanation from John Lim who is not here
- It is net Real Power capability – addressed in MOD 24
- Is this the time to discuss 1.2a? Brings threshold down to units over 200 MW – individually a very small amount,
- Should say a reserve sharing group – at least an "and/or"
- Three levels to ensure capture key assets
- Still calculating your contingency reserve as a BA, then figuring out shares
- Requirement as a BA may be lower than the total of a shared group

- Is premise for a shared group valid in cyber system attack
- Contingency reserve for BA bigger than the total for the shared group? The opposite
- Say which ever is the larger of the two.
- If go to the largest, then the 2,000 number becomes the criteria.
- SR – but only if you don't have either the BA or shared contingency categories – instead of the "lowest" use the "larger" of the two or the 2,000 with "total" in front of load share
- Anna – 1.2a should read "the greater value of the Contingency Reserve requirement of the associated Balancing Authority or the Reserve Sharing Group…"
- Have to have one of them
- Went to "lowest" to get the lowest from the previous 12 months
- Can we delete "b" and "c" and just have "a"?
- Like deleting b and c then breaking a up
- We are not saying what the contingency reserve should be but that you can use it
- We are interested in the "high" level – otherwise we get lost in the weeds
- Never have a single unit that exceeds the total
- No single unit is essential to the system
- Offered replacement language for "a" – The CR requirement of the RSG of the BA that is not a member of a Reserve Sharing Group – picking the one number you have rather than the higher of two possible numbers
- Goal is to set a threshold – the threshold we are after is the larger number
- Entities under identifies units because they can move load around without any one unit carrying the load – the size of the unit does not matter
- This is not about how you carry your reserve
- Reality is that type of fuel does not matter and no single unit matters to reserve capacity – the issue of concern here came from separating the two – consider putting back into one
- Lean toward deleting 1.2.a
- Work on 1.3 – if not needed then delete 1.2a
- These were one point before – pull back to just one single number or bright line without need to determine which one you fall into
- Support return to a combined criteria

- Put unit or group of units back together
- What we have said is that no single generator (including nuclear) is considered critical
- No single generator is critical because of the contingency plans
- Point out that under this language no singe or nuclear plants identified as critical assets in the United States – since no nuclear units share control centers – be prepared to state and justify that fact
- No single unit is critical based on size – may be critical for other reasons such as as a black start unit
- Order says n-1 approach will give us nonsensical approach and that saying single units are not noncritical by size – isn't that what I just said
- Need to give NERC or FERC the language they need to explain why a nuclear unit is not "critical"
- That is where we were going with 010 and 011
- Assumption is that 002-4 is not to address the Order – that is the 010-011 effort which will put protection on all units
- The goal to get more big asset generation on the critical asset list? Pick a number to get a correspondingly higher number of units on the list?
- Consider using how much a unit produces over a year

Revisions to 1.9 and 1.10

Member and Participant Comments

- 1.9 – are we trying to say there is an area that does not have IROLs? I don't have them, so then I have to run studies on cascading
- Recall that is a null set that does not require a study
- Okay with taking that out – the whole second sentence in both 1.9 and 1.10
- No objections to the remaining language

1.11 - Same issue we discussed above

1.14 and 1.15 were one item before – split now to BES Elements and aggregate automatic load shedding

Member and Participant Comments:

- Distribution providers in smart grid? Smart meter network would argue not designed to dump load? Should it say "capable of performing" rather than "that perform"?
- May need to lose the word "automatic" – automatic load shed is different from capable of -need to decide to use one or the other, but not both.

- Reluctant to drop the automatic load shedding –
- If we stick with "or" then change common Cyber Asset.
- Tried to capture with common Cyber Assets
- 1.15 is more important
- Support keeping both 1.14 and 1.15 but prefer keeping them simpler – too many words, need straightforward sentence
- Lots of different ways to shed load – the drop due to automatic shedding is what we are getting at here.
- Does the wording in 1.15 automatic include unintended assets?
- Does it include 300 MW of air conditioners when we turn up the thermostat? A: Yes, under the current standard – the concept has not changed
- Distribution providers were not included – only the transmission providers were covered
- If dumping 300 MW – suggestion to remove distribution provider?
- Could you put in an exception in this requirement rather than remove from the whole standard?
- Example of creating interim solution after developing a better process – not fair to say do it this way for now and we will change the rules on you again soon.
- FERC only has authority over bulk power, not distribution.
- Actually for bulk system reliability –
- This is not related to CIP 003 – we need to keep eye on the ball
- We put distribution provider in then out and back again – concern is in the load shed?
- This is new stuff added in to interim step?
- This is a new introduction with big implications

Propose Take out distribution provider? Support 14; Oppose 1; Abstain 1 (93%)

- Much in the news about smart grid and dropping load shed – will be a question we will need to address in the future.
- Wording in 1.15 – propose putting in the wording from 002-3 R1.25 – "System and facilities critical to automatic load shedding under a common control system capable of shedding 300 MW or more."
- Need to address in 1.14 too
- Could we drop both 1.15 and 1.14 in favor of this language.

Support this change in wording and drop 1.15 and 1.14:

- **Support 14; oppose 0 (in the room)**

Preamble under Critical Asset Criteria

Member and Participant Comments

- I like the additional language upfront but what if facility has no impact?
- Concerned about including invites argument that a particular facility has no impact
- Read current definition of CA – do industry a disservice if we use different wording here
- Take a look again at 1.9 and 1.10 language – left the language in here
- Gives someone capability to declare an asset – they may want to keep it on their list and then drop later with new version
- Goes along with risk based assessment

Jackie Collett brought back a report from the evening session. She noted the purpose was to provide a version of 002-4 to go out with or inform the survey – trying to get information in the survey to help inform the final version of 002-4. How do we preserve critical assets already identified and build on that set? Give entity a chance to identify a list that will stay on for a few years before having to change it again – allow them the option of putting on assets that may not be required as well as require a minimum – keep those on the list from the risk based methodology in addition to a minimum set.

She suggested that the SDT should keep in mind the big cost is getting something into compliance. Once that is done, then it is the cost in maintaining compliance due to compliance exposure. Preserve what is already identified by current risk based. Question for Howard – how much can we change the data request form? May want to add specific questions to help inform team to tweak draft for final version. (Yes, some flexibility to modify data request)

Member and Participant Discussion

- Can we figure out how many assets are added beyond the current base, but not what those assets are – that would go beyond a simple data request.
- Ask for three sets of numbers – number of current assets identified by current risk based methodology, number by category (current CIP 003-009), and estimated total identified using attachment 1 in place of risk based methodology

- This exercise is to deal with perception that not enough assets are identified under the current system – develop a threshold and modify R2 category to identify the common cyber assets for the groups of units rather than individual units – interim phase to move toward 010 – captures more generation assets – question about whether it would apply to transmission, etc.
- Look at current version of 002-4 – how do we capture those concepts?
- Modify and add words from 002-3?
- Any previously identified assets not captured by bright lines need to be sure do not drop off.
- Focus on cyber assets in generation – in transmission?
- Came up with criteria for generation – not sure applies to transmission
- Routable protocol in control center is included – do we need a similar substation or transmission criteria - deleted "in its assessment in 1.19."
- 1.20 Any critical assets that are identified in the last 24 months that are not identified in the bright line criteria – buts a time limit on when I can stop using risk based assessment
- Don't think it is a disaster if those assets fell off the list – will be captured later under medium.
- Take off list, list is too small and list requirement may come back even worse
- What happens if the 010 and 011 are not in place within 24 months?
- Those assets fall off – incentive to complete next version.
- Data request helps determine if we need that item or not.
- FERC put out metrics saying to respond to standards work within 18 months.
- There could be many scenarios in which 10 and 11 are not in place in 24 months, not just FERC approval.
- Wording of 1.20 – have to go back two years to see what was on your list or what is on list now stays on for next 24 months?
- The intent is the latter – do not want to lose ground.
- These words imply the former – need to clarify or modify.
- Add "in a risk-based methodology.
- Don't have to specifically ask what drops out – based on this language are we maintaining risk-based? If not, then say "any CAs identified in CIP 002-3 will remain on the list for the next 24 months…."

- Understand 24 months but puts pressure to ensure next version is in place in time to prevent anything drops off
- Bringing the results back? Rather run the risk based methodology
- Running RBM or anything else you want to add doesn't guarantee anything – if trying to keep CA's on the list, doesn't guarantee it.
- If get to re-run it each year then no guarantees – we voted we did not want a hybrid system of RBM and bright lines.
- How do we accomplish maintaining what we have and building on it? Shouldn't build on current list?
- Shouldn't lose ground, but not sure how do that
- Started with control centers – how do we address those, keep those in?
- Keep thresholds for data collection to see if they do anything for us
- Recommendation to put off decision until we get the data to analyze?
- Yes, keep thresholds in for data request
- Need data to inform the decision for the final version
- Only have one shot at data collections
- If leave thresholds in here then set false expectation in the industry that smaller units will not need to be covered – acquiesce in doing it, but concerned
- Do we still add criteria to drive data request directed at control centers – one that just says control center to have a baseline to compare to?
- Suggestion for 1.20 – have criteria with a lot of numbers – is that the right number? If number goes down then adjust the criteria – this goes away if we use survey for its purpose.
- Survey does not tell us how to adjust if we do not get the number expected.
- Maintain what you are doing along with the minimum as an interim step
- Also need to pay attention to survey ability to test additional thresholds – to see how the different levels play out and allow us to adjust high and medium
- Would not capture below 2000 MW – we have a hole in the control centers we could identify TS – seems we need more granularity in the survey – still also don't know what the number should be – why are they reluctant to give us a "good" number they are looking for?
- Regions are still developing and do not have the numbers they are trying to establish.
- Possible to get numbers back to review in August?

- Scott Rosenberger suggested using the team members as an initial sample.
- Leverage EEI members to get some numbers? Question number 2 will help but may have multiple assets that cover across categories.
- What we put in the survey will drive industry expectation especially given attachment #1 is our criteria – otherwise Howard will have to respond to comments about why did you choose that level.
- Draft survey already out there for comment.
- Always free to add anything we want to the list
- Aware anything we put out will look like a possible standard – everything is under development until approved – language says looking for data to inform development – cannot prevent them from reading implications into language – need to be sure to state this is not the final product.
- There is a value in its looking different.
- Should the Team file formal comment to allow staff to respond and change?
- Would require a call before Chicago with a quorum which has been difficult to obtain on a call.
- Not putting developing final criteria language off indefinitely, but need data to inform us.
- May be rare opportunity to hold an email vote on this issue of comments to the survey.
- Additional discussion on transmission language?
- Beyond the survey is that a concept we need to capture?
- Requires changes to R2
- Are we good with the concept? We struggled with specific words – capture in concept statement – the "fence theory"

III. CIP 011 SUB-TEAM PROGRESS REPORTS

On Friday morning the Vice Chair asked each Sub-team lead to give a report on progress since the Sacramento meeting. He suggested that as a minimum, each sub-team should complete its summary of industry informal comments received as well as the Dallas workshop input so a response document can be developed and be prepared for posting.

A. Sub-Team Progress Reports

1. Systems Security and Boundary Protection

Members: Jay Cribb (Lead), Jackie Collett, John Varnell, John Van Boxtel, Philip Huff *(Observer Participant: Brian Newell) (FERC: Justin Kelly)*

Jay Cribb reported on the Sub-team's efforts since Sacramento. They have split up and assigned requirements to member and are making progress – one or two troublesome ones we may recommend deleting, will distribute explanation – working with DJ's team to coordinate on perimeters – putting a straw man for both groups to review.

Member Comments:

- How much more time does your Sub-team need? A: As much as the schedule will allow us – also trying to use terminology from 003-009 to make industry comfortable.

2. **Recovery Management**

*Members:*Scott Rosenberger (Lead), Joe Doetzl, Tom Stevenson (*Observer Participant: Jason Marshall)(FERC: Dan Bogle)*

Scott Rosenberger reported that the Sub-team made some but not substantial progress over the past several weeks.

3. **Personnel and Physical Security**

Members: Doug Johnson (Lead), Rob Antonishen, Patrick Leon, Kevin Sherlin *(FERC: Drew Kittey)*

Doug Johnson spent time looking at rationale and his sub-team still needs to know if we are splitting the rationale out into one box and guidance into a separate box – still need to look at the levels again and be sure incorporated external communication and connections in proper way – meeting and coordinating with Jay's group – also working to coordinate with Sharon's group on revocation

4. **Change Management, System Lifecycle, Information Protection, Maintenance, and Governance**.

Members: Dave Revill (Lead), Jon Stanford, Keith Stouffer, Bill Winters *(Observer Participant: Brian Newell)(FERC: Jan Bargen, Matthew Dale)*

David Revill offered a report from the "hodge-podge" sub-team. He noted they had made good progress based on feedback in Sacramento. They have tried to address areas of overlap with other teams. They have also crafted new requirement for vulnerability assessment and believe they are a few side meetings away from presenting to full group.

Have not documented responses to informal comments yet – we need whatever time we can get plus one day.

5. Access Control

Members: Sharon Edwards (Lead), Jeff Hoffman, Jerry Freese *(Observer Participants: Roger Fradenburgh, Sam Merrell) (FERC: Mike Keane)*

Sharon Edwards reported on the sub-team electronic access good meetings. R7 added text boxes – reviewed other changes by requirement: R9 combined with R13, divided revocation into 4 distinct categories, leave of absence, voluntary and involuntary revocation,
R10 – passwords, if used as authenticators – tried to avoid TFEs.

6. Implementation Plan Sub-Team

Members: Scott Mix (Lead), Doug Johnson, John Lim, Jim Brenton, Tom Stevenson, Joe Bucciero, Bradley Yeates, William Gross, *(Jeff Drowley)(FERC: Jan Bargen, Mike Keane)*

This Team will be assisting with the CIP 002-4 implementation plan.

The Vice Chair thanked the sub-teams for the significant work done by sub-teams despite the political sideshow. He noted he had underestimated when the SDT could get back to 010 and 011 which may not be until December. Many in industry will want to know what was said and done at the Dallas workshop as well as the industry's informal comments. We need to decide soon how we want to address and respond to those in the future, but for now we need some closure on summarizing the comments we have received. WE may need a conference call or a webinar to explain why we are moving 002-4 and putting the 010 and 011 on hold. He urged each sub team to hold at least another call in order to create a response summary to industry comment by the Chicago meeting.

Industry Response Format Comments

- Format for that? # and summary of responses?
- Similar to responses last December – highlight of responses.
- Responses by question or free form – do we need a common format?
- Our team cannot respond by question but a common format might be helpful – will template a format for sub teams to use.
- Can say this is what we heard but not formulate how we will address the comment yet.
- Sub teams were provided summaries of comments related to their group – promised the industry we would publish comments from Dallas workshop

- Each group needs to review the transcripts from Dallas
- Spreadsheet from Bryan might be helpful in this process

B. Initial Discussion of CIP 010 and 011 Schedule

In light of the CIP 002-4 effort and the Sub-Team reports the Vice Chair asked the SDT to discuss issues surrounding the development of a revised CIP 010 & 011 schedule. Below are discussion points made.

Member Discussion Points

- Schedule – no end date formally communicated yet.
- Allen Mosher – finish product enacted by Dec 2011.
- What date does team have to deliver product to get approval by Dec. 2011.
- Sooner we get product to industry for comment the better the end product and more opportunity for industry to internalize the implications and build acceptance.
- Only have the schedule that starts ballots in January and ends in July
- Roughly move ballot in summer to end by December
- Try to prepare by May to get more rounds of comments
- Survey is in Word format – encourage team to offer suggestions
- Trying to put in additional criteria to establish useful numbers – should we break the h-m-l and instead put into a series of questions to avoid perception of moving toward a specific standard – allows to test different levels regarding control centers
- Concerned send out draft attachment 1 industry will take that as final product – reformat attachment?
- Just ask twenty-two questions rather than a table? Avoid industry expectation of the standard
- Trying to figure out how we capture the data
- Two different sets of questions
- More efficient to fill out the table?
- It is the h-m-l that will make people associated numbers to the potential standard
- More than twenty questions if ask about medium too
- Reorient the table in question 2
- We will use the results to explain why we changed the criteria numbers
- We are not set up to ask for the right threshold number
- We will know the response to the number of assets under threshold of 2000 and 1000
- Ask for as many pieces as you can to help inform 002-4 development and for 010 and 011 development
- But the more difficult you make it for entities to respond – trying to keep response burden to a minimum but get the most useful information – trying to balance

- Take the same assets from question 1 and now separate out into categories – sum of #2 will equal #1 – question #3 gets to the additional assets from bright lines – do we need a question to capture those assets that drop off
- May have a critical asset that is not even captured in question #1
- Question #3 gets to the delta between what you do today versus what you might do with bright line criteria
- Too complicated to ask questions to get to the right number? Need data to help set the hard break of bright lines
- Generation units we put on because of transmission constraints – but those units will not be identified in this survey
- We did an analysis based on the version 3 that went out in May for comment – ask the question more directly about what assets would be added and ask if items drop out ask why rather than asking for a number and then subtracting to figure out the corresponding numbers – makes information more transparent and will gain greater acceptance in the document
- That becomes more than a data request and would require team responses – team has to take data and respond by making changes to then post document within a week – captures a fine level of detail the team may not have enough time to respond to and reflect in the document to post
- Suggestions will be part of comment responses to the survey
- Sum of question #2 must equal #1 is lost in the middle of the paragraph – should make that more explicit in the directions or bolded
- Have to tell them they have to put items from #1 in one and only one spot in #2
- Any critical assets that cannot be categorized in #2 – we have a category for low
- We ask for anything else – this gets at the assets identified as important but not captured by the risk based assessment
- Can team members take an early run at completing survey as a sample to look at in Chicago
- Won't have final version of the survey ready until July 28 to be posted as part of package to Board of Trustees
- Won't be much advanced notice. Straw survey-
- Get a not quite final form. Fill out and then bring to Chicago. (before beginning)

IV. NEXT STEPS

Phil Huff noted the 002-4 team will continue working. Implementation plan development for 002-4 *(use the CIP 10 and 11 implementation team).* Guidance/ Rationale. Members will try to get their companies to do the survey. The suggestions on framing the survey will be incorporated as discussed by NERC. CIP 10 and 11 sub-teams should capture work done and keep meeting to develop industry comment summary. Phil offered to send out a template for the sub-teams to use. All members should review the transcription of workshop and provide NERC any feedback by Chicago on any red flags or mistakes.

The Vice Chair noted the Detroit open Smart Grid meeting next week. Phil will send out request of other SDT members to see if any can attend and suggested that the SDT would like to continue collaboration but was unlikely for their next meeting.

The SDT will consider going to 3-day meeting schedule after September with longer days on Tuesday –Thursday. The Vice Chair asked members to make the commitment to stay through to Friday noon at the next SDT meeting in Chicago. He also said that in light of the quorum requirements he and the Chair will consider an attendance policy and consult with members who have had difficulty in participating over the past several months. The SDT reviewed the issue of a letter of appreciation to the CEO's of the member companies from the President of NERC for the hard work and commitment of the members to the CIP revisions. It was agreed that NERC staff would take any requests from members to the NERC president.

Finally, the Vice Chair, on behalf of the SDT, thanked Sam Merrill and the CERT for their excellent hosting and facilities. He noted Doug Johnson will be our host in Chicago in August and urged members to register for the session.

Meeting adjourned at 11:30 a.m.

Appendix #1

Project 2008-06 Cyber Security Order 706 SDT

Draft 24th Meeting Agenda

July 13, 2010, Tuesday- 8:00 AM to 5:00 PM EDT

July 14, 2010 Wednesday- 8:00 AM to 5:00 PM EDT

July 15, 2010 Thursday- 8:00 AM to 5:00 PM EDT

July 16, 2010 Friday- 8:00 AM to 12:00 PM EDT

CERT Software Engineering Institute, Carnegie Mellon University

Pittsburgh, PA

NOTE:

1. Agenda Times May be Adjusted as Needed during the Meeting

2. Drafting and Sub-team Meetings May Not Have Access to Telephones and Ready Talk

Proposed Meeting Objectives/Outcomes:

- To review the CSO706 SDT 2010 Work Plan and Schedule for CIP-002-4
- To explore and clarify the Work Plan and Schedule for completing CIP-010 & 011
- To review, clarify and refine the strawman CIP-002-4 standard proposal
- To convene sub-teams to review the sub-team responses to Industry comments and proposed changes to CIP-010 and 011
- To provide SDT guidance so sub-teams can make further refinements to CIP 002-4, 010 & 011
- To agree on next steps and assignments

Tuesday, July 13, 2010 8:00 a.m. - 5:00 p.m.

- Introduction, welcome, and opening remarks -*(Morning)*
- Overview of CSO706 SDT Work plan and schedule for CIP 002-4 and Explore and Clarify CIP 010 & 011-*(Morning)*
- Review and seek agreement on proposal for refining the SDT Consensus Procedures -*(Morning)*
- Receive updates on other related cyber security initiatives- *NERC Staff and SDT Members (Morning)*
- Review and refine draft CIP 002-4 standard and related documents. *(Morning)*
- "Lunch and Learn"- Format Proposal*(Lunch)*
- Review and refine draft CIP 002-4 standard and related documents. *(Afternoon Plenary)*

Wednesday, July 14, 2010 8:00 a.m. - 5:00 p.m.

- Sub-teams present requirement changes and test SDT consensus on directions and changes *(Morning Plenary)*
- "Lunch and Learn"- NERC CIP SDT and the ASAP-SG Architecture Team
- Sub-teams present requirement changes and test SDT consensus on directions and changes *(Afternoon Plenary)*

Thursday, July 15, 2010, 8:00 a.m. - 5:00 p.m.

- Sub-teams present requirement changes and test SDT consensus on directions and changes *(Morning)*
- "Lunch and Learn"- Substation Networks (Varnell)

- CIP-010 and 011 Sub-Teams address changes in requirements in light of industry c*omments & i***n**puts from the SDT *(Afternoon)*
- Sub-teams present requirement changes and test SDT consensus on directions and changes *(Afternoon)*

Friday, July 16, 2010, 8:00 a.m. - 12:00 p.m.

- Review of CIP-002-4 Refinements (Morning)
- Review SDT Workplan Schedule to prepare new Draft CIP-010 and 011 Requirements documents. *(Morning)*
- Review Next Steps and Sub-Team schedule and SDT Chicago Meeting Agenda (*Late Morning)*

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

CSO 706 SDT DRAFTING SUB-TEAMS (JULY, 2010)

Sub-Team	
CIP 010 BES System Categorization	John Lim (Lead), Rich Kinas, Jim Brenton, Dave Norton *(Observer Participants: Rod Hardiman, Jim Fletcher)* *(FERC: Mike Keane, Peter Kuebeck)*
Personnel and Physical Security	Doug Johnson (Lead), Rob Antonishen, Patrick Leon, Kevin Sherlin *(FERC: Drew Kittey)*
System Security and Boundary Protection	Jay Cribb (Lead), Jackie Collett, John Varnell, John Van Boxtel, Philip Huff *(Observer Participant: Brian Newell)* *(FERC: Justin Kelly)*
Incident Response and Recovery	Scott Rosenberger (Lead), Joe Doetzl, Tom Stevenson (*Observer Participant: Jason Marshall)* *(FERC: Dan Bogle)*
Access Control	Sharon Edwards (Lead), Jeff Hoffman, Frank Kim, Jerry Freese *(Observer Participants: Roger Fradenburgh, Sam Merrell)* *(FERC: Mike Keane)*
Change Management, System Lifecycle, Information Protection, Maintenance, and Governance	Dave Revill (Lead), Jon Stanford, Keith Stouffer, Bill Winters *(Observer Participant: Brian Newell)* *(FERC: Jan Bargen, Matthew Dale)*
Implementation Plan	Scott Mix (Lead), Doug Johnson, John Lim, Jim Brenton, Tom Stevenson, Joe Bucciero *(Nuclear: Bradley (Brad) Yeates, William Gross, Jeff Drowley)* *(FERC: Jan Bargen, Mike Keane)*

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Appendix # 1— Meeting Agenda

Project 2008-06 Cyber Security Order 706 SDT
Draft 25th Meeting Agenda
August 10, 2010, Tuesday- 8:00 AM to 5:00 PM CDT
August 11, 2010 Wednesday- 8:00 AM to 5:00 PM CDT
August 12, 2010 Thursday- 8:00 AM to 5:00 PM CDT
August 13, 2010 Friday- 8:00 AM to 12:00 PM CDT
Exelon Corporation
10 S. Dearborn Street, 48th Floor , Chicago, IL
NOTE: 1. Agenda Times May be Adjusted as Needed during the Meeting
NOTE: 2. Drafting Sub-team Meetings May Not Have Access to Telephones and Ready Talk

Proposed Meeting Objectives/Outcomes:

- To review the adopted CSO706 SDT 2010 Work Plan and Schedule for CIP-002-4 in 2010
- To review and adopt a Work Plan and Schedule for completing CIP-010 & 011 in 2011
- To review and discuss the results and implications of SDT member companies' data survey results for the CIP 002-4 draft.
- To review, clarify, refine and adopt CIP-002-4 standard proposal for NERC staff review
- To review CIP-010 & 011 sub-teams draft responses to industry and Dallas workshop
- To agree on next steps and assignments

Tuesday, August 10, 2010 8:00 a.m. - 5:00 p.m.

- Introduction, welcome, and opening and guest remarks -*(Morning)*
- Receive updates on other related cyber security initiatives- *NERC Staff and SDT Members (Morning)*
- Review of CSO706 SDT Work plan and schedule for CIP 002-4 *(Morning)*
- Review of CSO706 Draft SDT Work plan and schedule for CIP 010 & 011 *(Morning)*
- "Lunch and Learn"- Forensics U.S. CERT *(Lunch)*
- Overview of NERC Survey Development and Industry Comments *(Afternoon)*
- Review and refine draft CIP 002-4 standard and related documents *(Afternoon)*

Wednesday, August 11, 2010 8:00 a.m. -5:00 p.m.

- Review and discuss the SDT member survey responses and their implications for CIP 002-4 drafting *(Morning)*
- Review and refinement of CIP-002-4 documents including implementation plan for NERC staff review *(Afternoon)*

Thursday, August 12, 2010, 8:00 a.m. - 5:00 p.m.

- Adoption of CIP 002-4 documents for NERC staff review *(Morning)*
- Adoption of CIP 010 & 011 Draft Schedule *(Morning)*
- CIP-010 and 011 Sub-teams present draft summary responses to Industry Comments and Workshop input *(Morning and Afternoon)*
- Agree on schedule for incorporating draft responses to Industry Comments and Workshop input into a single response document. *(Afternoon)*

Friday, August 13, 2010, 8:00 a.m. - 12:00 p.m.

- Review directions and next steps to CIP-010 and 011 Sub-teams – *as needed (Morning)*
- Address 002-4 planning for September Webinar *(Morning)*
- Review SDT September 8-10, 2010 Winnipeg Meeting Agenda (*Late Morning)*

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Project 2008-06 Cyber Security Order 706 SDT
Draft 25th Meeting Agenda
August 10, 2010, Tuesday- 8:00 AM to 5:00 PM CDT
August 11, 2010 Wednesday- 8:00 AM to 5:00 PM CDT
August 12, 2010 Thursday- 8:00 AM to 5:00 PM CDT
August 13, 2010 Friday- 8:00 AM to 12:00 PM CDT
Exelon Corporation, Chicago, IL
NOTE: 1. Agenda Times May be Adjusted as Needed during the Meeting
NOTE: 2. Drafting Sub-team Meetings May Not Have Access to Telephones and Ready Talk

Proposed Meeting Objectives/Outcomes:

- To review the adopted CSO706 SDT 2010 Work Plan and Schedule for CIP-002-4 in 2010
- To review and adopt a Work Plan and Schedule for completing CIP-010 & 011 in 2011
- To review and discuss the results and implications of SDT member companies' data survey results for the CIP 002-4 draft.
- To review, clarify, refine and adopt CIP-002-4 standard proposal for NERC staff review
- To review CIP-010 & 011 sub-teams draft responses to industry and Dallas workshop
- To agree on next steps and assignments

Draft Agenda

Tuesday	**August 10, 2010 - 8:00 a.m. - 5:00 p.m.**
8:00 a.m.	Welcome and opening remarks- *John Lim, Chair & Phil Huff, Vice Chair* Roll Call; NERC Antitrust Compliance Guidelines- *Joe Bucciero* Facilitator review and SDT acceptance of July 13-16, 2010 Pittsburgh SDT meeting summary
8:15	Review of meeting objectives, agenda and meeting guidelines- *Bob Jones*
8:20	Standards Committee Chair and Senior NERC Management Comments to the SDT on their work
8:40	Review of CSO 706 SDT CIP 002-4 adopted work plan and schedule: *Stu Langton*
8:45	Review and Discussion of CSO 706 SDT CIP 010 & 011 draft work plan and schedule: *Stu Langton*
9:30	Updates on other related cyber security initiatives- *NERC Staff and SDT Members*
10:00	*Break*
10:15	Overview of SDT CIP 002-4 Strawman documents
10:45	Review and refine draft CIP 002-4 standard and related documents
12:00	"Lunch and Learn"- Forensics U.S. CERT *(Lunch)*
1:30	Overview of NERC Survey development and industry comments
2:00	Review and refine draft CIP 002-4 standard and related documents
3:15	*Break*
3:30	Review and refine draft CIP 002-4 standard and related documents
4:50	Review any drafting assignments and Wednesday agenda
5:00	*Recess*

- *Possible Ad Hoc Drafting or Sub Team Meetings- Evening*

Wednesday	**August 11, 2010 - 8:00 a.m. - 5:00 p.m.**
8:00	Welcome and Agenda Review, Roll Call and Antitrust Guidelines- *John Lim, Phil Huff, Joe Bucciero*
8:15	Review and discuss the SDT member survey responses and their implications for CIP 002-4 drafting
10:00	*Break*
10:15	Review and discuss the SDT member survey responses and their implications for CIP 002-4 drafting
12:00	*Lunch*
1:00	Review and refinement of CIP-002-4 documents including implementation plan for NERC staff review
3:00	*Break*
3:15	Review and refinement and consensus testing of CIP-002-4 documents including implementation plan for NERC staff review
4:50	Review any drafting assignments and Thursday agenda
5:00	*Recess*

- *Possible Ad Hoc Drafting or Sub Team Meetings- Evening*

Thursday	**August 12, 2010 - 8:00 a.m. - 5:00 p.m.**
8:00	Welcome and Agenda Review, Roll Call and Antitrust Guidelines- *Phil Huff, Joe Bucciero*
8:15	Adoption of CIP 002-4 documents for NERC staff review
9:00	Review and Adoption of CIP 010 & 011 Draft Schedule
10:00	*Break*
10:15	CIP-010 and 011 Sub-teams present draft summary responses to Industry Comments and Workshop input
12:00	*Lunch*
1:00	CIP-010 and 011 Sub-teams present draft summary responses to Industry Comments and Workshop input
3:00	*Break*
4:30	Agree on schedule for incorporating draft responses to Industry Comments and Workshop input into a single response document *(Afternoon)*
4:50	Review any drafting assignments and Friday agenda
5:00	*Recess*

- *Possible Ad Hoc Drafting or Sub Team Meetings- Evening*

Friday	**August 13, 2010 - 8:00 a.m. - 12:00 p.m.**
8:00	Welcome and Agenda Review, Roll Call and Antitrust Guidelines- *Phil Huff, Joe Bucciero*
8:15	Address CIP 002-4 schedule and tasks including planning for September Webinar
10:00	*Break*

10:15	Review directions and next steps to CIP-010 and 011 Sub-teams
11:00	Review CIP-010 and 011 Sub-Team Schedule
11:30	Review the Winnipeg Meeting Agenda and Next Steps and Assignments
12:00	*Adjourn & Lunch*

- **Appendix # 2 Attendees List**

July 13-16, 2010, Pittsburgh PA

Attending in Person — SDT Members and Staff

1. Rob Antonishen	Ontario Power Generation (T/W)
2. Jim Brenton	ERCOT
3. Jay S. Cribb	Southern Company Services
4.Jackie Collett	Manitoba Hydro (W/Th/F)
5.Joe Doetzl	Kansas City Pwr. & Light Co (T/W/Th)
6. Sharon Edwards	Duke Energy (T/W/Th)
7.Gerald S. Freese	America Electric Pwr.
8. Jeff Hoffman	U.S. Bureau of Reclamation, Denver (T/W/Th)
9. Phillip Huff, Vice Chair	Arkansas Electric Coop Corporation
10. Doug Johnson	Exelon Corporation – Commonwealth Edison
11.Rich Kinas	Orlando Utilities Commission (T/W/Th)
12. Patricio Leon	Southern California Edison
13. John Lim, Chair	Consolidated Edison Co. NY (T/W)
14. David Norton	Entergy (T/W)
15. David S. Revill	Georgia Transmission Corporation
16. Scott Rosenberger	Luminant Energy
17. Kevin Sherlin	Sacramento Municipal Utility District (T/W/Th)
18.Tom Stevenson	Constellation
19. John Van Boxtel	WECC (T/W/Th)
Scott Mix	NERC
Roger Lampila	NERC
Howard Gugel	NERC
Joe Bucciero	NERC/Bucciero Consulting, LLC
Robert Jones	FSU/FCRC Consensus Center
Stuart Langton	FSU/FCRC Consensus Center

SDT Members Attending via ReadyTalk and Phone

19. John D. Varnell	Technology Director, Tenaska Power Services Co.

SDT Members Not Participating

Frank Kim	Hydro One Networks Inc. (Th/F)
Keith Stouffer	National Institute of Standards & Technology (T/W/Th)
Jonathan Stanford	Bonneville Power Administration
William Winters	Arizona Public Service, Inc.

Others Attending in Person

Jan Bargen	FERC
Summer Esquerre	NextEraEnergy (FPL)
Jim Fletcher	American Electric Power
Michael Keane	FERC
Drew Kittey	FERC
Jason Marshall	Midwest ISO
Sam Merrell	CERT/Software Engineering Institute
Brian Newell	American Electric Power
Anna Wang	Burns & McDonnell

Brian Newell - AEP
-
Robert Preston Lloyd - SCE
Alex Salinas - SCE
Sam Merrell - SEI/CERT
Jim Stevens - SEI/CERT

Others Attending via Readytalk and Phone
July 13, 2010, Tuesday
July 14, 2010, Wednesday
July 15, 2010, Thursday
July 16, 2010, Friday

Appendix #3 NERC Antitrust Compliance Guidelines

I. General

It is NERC's policy and practice to obey the antitrust laws and to avoid all conduct that unreasonably restrains competition. This policy requires the avoidance of any conduct that violates, or that might appear to violate, the antitrust laws. Among other things, the antitrust laws forbid any agreement between or among competitors regarding prices, availability of service, product design, terms of sale, division of markets, allocation of customers or any other activity that unreasonably restrains competition.

It is the responsibility of every NERC participant and employee who may in any way affect NERC's compliance with the antitrust laws to carry out this commitment.

Antitrust laws are complex and subject to court interpretation that can vary over time and from one court to another. The purpose of these guidelines is to alert NERC participants and employees to potential antitrust problems and to set forth policies to be followed with respect to activities that may involve antitrust considerations. In some instances, the NERC policy contained in these guidelines is stricter than the applicable antitrust laws. Any NERC participant or employee who is uncertain about the legal ramifications of a particular course of conduct or who has doubts or concerns about whether NERC's antitrust compliance policy is implicated in any situation should consult NERC's General Counsel immediately.

II. Prohibited Activities

Participants in NERC activities (including those of its committees and Subroups) should refrain from the following when acting in their capacity as participants in NERC activities (e.g., at NERC meetings, conference calls and in informal discussions):

- Discussions involving pricing information, especially margin (profit) and internal cost information and participants' expectations as to their future prices or internal costs.
- Discussions of a participant's marketing strategies.
- Discussions regarding how customers and geographical areas are to be divided among competitors.
- Discussions concerning the exclusion of competitors from markets.
- Discussions concerning boycotting or group refusals to deal with competitors, vendors or suppliers.

III. Activities That Are Permitted

From time to time decisions or actions of NERC (including those of its committees and Subgroups) may have a negative impact on particular entities and thus in that sense

adversely impact competition. Decisions and actions by NERC (including its committees and Subgroups) should only be undertaken for the purpose of promoting and maintaining the reliability and adequacy of the bulk power system. If you do not have a legitimate purpose consistent with this objective for discussing a matter, please refrain from discussing the matter during NERC meetings and in other NERC-related communications.

You should also ensure that NERC procedures, including those set forth in NERC's Certificate of Incorporation and Bylaws are followed in conducting NERC business. Other NERC procedures that may be applicable to a particular NERC activity include the following:

- Reliability Standards Process Manual
- Organization and Procedures Manual for the NERC Standing Committees
- System Operator Certification Program

In addition, all discussions in NERC meetings and other NERC-related communications should be within the scope of the mandate for or assignment to the particular NERC committee or Subgroup, as well as within the scope of the published agenda for the meeting.

No decisions should be made nor any actions taken in NERC activities for the purpose of giving an industry participant or group of participants a competitive advantage over other participants. In particular, decisions with respect to setting, revising, or assessing compliance with NERC reliability standards should not be influenced by anti-competitive motivations.

Subject to the foregoing restrictions, participants in NERC activities may discuss:

- Reliability matters relating to the bulk power system, including operation and planning matters such as establishing or revising reliability standards, special operating procedures, operating transfer capabilities, and plans for new facilities.
- Matters relating to the impact of reliability standards for the bulk power system on
- electricity markets, and the impact of electricity market operations on the reliability of the bulk power system.
- Proposed filings or other communications with state or federal regulatory authorities or other governmental entities.
- Matters relating to the internal governance, management and operation of NERC, such as nominations for vacant committee positions, budgeting and assessments, and
- employment matters; and procedural matters such as planning and scheduling meetings.

Any other matters that do not clearly fall within these guidelines should be reviewed

with NERC's General Counsel before being discussed.

APPENDIX # 4
CSO 706 SDT MEETING SCHEDULE
OPTIONS 1 AND 2

Appendix X
CIP VERSION 4 PARKING LOT (JUNE, 2010)

Issue (Reference)	Raised By	Date Raised	Sub-Team Assigned	Resolution (Date)
Review clarity of item 1.1, Attachment 2 – Generation Facilities and criteria for Contingency Reserve and Reserve Sharing	Rich Kinas	4/29	CIP-002	**AI:** Revise item 1.1 with input from the industry through the informal comments received.
Shouldn't there be delegations made by the Senior Manager for any exceptions (CIP-011 R2 & R3)	Jackie Collett	4/29	Governance	**Resolved** by the revised CIP-011 text that was posted.
User type access (R3) 3.2 Review the need for network device training (Operators, etc.)	Jim Brenton	4/29	Physical/Cyber & Access Control	Possibly regarding the level of access for outward facing and inward facing devices. What type of user training is required for each level? **Add role-based access (e.g., admin vs. application level access) – physical access & training requirements. Awareness training for everyone, and role-based training as required.**
Combine tables for electronic and physical access control systems (R6, R20, & R22)	Philip Huff	4/29	Physical and System Security	**AI:** Double-check that the proper requirements are incorporated in the respective tables.
Remove ~~Training~~ Termination for physical	Doug	4/29	Physical	

Issue (Reference)	Raised By	Date Raised	Sub-Team Assigned	Resolution (Date)
access to Low Impact (R9)	Johnson			
What do the blank cells mean in the tables in instances where a timeframe is given? (R9)	Jackie Collette	4/29	Howard Gugel	Do they mean there is no requirement at that particular level? **AI:** Double-check the table entries to ensure that the entries are indicative of the requirement. Possibly a statement should be added to the Guidance Document that describes what is meant by a blank entry in a table.
Monitoring the baseline configuration means monitoring the physical location as written. (R23)	Rob Antonishen	4/29	Change Management (Dave Revill)	**AI:** Is baseline the right term? What do we mean by changing physical location?
What timeframe for issuing alerts (Table entry 18.2)	Jackie Collett	4/29	System Security	**AI:** What is the response time requirement? In what timeframe should the alerts be issued?
Need to address what disciplinary actions are? Should physical or cyber access be revoked?	Jackie Collett	5/11	Disciplinary actions (physical/cyber access)	AI:
Combine the revocation of physical and electronic access requirements (including remote access) into one topical area of the standard	Phil Huff	5/11/2010	Personnel access (Sharon Edwards)	**AI:** Need to investigate possible alternatives. Have a requirement to develop a procedure for handling

Issue (Reference)	Raised By	Date Raised	Sub-Team Assigned	Resolution (Date)
				revocation of access.
Review "objective" statements to ensure they do not implicate requirements	FERC	5/27/2010	All	
Make requirements text consistent throughout the Standard	FERC	5/27/2010	All	
Global review of adjectives like "sufficient", "appropriate", etc.	FERC	5/27/2010	All	
Baseline for Low level of Impact	Drafting Teams	6/10/2010	ALL	**Completed on 6/10/2010**
Description of Timing (e.g., annual, months, etc.)	Howard	6/10/2010	NERC	
Protection requirements for electronic and physical access control systems	Doug/Phil	6/10/2010	ALL	
Broad Application of TFE Statement	SDT	6/9/2010	ALL	
Gantt Chart for Compliance Deadlines	Varnell	6/9/2010	Howard	
Exclusion for Entities that don't own cyber systems	Doug	6/10/2010	Full SDT	

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Appendix #5 SDT Consensus Procedures
CYBER SECURITY FOR ORDER 706 STANDARD DRAFTING TEAM
Proposed Refined Consensus Guidelines (May, 2010)

The Cyber Security for Order 706 Standard Drafting Team (Team) will seek consensus on its recommendations for any revisions to the CIP standards.

Consensus Defined. Consensus is a participatory process whereby, on matters of substance, the Team strives for agreements which all of the members can accept, support, live with or agree not to oppose. In instances where, after vigorously exploring possible ways to enhance the members' support for posting CIP standards documents for industry comment or balloting, and the Team finds that 100% acceptance or support of the members present is not achievable, decisions to adopt standards documents for balloting will require at least ~~75%~~ 2/3rds favorable vote of all members present and voting. This super majority decision rule underscores the importance of actively developing a Team consensus on substantive issues ~~which the industry will need to approve by a 2/3's vote.~~

Quorum Defined. The Team will make decisions only when a quorum is present. A quorum shall be constituted by at least 2/3 (18 members) of the 26 appointed members being present in person or by telephone.

Electronic Mail Voting. Electronic voting will only be used when a decision needs to be made between regular meetings under the following conditions:

- It is not possible to coordinate and schedule a conference call for the purpose of voting, or;
- Scheduling a conference call solely for the purpose of voting would be an unnecessary use of time and resources, and the item is considered a small procedural issue that is likely to pass without debate.

Electronic voting will not be used to decide on issues that would require a super majority vote or have been previously voted on during a regular meeting or for any issues that those with opposing views would feel compelled to want to justify and explain their position to other team members prior to a vote. The Electronic Voting procedure shall include the following four steps:

1. The SDT Chair or Vice-Chair in his absence will announce the vote on the SDT mailing list and include the following written information: a summary of the issue being voted on and the vote options; the reason the electronic voting is being conducted; the deadline for voting (which must be at least 4 hours after the time of the announcement).
2. Electronic votes will be tallied at the time of the deadline and no further votes will be counted. If quorum is not reached by the deadline then the vote on the proposal will not pass and the deadline will not be extended.
3. Electronic voting results will be summarized and announced after the voting deadline back to the SDT+ mailing list.
4. Electronic voting results will be recapped at the beginning of the next regular meeting of the SDT.

Consensus Building Techniques and Robert's Rules of Order. The Team will develop its recommendations using consensus-building techniques with the leadership of the Chair and Vice Chair and the assistance of the facilitators. Techniques such as brainstorming, ranking and prioritizing approaches will be utilized. The Team's consensus process will be conducted as a facilitated consensus-building process. Only Team members may participate in consensus ranking or votes on proposals and recommendations. Observers/members of the public are welcome to speak when recognized by the Chair, Vice Chair or Facilitator. The Team will utilize Robert's Rules of Order *(as per the NERC Reliability Standards Development Procedure)*, as modified by the Team's adopted procedural guidelines, to make and approve formal motions. However, the 2/3rds super-majority voting requirement will supersede the normal voting requirements used in Robert's Rules of Order for decision-making on substantive motions and amendments to motions. The Team will develop substantive written materials and options using their adopted facilitated consensus-building procedures, and will use Robert's Rules of Order only for formal motions once the Chair determines that a facilitated discussion is completed.

Appendix #
CSO 706 SDT DRAFTING SUB-TEAMS AND PRINCIPLES

Sub-Team	
CIP 010 (002-4) BES System Categorization	John Lim, Rich Kinas, Jim Brenton, Jackie Collett, *Bill Winters*, Dave Norton, *Jay Cribb* *Rod Hardiman (Observer)*
Personnel and Physical Security	Doug Johnson (Lead), Rob Antonishen, Patrick Leon, Kevin Sherlin
System Security and Boundary Protection	Jay Cribb (Lead), John Varnell John Van Boxtel, Jackie Collett, Phil Huff
Incident Response and Recovery	Scott Rosenberger (Lead), Joe Doetzl, Tom Stevenson, (*Observer Participants: Jason Marshall*
Access Control	Sharon Edwards (Lead), Gerry Freese, Jeff Hoffman, Frank Kim *Observer Participants: Sam Merrell*
Governance, Change Management, System Lifecycle and Information Protection and Maintenance	Dave Revill (Lead), Keith Stouffer, Bill Winters, Jon Stanford, Phil Huff *Observer Participants: John Fridye*

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Agenda
Cyber Security Order 706 SDT — Project 2008-06

August 10, 2010 | 8:00 AM to 5:00 PM CDT
August 11, 2010 | 8:00 AM to 5:00 PM CDT
August 12, 2010 | 8:00 AM to 5:00 PM CDT
August 13, 2010 | 8:00 AM to 12:00 PM CDT

Exelon Corporation
10 S. Dearborn Street
Chicago, IL, 48th Floor

NOTE: 1. Agenda Times May be Adjusted as Needed during the Meeting
NOTE: 2. Drafting Sub-team Meetings May Not Have Access to Telephones and Ready Talk

Proposed Meeting Objectives/Outcomes:

- To review the adopted CSO706 SDT 2010 Work Plan and Schedule for CIP-002-4 in 2010
- To review and adopt a Work Plan and Schedule for completing CIP-010 & 011 in 2011
- To review and discuss the results and implications of SDT member companies' data survey results for the CIP 002-4 draft.
- To review, clarify, refine and adopt CIP-002-4 standard proposal for NERC staff review
- To review CIP-010 & 011 sub-teams draft responses to industry and Dallas workshop
- To agree on next steps and assignments

Tuesday, August 10, 2010 8:00 a.m. - 5:00 p.m.

- Introduction, welcome, and opening and guest remarks -*(Morning)*
- Receive updates on other related cyber security initiatives- *NERC Staff and SDT Members (Morning)*
- Review of CSO706 SDT Work plan and schedule for CIP 002-4 *(Morning)*
- Review of CSO706 Draft SDT Work plan and schedule for CIP 010 & 011 *(Morning)*
- "Lunch and Learn"- Forensics U.S. CERT *(Lunch)*
- Overview of NERC Survey Development and Industry Comments *(Afternoon)*

- Review and refine draft CIP 002-4 standard and related documents *(Afternoon)*

Wednesday, August 11, 2010 8:00 a.m. -5:00 p.m.

- Review and discuss the SDT member survey responses and their implications for CIP 002-4 drafting *(Morning)*
- Review and refinement of CIP-002-4 documents including implementation plan for NERC staff review *(Afternoon)*

Thursday, August 12, 2010, 8:00 a.m. - 5:00 p.m.

- Adoption of CIP 002-4 documents for NERC staff review *(Morning)*
- Adoption of CIP 010 & 011 Draft Schedule *(Morning)*
- CIP-010 and 011 Sub-teams present draft summary responses to Industry Comments and Workshop input *(Morning and Afternoon)*
- Agree on schedule for incorporating draft responses to Industry Comments and Workshop input into a single response document. *(Afternoon)*

Friday, August 13, 2010, 8:00 a.m. - 12:00 p.m.

- Review directions and next steps to CIP-010 and 011 Sub-teams – *as needed (Morning)*
- Address CIP-002-4 planning for September Webinar *(Morning)*
- Review SDT September 8-10, 2010 Winnipeg Meeting Agenda (*Late Morning)*

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Notes
Cyber Security Order 706 SDT — Project 2008-06

August 10, 2010 | 8 AM to 5 PM CDT
August 11, 2010 | 8 AM to 5 PM CDT
August 12, 2010 | 8 AM to 5 PM CDT
August 13, 2010 |8 AM to 12 PM CDT
Chicago, Illinois

Robert Jones, Stuart Langton, and Hal Beardall
Facilitation and Meeting Design
FCRC Consensus Center, Florida State University

Joe Bucciero, Bucciero Consulting, LLC

http://www.nerc.com/filez/standards/Project_2008-06_Cyber_Security.html

116-390 Village Blvd.
Princeton, NJ 08540
609.452.8060 | www.nerc.com

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

CSO706 SDT August 10-13, 2010 Meeting Summary Contents

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Cyber Security Order 706 SDT- Project 2008-06
25TH MEETING
August 10-13, 2010
Chicago, IL

EXECUTIVE SUMMARY

On Tuesday morning, John Lim, Chair & Phil Huff, Vice Chair of the CSO 706 SDT welcomed members and other participants to Chicago and thanked Doug Johnson for hosting the meeting. Doug reviewed the logistics for the meeting. Joe Bucciero conducted a roll call of members and participants in the room and on the conference call. Mr. Bucciero also reviewed the need to comply with NERC's Antitrust Guidelines each day of the meeting, and reminded all participants that the meeting has been publicly noticed and is open to the public. John Lim reviewed the proposed meeting objectives and agenda.

On Thursday morning, the SDT unanimously adopted the July 13-16 Pittsburgh meeting summary with edits presented by John Van Boxtel.

The Chair noted the opportunity of the SDT to hear from Allen Mosher, Chair of the NERC Standards Committee on the SDT's efforts and progress. Allen Mosher addressed the SDT noting the atypical external pressures on the Team related to the nature of the CIP changes the Team has been charged to develop and the level of scrutiny due to the high degree of interest in Washington among agencies and congress in cyber security. He urged the SDT to preserve the two-track approach to developing the CIP standards noting this is an important opportunity to prove to political and regulatory interests that the industry can produce effective cyber security standards and do it promptly. Completing the CIP 002-4 process by the end of this year will help demonstrate to Congress that the industry is capable of self-regulation. Mr. Mosher reiterated that he believed that CIP-010 and CIP-011were the right model, and he hoped the SDT would be focusing again soon on that task. He acknowledged that the CIP 002-4 approach was not a risk based assessment, but stressed the importance of analyzing the data rewquest results regarding "bright lines" to determine whether there will be an increased number of CAs and CCAs. At the end of the day on Tuesday, Allen Mosher thanked the SDT for what it is doing in working as a drafting team to develop consensus. He suggested the SDT is making significant progress on something that is very hard to do.

On Thursday morning, John Lim introduced Herb Schrayshuen, the new NERC Vice President and Director of Standards, who joined the SDT meeting on Thursday morning. He thanked each member for their service and understood and welcomed their questions, recognizing the tensions in the process and feelings about how the SDT has been treated over the past couple months. He took questions from SDT members on: what is success for CIP 002-4; system vs. assets approaches; physical security; and the present culture of

compliance and standards. He noted that process is important but so is delivery. Responding to a question of what success looks like for the SDT's work, he suggested that a standard that helps the industry deal with deficiencies in the current standards and delivers results that improve the cyber security framework of the grid could be characterized as success. He promised to help the SDT secure the necessary resources and assistance to get their job done successfully. The culture of compliance versus the culture of reliability is an on-going debate on how to approach cyber security. He noted that we cannot comply our way to reliability. Mr. Schrayshuen noted that NERC will soon release a new reliability standards approach, including how to prioritize the work to be accomplished.

On Wednesday morning, NERC staff (Howard Gugel) reviewed with the SDT the industry's comments and the NERC responses and changes on the draft NERC Data Request. Howard also presented a summary of the inputs received from the six entities that volunteered, as SDT members, to provide an early unofficial response to the Data Request. This very small sample of inputs included data from some large and small entities. Although this represented a very insignificant sampling as a statistical analysis, it did show a net gain in the number of assets being classified as critical. No one entity showed fewer assets as critical by using the bright line criteria included in the draft Data Request.

On Tuesday morning, John Lim provided an overview of the work by the CIP-002-4 sub-team in refining the CIP 002-4 draft taking into account the inputs received during the Pittsburgh meeting. He noted that following its review and refinement at the Chicago meeting, the SDT will seek to adopt the revised draft CIP-002-4 standard and provide a draft to NERC staff for their review and proposed edits. In Winnipeg, the SDT will review and analyze industry's responses to the NERC Data Request, review NERC staff edits to the draft CIP 002-4 standard text, and review and refine several associated documents including: an implementation plan, a guidance document (including rationales for Attachment 1 criteria), and a summary of industry informal comments on CIP 010 Attachment 2 from which CIP-002-4 Attachment 1 is drawn.

The SDT reviewed and refined each section of the draft CIP 002-4 standard text, and as needed, conducted straw polls on the acceptability of the proposed language. The SDT reviewed, refined, and tested the criteria listed in Attachment 1 of the draft CIP-002-4 standard text, which was prepared in advance of the Chicago meeting. On Thursday morning the SDT unanimously adopted the draft CIP-002-4 standard text as revised for review by NERC staff before the Winnipeg session.

NERC staff (Scott Mix) presented a proposed approach for the CIP-002-4 Implementation Plan to the SDT, which is based on utilizing the currently FERC approved CIP V3 "Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities" document. Since the SDT isn't making any significant changes to the CIP-003 through CIP-009 standards, the only significant addition would be to determine the

implementation for CIP-002-4, which was proposed as the start of the first quarter following FERC approval. Based on the assumptions discussed in the meeting, the starting date for this plan would be July 1, 2011.

This approach was presented to the SDT at the Pittsburgh meeting and then refined based on that discussion. Scott noted that the schedule assumes a FERC order on the last day of a calendar quarter, and therefore the proposed schedule is aggressive, but achievable, and probably meets FERC's expectations. He suggested that a 24-month implementation schedule in all cases would likely not be acceptable to FERC based on past experience. The Chair suggested that following the review and testing of alternative approaches he would look to forming a drafting sub-team to develop a proposed implementation plan for review and adoption in Winnipeg. (See Appendix #7 for the full set of discussion notes).

SDT Member and participant discussion comments on the proposed implementation plan approach touched on: the importance of a communication plan to the industry; the possibilities for FERC approval of the plan; the impact of bright lines on implementation timing questions; the ability to budget for these changes in a timely manner; whether the NERC Data Request information will help guide the implementation plan draft; and the implementation timing regarding nuclear generation facilities.

Following the discussion of the proposed approach, a revised implementation plan concept statement was presented by Scott Mix. The discussion of the revised implementation concept included: clarifying its approach as covering the one time exemption/override for 24 months for newly identified CCAs at newly identified CAs but with all other requirements being consistent with the currently approved implementation plan; factoring in Order 706B requirements and the timing requirements for filing TFEs; and clarifying how this implementation plan would impact or be impacted by the new Urgent Action SAR on CIP 005 that is being drafted. A straw poll on the acceptability of this implementation plan concept did not gain a supermajority of support (2/3s) from the SDT.

Following the straw poll the SDT identified and discussed the following potential alternative approaches:

a. Implementation plan would require identification of CAs within 1 quarter and CCAs within 4 quarters of its approval. Existing Newly Identified CCA Plan could be used, but the clock would not start for these new CCAs until 4 quarters (12 months) after approval
b. Develop a new implementation plan that allows:
    1. 24 months for implementation of Newly Identified CCAs at New CAs and
    2. Uses the existing implementation plan criteria for the Newly Identified CCAs for New CCAs at existing CAs

c. Keep the existing Newly Identified CCA Implementation Plan but add one quarter to Scott Mix's original plan for the effective date

d. Develop a one-shot/one time exception of 18 months (for specific circumstances) with a sunset to the existing implementation plan schedule
e. Provide six months to identify new CCAs and 24 months to implement compliance for the Newly Identified CCAs.

SDT Member and participant discussion of the potential alternatives included: clarifying the impact and pros and cons of each alternative approach in terms of the possibility of delaying FERC's approval; the observation that the issues affect mostly generation with some transmission; considering these options from an audit enforcement perspective; the visibility of a clear date for compliance is critical to show movement forward on implementation; and less effort to justify changes if tied to the already FERC approved implementation plan. The consensus was that the SDT had reached general agreement on the implementation plan concepts, but hadn't settled on the length of time allowed for compliance. Building on this discussion, the following revised concept was presented:

- For the initial application of the "bright lines" in CIP 002-4, CCAs at newly identified CAs will be compliant at 24 months from identification (includes 706B items and TFEs)

- By the effective date of the CIP-002-4 standard (the first day of the second full calendar quarter after regulatory approval), the registered entity will need to identify its CAs and CCAs and has xx months from that date to be compliant with CIP-003 through CIP-009

- For subsequent application of the "bright lines" in CIP-002-4, CCAs at newly identified CAs will be compliant according to the existing Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities

- For all implementations of Newly Identified CCAs at existing CAs, the existing Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities will apply as it currently exists.

The Chair and Vice Chair suggested that there was now enough input for a drafting sub-team to prepare a new implementation plan proposal, and volunteers for a drafting sub-team were solicited to develop a plan and bring it back for the SDT's consideration in September. The following members agreed to join the implementation plan drafting sub-team: Sharon Edwards, Phil Huff, Dave Norton, Dave Revill, Scott Rosenberg, and Kevin Sherlin. Mike Keane (FERC) and Scott Mix also asked to participate. Joe Bucciero will facilitate the discussions.

On Tuesday morning, Phil Huff presented a draft project schedule for CIP-010 and CIP-011, which had been circulated to the SDT prior to the meeting, and asked Allen Mosher to provide the Team with any preliminary feedback prior to its fuller discussion and proposed adoption on Thursday. Phil reviewed the draft project schedule that includes a

posting for 45-day formal comment period in late May 2011 and with no informal postings between January and May anticipated. This approach is based on the SDT's experience and feedback from industry earlier this year with CIP-010 & CIP-011. Mr. Mosher suggested the SDT may still want to consider an informal comment period. The Chair noted the SDT's hope and expectation is that if NERC can develop a good communication plan, it can help prevent or minimize the industry's confusion and reduce the anxieties as well as allow for some informal feedback. The SDT will be focused on providing clear requirements for the standards, along with an explanation of the rationale, and build on multiple rounds of formal comment. The draft schedule proposes three rounds of comment and balloting.

On Thursday afternoon, the SDT took up the review of the schedule and tasks for completing its work on the CIP 010 & 011 standards. There was an extended SDT member and participant discussion that covered three broad issues: agreeing on the SDT schedule; preliminary work on next phase; and a deeper issue of the approach to drafting during the next phase.

The discussion on Thursday afternoon covered the following topics: schedule; industry confusion vs. communication; clarification of SDT deliverables- short and long term; sub-team role in setting out proposed approach for full SDT review; SDT organization and management in 2011; clarification of the SDT's overall approach to CIP and validating the work to date; the role of security and costs in designing the CIP standards approach; clarification of FERC's direction to the SDT; clarification of the problem the SDT is addressing- including reviewing the original SAR; NERC's investment and expectations of the SDT in getting the job done; conflicting industry and regulator expectations; and the need for a high level of communication with the industry in 2010 and 2011.

On Friday morning, John Lim reminded SDT members of the importance of working together as a team. Phil Huff offered two new motions describing a process for moving forward on foundational concepts based on Thursday's discussion. The first motion was approved by a voted of 16-1, and the second motion was unanimously approved by a vote of 17-0.

1. The CSO706 SDT will prepare a complete package for initial posting to the industry for consideration and ballot in July 2011, in response to FERC Order 706, with the expectation of ballot body approval and filing to FERC by the end of the year 2011. This is contingent upon the SDT being allowed to complete this work without major redirection of SDT efforts.

2. The CSO706 SDT will form a sub-team to develop a framework for presenting and scoping cyber security requirements for preliminary delivery in October 2010 and completion in December 2010. This deliverable would include the form of the standards and the basis by which the requirements are written and applied. The output of this team would go before the full SDT for review and

approval. This task would not include the actual development of security requirements.

The Chair asked for volunteers for the Framework Sub-Team and the following members responded: Dave Norton (Lead), Joe Doetzl, Phil Huff, Doug Johnson, Dave Revill, Jon Stanford, and John Van Boxtel. In addition, Mike Keane and Scott Mix will join and Joe Bucciero will serve as facilitator. It was agreed that Joe Bucciero would send a note to those members of the SDT not present asking for others who might want to volunteer.

Following the vote, the SDT agreed on the following direction to the current CIP-011 Sub-Teams: the sub-teams need to prepare and finalize the responses to industry comments on CIP-010 & CIP-011 as well as the workshop comment summaries so these documents can be posted in October and recognize industry's investment into those comments.

On Friday, Scott Mix provided an overview of the CIP 005 Urgent Action SAR and the process to date. He urged individual members to provide their comments when the SAR is posted and raise issues they discussed at this meeting.

The Chair and Vice Chair discussed with the SDT the Winnipeg agenda that will start on Wednesday morning, September 8 through mid-morning Friday, September 10. The meeting will include the final adoption by the SDT for posting of CIP-002-4, a review of the NERC Data Request results to determine whether any criteria need changes, review of a CIP 002-4 comment response document drawn from the relevant comments on Attachment 2 of the CIP-010 informal posting, and preparation for the September 23 webinar. Brian Newell has offered to create a database that the SDT can use to calculate Data Request question totals. This will be sent around for the SDT to review in advance of the Winnipeg meeting. Herb Schrayshuen, NERC, noted the discussion of whether additional project management service is needed. The Chair suggested that the SDT develop a better clarification of scope for CIP 010 and 011 after December, 2010 discussions of the Framework sub-team and that a review for such a requirement be made at that time.

The Chair asked Joe Bucciero to send out a recurring meeting invitation to put on everyone's schedule for four hours during the fourth week of each month. The first session will be scheduled for Thursday, August 26, from 12-4 p.m., Eastern time. The Chair and Vice Chair thanked Doug Johnson for the excellent hosting and accommodations, especially the Blue Angels demonstration.

Meeting adjourned at 11:15 a.m.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

25TH DRAFT MEETING SUMMARY
Cyber Security Order 706 SDT- Project 2008-06
Chicago, IL
August 10-13, 2010

I. AGENDA REVIEW, UPDATES, WORKPLAN, SCHEDULE AND REVIEW OF NERC DATA REQUEST

A. Agenda Review and Meeting Logistics

John Lim, Chair & Phil Huff, Vice Chair of the CSO 706 SDT welcomed members and other participants to Chicago and thanked Doug Johnson for hosting the meeting who reviewed the logistics for the meeting. Joe Bucciero conducted a roll call (See Appendix #2) and reviewed the antitrust and public meeting guidelines (See Appendix #3) with the meeting participants. On Thursday morning, the SDT unanimously adopted the July 13-16 meeting summary with edits presented by John Van Boxtel. The Chair announced that Frank Kim has resigned from the SDT for professional and personal reasons but will follow the SDT progress and contribute comments where possible. This means that there are 25 SDT members resulting in a quorum rule of 17 members to conduct business. The meeting began with a quorum 17 members in the room and 2 members participating by phone/ready talk.

John Lim reviewed the proposed meeting objectives noting the following three outcomes needed at this meeting: 1. Adopt draft CIP 002-4 – everyone agreeing with language and criteria and utilizing the data request responses of some of the member companies as a guide; 2. Agree on a schedule for CIP 010 and 011 to deliver to the Standards Committee; and 3. review the Sub-team summaries of informal comments and the workshop input. The facilitator Bob Jones reviewed and the SDT agreed to the proposed timed agenda.

The Chair noted the opportunity of the SDT to hear from Allen Mosher, Chair of the Standards Committee on the SDT's efforts and progress.

B. Updates on other related cyber security initiatives- *NERC Staff and SDT Members*

Scott Mix provided the SDT an update on the urgent action CIP 005 SAR. Once the Standards Committee approves then it will go out to ballot for SDT formation. The proposed revisions may land about the same time as this groups work on CIP 002. It may be helpful to post together or at the same time. The intention is to include a compliance guidance document that is still being developed with input from companies of differing levels. They are still putting together the SAR

Member Comments

- I would like this group to have a look at this before it is pushed through – within the rules but think this group should look at it.
- When is the CAN is issued? When is it guidance versus compliance? It seems multiple people are now writing requirements.
- Allan Mosher noted that compliance is written by NERC staff, reviewed with regions and others – it is compliance guidance to regional staff for understanding for compliance purposes. The Standards Committee is working on setting up a one-stop shop for interpreting standards though interpretations could still be formal or informal.
- This seems like a back door approach to compliance requirements.
- Response to unofficial request for interpretation that was pulled without interpretation – I will submit request in the near future – need formal guidance.
- The CAN process is causing concerns for the industry as a whole. Even if it provides guidance for auditors, it seems that it adds requirements not necessarily in the standard.
- The new SAR seems closely related to our activities.
- There is a different definition of "critical." NERC needs a methodology for what is most critical for reliability – not sure what the background is for that SAR.
- Note that regional entities do not own "assets."
- If it is "critical" it needs to be uniform across industry with a common list. Industry would support unifying such a list to limit confusion and number of compliance officers.
- Unlikely that industry would support lining up critical assets with critical facilities at this point.

Keith Stouffer reported that latest version of the NISTER report was released last week for review. The person leading that effort has moved to FERC. Dave Norton noted that a recent report of insider incidents showed that they were up 28% last year.

C. Standards Committee Chair Comments to the SDT

Allen Mosher addressed the SDT noting the atypical external pressures on the Team related to the nature of the CIP changes the Team has been charged to develop and the level of scrutiny due to the high degree of interest in Washington among agencies and congress in Cyber security. He noted the industry's high level of concern regarding compliance issues as NERC is in the midst of trying to revamp its compliance system and culture.

He urged the SDT to preserve the two-track approach to developing the CIP standards noting this is an important opportunity to prove to political and regulatory interests that the industry can produce effective cyber security standards and do it promptly. Completing the CIP 002-4 process by end of this year will help demonstrate to Congress that the industry

capable of self-regulation. There is no dispute about the need for a higher degree of regulation of cyber security or statutory authority, though some still question how far that authority should go. By being successful on CIP 002-4 we can take some of the wind out of the sails of those arguing to simply drop the NIST into the CIP security standards. This would cost industry billions of dollars without a guarantee of better security for the grid. We need to provide an effective industry developed alternative or the continued deference to industry self-regulation in terms of NERC's standards process will be in question. If we fail here, it may mean loss of authority in other areas – cyber security is just the initial test.

SDT Member Questions:

Members expressed frustration with the SDT's re-direction on CIP 002-4 noting that a political problem has been assigned to a technical group to solve. There was discussion of the perception of some in the industry and those observing this effort that political drivers have resulted in a deadline to identify more critical assets but that CIP 002-4 is not enough.

Mr. Mosher reiterated that he believed that CIP 010 and 011were the right model and he hoped the SDT would be focusing soon on that task. He acknowledged the CIP 002-4 approach was not a risk based assessment, but stressed the importance of analyzing the results of the data request regarding "bright lines" in September to determine whether there will be an increased number of CAs and CCAs. He also acknowledged SDT and industry concerns about creating a workable transition to CIP-010 and 011 and the concerns with compliance and auditing confusion with multiple CIP versions in play. The SDT also discussed that for cyber security the size of the asset may not be the controlling factor. There was also acknowledgement of the need for uniformity of an industry approach. Finally a phase-in period for a risk-based system anticipated by CIP 010 and 011 should be developed to allow the industry to get controls in place.

Mr. Mosher noted his target and focus is on the CIP 010 and 011. He noted that the industry needs an interim step to fix the most egregious gaps in identifying assets in current CIP system but it does not make sense for the SDT to stop at 002-4. The hope is the NERC Data Request results will help guide the team in determining what percentage of increased assets is the right amount or target. It was noted that NERC President Gerry Cauley stated that success in the short term for the SDT would be that industry adopts bright line criteria that can be technically supported. Technical justification for each bright line will be an important part of the SDT discussions going forward vs. the exact number of CAs.

In the last meeting the SDT adopted plan to complete 002-4 as soon as possible and no later than December in order to get back to work of CIP 010-011 development.

At the end of the day on Tuesday, Allan Mosher thanked the SDT for what it is doing in working as a drafting team to develop consensus. He suggested it is making significant progress on something that is very hard to do. He urged them not to fix it for a member's sector or company, but for the industry as a whole, i.e. a set of criteria driven by reliability

that you can justify with engineering. He acknowledged the heartburn on CIP 002-4, but suggested it will make it easier for the SDT to do CIP 010 and 011. Many in the industry are concerned about the big jump to the latter. However, it is the path we are on and you can make it work by explaining why we are doing it and advocating for its adoption.

D. NERC Vice President and Director of Standards Comments to the SDT

John Lim introduced Herb Schrayshuen, the new NERC Vice President and Director of Standards, who joined the SDT on Thursday morning. He thanked each member for their service and understood and welcomed their questions, recognizing the tensions in the process and feelings about how the SDT has been treated over the past couple months. He noted that process is important but so is delivery. Responding to a question of what success looks like for the work of SDT, he suggested a standard that helps the industry deal with deficiencies in the current standards and delivers results that improve the cyber security posture for the grid. He promised to help the Team secure the necessary resources and assistance and help them get their job done successfully. In response to a question of whether there was some number required to be covered in terms of critical assets under CIP 002-4, Mr. Schrayshuen suggested that the NERC Data Request results will provide some guidance but that there will need to be a technological basis for number of assets covered. He urged the SDT to keep in mind the industry frame within which they are working and the reality that the SDT is going to get more "help" than you may want and that the SDT is on a pragmatic schedule spurred by industry input, although not an ideal schedule from the SDT perspective.

He noted that some members of the SDT have superior knowledge in terms of security clearances and may have concerns about what security approaches work and don't work, e.g. data on frequency issue. This may create an uneven base of knowledge which impedes progress on problem solving. On another SDT, the dynamic within the team led to failure at the ballot. Issues were voiced in drafting team process but not resolved so members left the Team prepared to vote no in the ballot. The drafting team had thought their job was done by simply voicing concerns and then expressing opinions to the industry and voting no on the resulting proposed standard. The lesson is that it is a breakdown of the process for a team not take an issue and try to resolve it here, and when all is said an done, make a team decision informed by this problem solving.

The culture of compliance versus culture of reliability is an important debate on how to approach cyber security. He noted that we cannot comply our way to reliability. Quality control plan training has started and we are looking for conflicts between standards. My last job was compliance manager and I got a zero finding showing it can be done. Experience with the audit process should influence results but not at the expense of lowering the bar. The SDT should try to use it to inform and improve standards.

Mr. Schrayshuen noted that NERC will soon release a new standards approach, including how to prioritize. We are trying to put everyone in the same room, including FERC, to create one list of priorities moving forward in an effort to avoid redirects.

Member Comments on the SDT's Challenges

- **What is success for CIP 002-4?** We were on a process to deliver broad coverage, when the team was redirected to a bright line criteria –with a challenge to deliver by end of this year something that the industry must support and regulators have to see as a real "improvement." Do we have a certain number of assets identified to equal "success"?
- Taking your position at an interesting point – this is a whole new thing and responding in an atmosphere of fear – trying to address 100 years of effort with new threats – cyber security overlay with two parts for generation and for transmission worlds resulting in a complex puzzle. Mr. Schrayshuen noted he understand distinctions between them.
- Industry in better shape now from standards and compliance. However, standards Committee and CCC don't have substantive expertise on cyber issues. Also need better subject matter quality control on auditor hires.
- **System vs. Assets Approaches.** The SDT has struggled with two different approaches: a systems focus versus an assets and sites focus. In essence, by analogy, we are being asked to say which airports are the most important vs. protecting the air traffic control system. Mr. Schrayshuen noted he favors an incremental progress to improvement – don't go for "the bridge too far" but don't preclude improved approaches in the future. There may be a need to prioritize in terms of timing – not everything can be important at the same time – build toward a better long term approach.
- Size matters for impact optics, but vulnerability can come from smaller venues.
- **Physical Security.** We are hearing that many are interested in physical security and concerns about how that issue can rearrange priorities. Physical securities over the next five years. That is not within scope. Prioritization is predicated by someone writing a SAR. Since no SAR has been submitted yet on physical security, we cannot assess priority.
- **Culture of Compliance and Standards.** There is a disconnect between standards writing and the nits of compliance. The latter doesn't add security but it does add huge expense. We have to worry about how an auditor will interpret, rather than focus on most reasonable interpretations, (e.g. antivirus on a switch when there has never been a virus on a switch because auditors are asking for it).
- There is growing unrest in the industry about compliance which will need to be addressed sooner rather than later. Inconsistency between regions is one aspect. FERC participation in audits is new as well. The industry looks to requirements as the yardstick, but now having to look at things from FERC that may not yet be in the

requirements. It is increasingly hard to figure out what the yardstick is for measuring compliance.

- Auditing process needs to be better coordinated – need to know the limits, auditors can go anywhere and we can't standardize our compliance programs
- Compliance with TFE process is not equal to the return of effort – cited for insufficient senior manager designation – that is not helpful.
- Many SDT members have gone through audits during the drafting process and they return with a heightened concern about the wording of standards.
- No matter what words are used in the standards, compliance agonizes over the words rather than the intent – examples of the absurd and the pain level and frustration of industry is immense –
- Affects reliability if just focused on paper work.

E. Briefing on the NERC Data Request

On Wednesday morning, NERC staff Howard Gugel reviewed with the Team the industry comments and the NERC responses and changes on the draft NERC Data Request *(See Appendix #4)/*
He then presented a summary document showing the results of the six entities whose SDT members responded which included some large and small entities. Although this is a very insignificant sampling as a statistical analysis, it does show a net gain in cyber assets. No one entity showed fewer assets by using the bright line requirement. The SDT will need to categorize by type for the full set in September. The Chair encouraged members to think of questions we could ask of the data that would help our analysis of CIP 002-4.

Member Comments

- Looking at high category as equal to "critical." The SDT would be interested in seeing what would be "medium" as a distinction with 010-011 versus CIP-4. This should include high and medium and be a positive number.
- We need to see if we can find the number of "high" – how many more sites would be subject to the standard as a "high?" A: the data from the Data Request should help define that – but does not identify "cyber" assets.
- We will need to document the technical justification for each element of our work
- Responses are in numbers not text to allow for quick compilation in spread sheet form for analysis
- No one listed anything new in category 1.2 – nothing new additional under bright line – none of the six members listed nuclear, though some have nuclear facilities.
- Catch data on switchyards to nuclear? Yes, as the interface which is important to us.
- Generation control centers only exist in "high" or "low" - not "medium" – intended?

II. SDT CIP 002-4 STRAWMAN DOCUMENT REVIEW

A. Overview

John Lim provided an overview of the work by a sub-team in refining the CIP 002-4 draft following the Pittsburgh meeting. *(See, Appendix # 6)* He noted that following its review and refinement at this meeting, the SDT will seek to adopt it to provide a draft to the NERC staff for their review and proposed edits. In Winnipeg the SDT will review and analyze industry responses to the Data Request, review the NERC staff edits to the CIP 002-4 with the VSLs and VRFs, and review and refine several associated documents including: an implementation plan, a guidance document including rationales for Attachment 1 and a summary of industry informal comments on CIP 010 Attachment 2, on which CIP 002-4 Attachment 1 is based.

Phil Huff and Howard Gugel took notes on possible rationales and justification and checked with the SDT periodically following discussions to clarify the justifications. Their notes will be used to develop the justification draft following this meeting.

B. Review and Refinement of the Strawman CIP 002-4

The SDT reviewed each section of the CIP 002-4 strawman, and as needed, conducted straw polls on the acceptability of the language. The final adopted text is included in Appendix #5 and a full set of SDT comments and polls is included in Appendix #6.

1. Applicability

Distribution Provider

***Straw Poll*: Support removing distribution provider from the applicability section. Yes-15 No-4 (74%)**

SDT comments included: helps to improve possible industry acceptance in balloting; Version 3 did not have this; wait for CIP 010 and 011 to re-introduce as responsive to Order 706 and could be an attack vector will need protection

4.2: SDT question: What was the rationale for taking out this section? It is covered under 706b – no longer exempt.

4.2.1 - last sentence added
***Straw Poll*: Favor removing "However all access points to the ESP are not exempt.": Yes-16 No – 0 (100%)**

The SDT discussion before the straw poll included the following points: this comment belongs to the requirements; this clause is already in CIP003; why include one item here but not serial dial up; and, clarifying what is on or off a list, not the protections required.

2. CIP 002-4 Requirements

John Lim noted that the SDT agreed in Pittsburgh to delete the original R1. This is modified version of the original R2 in Version 3 which was accepted in Pittsburgh.

R1. Critical Asset Identification — Each Responsible Entity shall develop a list of its identified Critical Assets determined through an annual application of the ~~create, maintain and review on an annual basis, a list of its Critical Assets identified according to the~~ criteria contained in *CIP-002-4 Attachment I – Critical Asset Criteria*. The Responsible Entity shall review this list at least annually, and update it as necessary.

Re-insert the original R1 language on annual review
***Straw Poll*:** support using the original language (underlined above):
Yes - 17 No – 0

Discussion before the straw poll resulted in some edits to make the statement clearer. Other comments before the straw poll included: whether to leave "annual" as it is here or whether to stick with the original R1 language; should acquisition of new assets be included here; and should this address including new asset as a CA and not waiting until the end of the annual period

R2. Critical Cyber Asset Identification — Using the list of Critical Assets developed pursuant to Requirement R1, each Responsible Entity shall develop a list of associated Critical Cyber Assets. ~~essential to the operation of the Critical Asset. Examples at control centers and backup control centers include systems and facilities at master and remote sites that provide monitoring and control, automatic generation control, real time power system modeling and real time inter utility data exchange.~~ For each group of generating units (including nuclear generation) at a single plant location identified in Attachment 1, criterion 1.1, the only Cyber Assets that must be considered are those shared Cyber Assets that could adversely impact the reliable operation of any combination of units that in aggregate exceed Attachment 1, criterion 1.1 within 15 minutes. The Responsible Entity shall review this list at least annually, and update it as necessary. For the purpose of Standard CIP-002-4, Critical Cyber Assets are further qualified to be those having at least one of the following characteristics:

Member comments on R2 included: changes made in R2 need to be consistent with Attachment 1; change "essential to operation" because it may leave too much flexibility

for entities; NERC Glossary definition of CA includes "essential" to operations; worried about how rather than what they are doing; moving it is a way of mitigating the risk; examples and definitions should not be in the requirement; and add a box explaining it is redundant and is covered by definition.

The SDT tested the following changes with straw polls:

***Straw Poll*:** Remove "essential to operation of the Critical Assets":
Yes - 13 No – 6 (68%)

***Straw Poll*:** Remove Examples sentence –
Yes - 15 No – 4 (79%)

- Opposed. The SDT should take minimalist approach to editing so as to avoid comments on why language is removed. We can address many of these in CIP 010-011.

***Straw Poll*: Put Last sentence above**
Yes 19 No- 0

- M1 was removed earlier and needs to be noted in the final redline

3. Critical Assets Criteria- Attachment 1

The SDT reviewed, refined and tested the criteria listed in the CIP-002-4 strawman prepared in advance of the Chicago meeting. As a result of the Chicago discussion, straw polling and refinements to the criteria taking place on Tuesday and Wednesday *(See Appendix 6 for the SDT discussion notes and straw polls)*, the following 16 criteria were adopted unanimously by the SDT on Thursday morning for review by NERC staff before the Winnipeg session:

1.1. A generating unit or group of generating units (including nuclear generation) at a single plant location with an aggregate highest rated net Real Power capability in the preceding 12 months exceeding the lowest Contingency Reserve identified over the preceding 12 months by the Reserve Sharing Group or the Balancing Authority if it is not a member of a Reserve Sharing Group, at the time the CIP-002 is reviewed.

1.2. Any reactive resource or group of resources at a single location (excluding generation Facilities) having aggregate net Reactive Power nameplate rating of 1000 MVARs or greater.

1.3. Generation Facilities that the Planning Coordinator or Transmission Planner designated as required for reliability purposes.

1.4. Each Blackstart Resource identified in the Transmission Operator's restoration plan.

1.5. The Facilities comprising the Cranking Paths and initial switching requirements identified in the Transmission Operator's restoration plan.

1.6. Transmission Facilities operated at 500 kV or higher.
1.7. Transmission Facilities operated at 300 kV or higher at stations interconnected at 300 kV or higher with four or more other stations in the Eastern Interconnection or the Western Interconnection.
1.8. Transmission Facilities operated at 200 kV or higher at stations interconnected at 200 kV or higher with four or more other stations in the Texas Interconnection or the Quebec Interconnection.
1.9. Transmission Facilities that, if destroyed, degraded, misused or otherwise rendered unavailable, violate one or more Interconnection Reliability Operating Limits (IROLs).
1.10. Flexible AC Transmission Systems (FACTS), that, if destroyed, degraded, misused or otherwise rendered unavailable, violate one or more Interconnection Reliability Operating Limits (IROLs).
1.11. Transmission Facilities providing the generation interconnection required to directly transmit generator output to the transmission system that, if destroyed, degraded, misused, or otherwise rendered unavailable, would result in the loss of the assets identified in Attachment 1, criteria 1.1 or 1.3.
1.12. Transmission Facilities identified as essential to meeting Nuclear Plant Interface Requirements.
1.13. Special Protection Systems (SPS), Remedial Action Schemes (RAS) or automated switching systems that operate BES Elements that, if destroyed, degraded, misused or otherwise rendered unavailable, violate one or more Interconnection Reliability Operating Limits (IROLs).
1.14. Common control system(s) that are capable of performing automatic load shedding of 300 MW or more.
1.15. Any control center or control systems, and backup control center or backup control systems, used to perform the functional obligations of the Reliability Coordinator or Balancing Authority or Transmission Operator.
1.16. Any control center, or backup control center, used to control generation that is identified as a Critical Asset, or used to control generation greater than an aggregate of 2300 MWs in a single Interconnection.

C. CIP 002-4 Implementation Plan

1. Initial Proposed Approach

Scott Mix reviewed the a proposed approach for the Implementation Plan with the SDT which is based on utilizing the currently FERC approved CIP implementation plan and included the following components:

Proposed Effective Date Language

- "The first day of the first full calendar quarter after applicable regulatory approvals have been received; or, the first day of the second full calendar quarter after BOT adoption in those jurisdictions where regulatory approval is not required."
- *Assuming* FERC acts within one quarter, issuing an order on March 31, 2011, the effective date would be July 1, 2011 in both the US and Canada.
- Outreach to inform industry to start identification process upon filing.

The Rest of the Standards

- Since we aren't making changes to CIP-003 through CIP-009, the currently approved "Implementation Plan for newly Identified Critical Cyber Assets and Newly Registered Entities" would apply
- This plan was designed to apply to "Newly registered Entities", and was modeled after the Version 1 Table 4.
- Assuming the previous timeline, the starting date for this plan would be July 1, 2011.

Newly Identified CCA Plan Recap

- The Newly Identified CCA Plan allows:
- •24 months for entities without any Version-3 CCAs
- •For entities with Version-3 CCAs:
- Immediate for Policy, Leadership, Exceptions (CIP-003), Awareness (CIP-004)
- 6 months for Information Protection, Access Control, Change Control (CIP-003), Incident Reporting and Response (CIP-008), Recovery Plans, Backup & Restore, Testing Backup Media (CIP-009)
- 12 months for Electronic Security Perimeter (CIP-005), Physical Security (CIP-006), Systems Security Management (CIP-007), Exercises, Change Control (CIP-009)
- 18 months for Training, Personnel Risk Assessment, Access (CIP-004)

This approach was presented in Pittsburgh to the SDT and then refined based on that discussion. He noted the schedule assumes for a FERC order on the last day of a quarter and suggested the proposal is aggressive achievable and probably meets FERC's expectations. He suggested that 24 months would not be acceptable to FERC based on past experience. The Chair suggested that following the review and testing of approaches he would look to forming a drafting team to develop a proposal for review and adoption in Winnipeg. (See Appendix #7 for the full set of discussion notes.

Member and participant discussion comments on the approach touched on: the importance of a communication plan**;** the likelihood of FERC Approval of the plan; the impact of bright lines on timing questions; the ability to budget for these changes; whether the information from the NERC Data Request will help guide the implementation plan draft; the newly identified CCA plan; and nuclear generation.

2. Revised Approach Concept

Following the discussion of the approach above a revised concept statement was presented by John Lim and Scott Mix providing:

> "For the initial implementation of CIP 002-4, CCAs at newly identified CAs will be 24 months (i.e., follow Milestone Category 1 in Table 2, Implementation Milestones for Newly Identified Critical Cyber Assets) in the IPFNICCAANRE (Add 706B items and TFEs)
>
> For subsequent implementations of CIP 002-4 at newly identified CAs, the IPFNICCAANRE will be followed as written
>
> For all implementation of newly identified CCAs at existing CAs will follow the IPFNICCAANRE as written."

The discussion of the revised implementation concept included: clarifying its approach as covering the one time exemption/override for 24 months for newly identified CCAs at newly identified CAs but with everything else is consistent with existing effort; factoring in 706b and when to file TFEs; clarifying how this implementation plan would impact or be impacted by the new CIP 005 version; covering the need for outages to implement.

Straw Poll on Proposal
Favoring proposed approach to drafting implementation plan
Yes=9 Oppose=4 Abstain=5

3. Alternative Approaches to Developing the Implementation Plan

Following the poll the SDT identified and discussed the following potential alternative approaches:

a. Implementation plan that requires identification of CAs within 1 quarter and CCAs in 4 quarters. Existing Newly Identified CCA Plan could be used (but the clock would not start for these new CCAs until 4 quarters (12 months) after approval

Or

b. Develop a new implementation plan that allows
   1. 24 months for Newly Identified CCAs and New CAs and
   2. Uses the existing Newly Identified CCAs for New CCAs at existing CAs
   3. Keep the newly identified CCA

Or

c. Add one quarter to Scott Mix's original plan for effective date.

Or

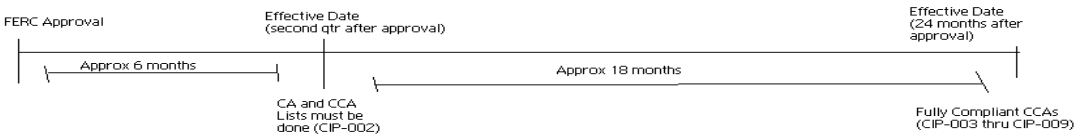
d. Develop a one-shot/one time exception (for specific circumstances) with a sunset to the existing implementation plan schedule.

Or
e. Provide six months for identifying and 24 months to comply.

Member discussion of potential alternatives included: clarifying the impact and pros and cons of each option in terms of the possibility of opening up the implementation plan and delaying FERC's approval; the observation that the issues affect mostly generation with some transmission; consider these options from an audit enforcement perspective; the visibility of a clear date is critical to show moving forward on implementation; It will be easier to justify if tied to the a already FERC approved implementation; general agreement on the concept but we haven't settled on the length for compliance. Following this discussion, over lunch John Lim and Scott Mix drafting the following revised concept:

For the initial application of the "bright lines" in CIP 002-4, CCAs at newly identified CAs will be compliant at 24 months from identification (add 706B items and TFEs)

The effective date of the standard (upon the regulatory approval) the registered entity will need to identify CAs and CCAs within six months and xx months to be compliant with 003-009



4. Implementation Plan Drafting Team

The Chair and Vice Chair thought there was enough input for a drafting team to develop a new proposal and solicited volunteers for a drafting team to bring back for the SDT's consideration in September.

Implementation Plan Drafting Team Volunteers: Sharon Edwards, Dave Revell, Kevin Sherlin, Scott Rosenberg, Mike Keene (FERC), Dave Norton and Phil Huff and Scott Mix.

III. REVIEW AND DISCUSSION OF CSO 706 SDT CIP 010 & 011 DRAFT WORK PLAN AND SCHEDULE

A. Initial Review and Discussion of CIP 010 & 011 Schedule and Workplan

On Tuesday morning, Phil Huff presented a strawman draft 010-011 schedule circulated to the SDT prior to the meeting and asked Allen Mosher to provide the Team with any feedback prior to its fuller discussion and adoption on Thursday. Phil reviewed meeting schedule with approval for posting for 45 day formal comment in late May and with no informal postings between anticipated based on experience and feedback earlier this year with CIP 011 & 012.

Mr. Mosher suggested the SDT may still want to consider an informal comment period. John Lim noted that we have tended to get the same comments for both informal and formal postings and the industry has been confused when the informal draft is incomplete. They might appreciate dealing with as complete a package as possible. He noted the SDT's hope and expectation is that if NERC can develop a good communication plan, it can prevent or minimize the confusion and reduce the anxieties as well as allow for some informal feedback. The Team should be providing what is the standard, along with an explanation of the rationale and build in multiple rounds of formal comment. The draft schedule proposes at least three rounds to build expectation and understanding allowing the SDT to refine and focus on the key issues for industry acceptance.

One company has estimated $150 million to implement CIP 010 and 011 and the chance for companies to provide informal input is vital now that it is mandatory with huge fines potentially. The visibility of this effort is high as is the industry anxiety. For example, one potential unintended consequence may be that companies would shut down marginal plants rather than implement the new cyber security requirements.

Investments in cyber security should be aimed at highest benefit. Some entities are hiring compliance officers to check boxes focusing on the trivial. This is a problem in current CIP 002-009 standards. Cyber security is not vegetative management. Rather it is fundamentally different effort in terms of enforcement. The industry may need a system of certification. There is anger out among entities about compliance with CIP 002-009. We may need to look at the FSMA model for certification methodology and lessons learned.

How do we agree on a schedule if we do not have general acceptance of our approach to CIP 010-011?

B. 2nd Review and Refinement of Workplan and Schedule for CIP 010-011

On Thursday, the SDT took up the review of the schedule and tasks for completing its work on the CIP 010 & 011. Phil Huff reviewed with the Team the key highlights of the draft schedule:

- First posting for Formal Comment is proposed for May 31, 2011.
- This assumes an aggressive NERC industry communication campaign to support the effort prior to posting for formal comment.
- By December the SDT will turn its full time attention to CIP 010 & 011.
- By March the SDT will send a package for review with NERC staff, compliance and legal.
- Review in April any edits and Approve in May.

There was and extended SDT member and participant discussion that covered many issues (*See Appendix #7 for a detailed version of the comments).* Stu Langton suggested there was an important discussion of three distinct issues: schedule; preliminary work on next phase; and deeper issue of approach to drafting during the next phase. We may need someone to work on and present a suggestion on the drafting approach for the next phase in Winnipeg.

The discussion on Thursday afternoon covered the following topics:

- Schedule & industry confusion and communication
- Clarifying SDT deliverables- short and long term
- Sub-team role in setting out proposed approach for full team SDT review.
- SDT organization and management in 2011
- Clarifying the SDT's overall approach to CIP and validating the work to date
- The role of security and costs in designing the CIP standards approach
- Clarifying FERC's direction to the SDT
- Clarifying the problem the SDT is addressing- including reviewing the SAR
- NERC's investment and expectations of the SDT getting the job done.
- Conflicting industry and regulator expectations
- The need for high level of communication with the industry in 2010 and 2011.

On Friday morning, John Lim reminded team members of importance of working together as a team. He then withdrew his motion on the proposed CIP 010-011 schedule from day before for the sake of inviting another motion that may be clearer and reflect the good discussion points from yesterday.

Phil Huff offered two motions (seconded by Dave Norton) that describe a process for moving forward on foundational concepts discussed yesterday. In general, the motion moves the posting date for formal comments back to July, 2011 and suggests taking time in front end to set foundation before launching into the requirements in January 2011. This will provide for at least three more months for the foundation discussion. In the course of

discussion of the motion, there were several amendments to the language of motion accepted by the maker and the following motion was adopted with 16 members in favor and 1 opposed:

1st Motion for CSO706 SDT Project Schedule

> **The CSO706 SDT will prepare a complete package for initial posting to the industry for consideration and ballot in July 2011, in response to FERC Order 706, with the expectation of ballot body approval and filing to FERC by the end of the year 2011. This is contingent upon the SDT being allowed to complete this work without major redirection of SDT efforts.**

Phil Huff offered his second motion (seconded by Dave Norton) that established a framework sub-team to be chaired by Dave Norton and will report back to the SDT in October for initial input and then in December for review, refinement and adoption of the CIP 010 & 011 approach. The discussion that followed noted that the motion draws on the essence from Phil's initial proposal (*See Appendix 8).* The following motion was adopted unanimously with 17 members in favor and none opposed:

2nd Motion Process for Implementing CIP 010-011 Schedule- Framework Sub-Team

> **The CSO706 SDT will form a sub-team to develop a framework for presenting and scoping cyber security requirements for preliminary delivery in October 2010 and completion in December 2010. This would include the form of the standards and the basis by which the requirements are written and applied. The output of this team would go before the full-team for review and approval. This task would not include the actual development of security requirements.**

The Chair asked for volunteers for the Framework Sub-Team and the following members responded: Dave Norton (Lead), Joe Doetzl, Phil Huff, Doug Johnson, Dave Revill, Jon Stanford and John Van Boxtel. In addition, Mike Keane and Scott Mix will join and Joe Bucciero will serve as facilitator. It was agreed that Joe Bucciero would send a note to those members of the SDT not present asking for others who might want to volunteer.

Following the vote the SDT agreed on the following direction to the current CIP-011 Sub-Teams: We need the output from the sub-teams on responses to industry comments and workshop comment summaries so they can be posted in October and recognize industry's investment into those comments.

IV. DISCUSSION OF URGENT ACTION SAR FOR CIP 005

Scott Mix provided an overview of the SAR and process to date. He noted the following link in the Board of Trustees packet that has the SAR information: http://www.nerc.com/docs/standards/sc/sc_081210a_complete_agenda_draft.pdf

He noted the draft Removes R2.4 and a new requirement R6 on remote access controls – attempts to capture what you do with cyber stuff from outside that needs access inside for remote maintenance and support. This an attempt to bring sanity to the issue and discusses process, procedures and who can do what. The 6.3 protocols for access through ESP still need a guidance document to explain the architecture. R6.5 was deleted – list of technical requirements of what you need to do to those remote sites to secure them. Next steps in urgent action will post the SAR and proposed modifications for comment but not sure if informal or for ballot and formal comment.

Member Comments

- Have not seen SAR – concern about requirements in CIP 006 that send you back to CIP 005 – would SAR allow us to clarify R2 and R3 to say you do not have to create an ESP, and would anything here create difficulty with physical access control?
- Effort was to narrowly address issue in the SAR, not open it up to broader issues. You would protect like an ESP without necessarily creating an ESP.
- Physical access control spans geography – treat like an ESP but not create one –
- Send me an email of your and others experience in audits and can look at CAN interpretation.
- Huge issue for our budget and WECC auditors have a different interpretation.
- Multiple ways to address the issues in R6 draft – guidance to auditors will be important
- It says what ought to be done, not how to do it – expectation that multiple correct answers to get the results – auditors need to understand there are multiple possible answers and not just the one they would have done themselves
- R 6.5 – original team intent – meant that outside device needed protections – if R 6.5 is out then need support contracts should require support to follow rules.
- How do you audit it if it is not in the standard?
- Put into guidelines at a minimum – also 6.3.1, host inside the end point or something else? Could create problems as written.
- Can't look at encrypted info as it crosses?
- Members should consider providing comments to spur team to look at the issue
- We are making conforming edits – is that included here or vice versa?

- NERC staff proposes references 005 to this posting. NERC will have to conform the two so not to complicate this teams work and avoid auditing confusion
- Any of the language from CAN or our work make it into this version? Do we need to do something in our version to incorporate the CAN? Would the CAN end up defining the requirement?
- This process will potentially create implementation and audit questions – what can we live with from an operational perspective – CAN addresses something we did not get to yet – not sure we have time and ability to fix it now, but may when we go back to 010-011 may need to consider it as input to that later work.
- How does this integrate with 004? Does it creates double jeopardy? CIP 003 lays out the governance, CIP 004 says who can have access, CIP 005 says how they can have access.
- CIP 004 seems to overlap with changes presented here – should we look at cleaning up the potential mess of remote access?
- SDT members should use the process for providing comment to get the new group to look at it – official documentation to ensure they look at it.
- Does the SAR allow them to look at CIP 004 to address?
- When will it be posted? Not sure of the mechanics of the posting, but the NERC BOT has authorized to post and the announcement may be soon, sometime new week.
- Who is working on conforming these two efforts? The industry will not care who it comes from. This should be put on the webinar call in September to educate the industry. It is a very complex topic.
- There will be comments on CANs too.
- Need to keep focus more narrow – and suggest Ed Goth as author of the SAR participate in the webinar and provide a one page summary *(Scott Mix will reach out to Ed)*
- Looking at interactive remote access or any remote access – the controls offered here all seem aimed at interactive remote access – does not say support and maintenance
- File a comment for clarification

V. NEXT STEPS AND ASSIGNMENTS

The Chair and Vice Chair discussed with the SDT the Winnipeg agenda. The meeting will start Wednesday morning, September 8 through mid-morning Friday, September 11. The meeting will include the final adoption by the SDT for posting of 002-4, a review of the results from the NERC Data Request and their tabulated database results to determine whether any criteria need changes, and review of a CIP 002-4 comment response document drawn from the relevant comments on Attachment 2 of CIP 010 informal posting.

Brian Newell has offered to create a database that the SDT can use to calculate the NERC Data Request question totals. This will be sent around for the SDT to review in advance of Winnepeg.

Herb Schrayshuen, NERC, noted the discussion of whether additional project management service is needed. The Chair suggested that the SDT will develop better clarification of scope for CIP 010 and 011 after December, 2010 discussions of the Framework sub-team and that a review of the need would be performed at that time.

The chair also noted the need to start working on planning for theSDT CIP 002-4 webinar to be conducted on September 23rd from 11:00-1:00 EST. It makes sense that the CIP 002-4 subteam lead the webinar presentation(s) with other SDT members providing technical support and NERC and others to provide industry support. A proposal going forward will be reviewed and adopted the Winnipeg meeting.

The Framework sub-team is planning to meet approximately twice a week on Monday and Thursday afternoons starting the week of August 23 for approximately 90 minutes to accomplish its objectives. Joe Bucciero will be sending out a scheduling tool to select the best meeting times for most people to participate.

Stu Langton noted that last month the SDT talked about setting aside a once a month conference call midway between their meetings which could be cancelled if not needed. The Chair asked Joe Bucciero to send out a recurring invitation to put on everyone's schedule for four hours. The first session will be scheduled for Thursday, August 26, from 12-4 p.m., EDT.

The Chair and Vice Chair thanked Doug Johnson for the excellent hosting and accommodations, especially the Blue Angels demonstration.

Meeting adjourned at 11:15 a.m.

Appendix # 1— Meeting Agenda

Project 2008-06 Cyber Security Order 706 SDT
Draft 25th Meeting Agenda
August 10, 2010, Tuesday- 8:00 AM to 5:00 PM CDT
August 11, 2010 Wednesday- 8:00 AM to 5:00 PM CDT
August 12, 2010 Thursday- 8:00 AM to 5:00 PM CDT
August 13, 2010 Friday- 8:00 AM to 12:00 PM CDT
Exelon Corporation
10 S. Dearborn Street, 48th Floor , Chicago, IL
NOTE: 1. Agenda Times May be Adjusted as Needed during the Meeting
NOTE: 2. Drafting Sub-team Meetings May Not Have Access to Telephones and Ready Talk

Proposed Meeting Objectives/Outcomes:

- To review the adopted CSO706 SDT 2010 Work Plan and Schedule for CIP-002-4 in 2010
- To review and adopt a Work Plan and Schedule for completing CIP-010 & 011 in 2011
- To review and discuss the results and implications of SDT member companies' data survey results for the CIP 002-4 draft.
- To review, clarify, refine and adopt CIP-002-4 standard proposal for NERC staff review
- To review CIP-010 & 011 sub-teams draft responses to industry and Dallas workshop
- To agree on next steps and assignments

Tuesday, August 10, 2010 8:00 a.m. - 5:00 p.m.

- Introduction, welcome, and opening and guest remarks -*(Morning)*
- Receive updates on other related cyber security initiatives- *NERC Staff and SDT Members (Morning)*
- Review of CSO706 SDT Work plan and schedule for CIP 002-4 *(Morning)*
- Review of CSO706 Draft SDT Work plan and schedule for CIP 010 & 011 *(Morning)*
- "Lunch and Learn"- Forensics U.S. CERT *(Lunch)*
- Overview of NERC Survey Development and Industry Comments *(Afternoon)*
- Review and refine draft CIP 002-4 standard and related documents *(Afternoon)*

Wednesday, August 11, 2010 8:00 a.m. -5:00 p.m.

- Review and discuss the SDT member survey responses and their implications for CIP 002-4 drafting *(Morning)*
- Review and refinement of CIP-002-4 documents including implementation plan for NERC staff review *(Afternoon)*

Thursday, August 12, 2010, 8:00 a.m. - 5:00 p.m.

- Adoption of CIP 002-4 documents for NERC staff review *(Morning)*
- Adoption of CIP 010 & 011 Draft Schedule *(Morning)*
- CIP-010 and 011 Sub-teams present draft summary responses to Industry Comments and Workshop input *(Morning and Afternoon)*
- Agree on schedule for incorporating draft responses to Industry Comments and Workshop input into a single response document. *(Afternoon)*

Friday, August 13, 2010, 8:00 a.m. - 12:00 p.m.

- Review directions and next steps to CIP-010 and 011 Sub-teams – *as needed (Morning)*
- Address 002-4 planning for September Webinar *(Morning)*
- Review SDT September 8-10, 2010 Winnipeg Meeting Agenda (*Late Morning)*

Appendix # 2 Attendees List
August 10-13, 2010, Chicago IL

Attending in Person — SDT Members and Staff

1. Rob Antonishen	Ontario Power Generation
2. Jim Brenton	ERCOT
3. Jay S. Cribb	Southern Company Services
4.Joe Doetzl	Kansas City Pwr. & Light Co
5. Sharon Edwards	Duke Energy
6.Gerald S. Freese	America Electric Pwr.
7. Jeff Hoffman	U.S. Bureau of Reclamation, Denver
8. Phillip Huff, Vice Chair	Arkansas Electric Coop Corporation
9. Doug Johnson	Exelon Corporation – Commonwealth Edison
10. Patricio Leon	Southern California Edison
11. John Lim, Chair	Consolidated Edison Co. NY
12. David Norton	Entergy
13. David S. Revill	Georgia Transmission Corporation
14. Scott Rosenberger	Luminant Energy (T/W/Th)
15. Kevin Sherlin	Sacramento Municipal Utility District
16. Jonathan Stanford	Bonneville Power Administration
17. Keith Stouffer	National Institute of Standards & Technology
18. John Van Boxtel	WECC
Herb Schrayshuen	*NERC Vice President and Director of Standards (Th/F)*
Scott Mix	*NERC*
Howard Gugel	*NERC*
Joe Bucciero	*NERC/Bucciero Consulting, LLC*
Robert Jones	*FSU/FCRC Consensus Center*
Stuart Langton	*FSU/FCRC Consensus Center*
Hal Beardall	*FSU/FCRC Consensus Center*

SDT Members Attending via ReadyTalk and Phone

19. John D. Varnell	Technology Director, Tenaska Power Services Co. (T/W)
20.Rich Kinas	Orlando Utilities Commission (T/W)
21. William Gross	(W/Th/F)
22. Tom Stevenson	Constellation (T/Th/)

SDT Members Not Participating

Jackie Collett	Manitoba Hydro (W/Th/F)
William Winters	Arizona Public Service, Inc.

Others Attending in Person

Jan Bargen	FERC
Joel Garmen	Next Era Energy (FPL) (T/W/Th)
David Batz	EEI (W)
Robert Preston Lloyd	Southern California Edison
Michael Keane	FERC
Jason Marshall	Midwest ISO
Bryn Wilson	OG & E
Brian Newell	American Electric Power
Mark Simon	Encari
Tom Alrich	Matrikon
Allen Mosher	APPA, Standards Committee Chair
Guy Zito	NPCC (T/W)

Others Attending via Readytalk and Phone

August 10, 2010, Tuesday

Peter	Kuebeck	FERC
Todd	Williams	MidAmerican
Larry	Camm	Schweitzer Engineering Laboratories, Inc.
Michael	Welch	Florida Power and LIght
Laura	Hussey	laura_hussey@mindspring.com
Thomas	Reina	FERC
David	Batz	Edison Electric Institute
Andres	Lopez	US Army Corps of Engineers
Justin	Kelly	FERC
Jerome	Farquharson	Burns & McDonnell
Roger	Fradenburgh	Network Security Technology, Inc
Rod	Hardiman	Southern Company
Nicholas	Snyder	FERC
Jacob	Van Wagoner	El Paso Electric
Amir	Hammad	Constellation Energy
Summer	Esquerre	NextEraEnergy, Florida Power and Light
Ingrid	Rayo	Constellation Energy
David	Gordon	Mass. Municipal Wholesale Electric Co.

August 11, 2010, Wednesday

Jacob	Van Wagoner	El Paso Electric
Justin	Kelly	FERC
Andres	Lopez	US Army Corps of Engineers
Rod	Hardiman	Southern Company

Sharla	Artz	Schweitzer Engineering Laboratories, Inc.
David	Gordon	Mass. Municipal Wholesale Electric Co.(MMWEC)
Larry	Camm	Schweitzer Engineering Laboratories, Inc.
Michael	Welch	Florida Power and Light
Maggy	Powell	Constellation Energy
thomas	reina	FERC
Amir	Hammad	Constellation Energy
Jerome	Farquharson	Burns & McDonnell
Matt	Dale	FERC
Ingrid	Rayo	Constellation Energy
Summer	Esquerre	Next Energy, Florida Power and Light
Drew	Kittey	FERC

August 12, 2010, Thursday

Rod	Hardiman	Southern Company
Jacob	Van Wagoner	El Paso Electric
Michael	Fischette	Lansing Board of Water and Light
Matt	Dale	FERC
Thomas	Reina	FERC
Jerome	Farquharson	Burns & McDonnell
Andres	Lopez	US Army Corps of Engineers
Larry	Camm	Schweitzer Engineering Laboratories, Inc.
David	Gordon	Mass. Municipal Wholesale Electric Co.(MMWEC)
Justin	Kelly	FERC
John	Fridye	AT&T
Amir	Hammad	Constellation Energy

August 13, 2010, Friday

Sharla	Artz	Schweitzer Engineering Laboratories, Inc.
Larry	Camm	Schweitzer Engineering Laboratories, Inc.
Jerome	Farquharson	Burns & McDonnell
Ingrid	Rayo	Constellation Energy
Jacob	Van Wagoner	El Paso Electric
David	Gordon	Mass. Municipal Wholesale Electric Co.(MMWEC)
Rod	Hardiman	Southern Company
Matt	Dale	FERC

Appendix #3 NERC Antitrust Compliance Guidelines

See Antitrust Compliance Guidelines read at the beginning of each day's session at:

(NEED LINK)

The NERC reminder below was read at the beginning of each day's session.

NERC REMINDER FOR USE AT BEGINNING OF MEETINGS AND CONFERENCE CALLS THAT HAVE BEEN PUBLICLY NOTICED AND ARE OPEN TO THE PUBLIC

For face-to-face meeting, with dial-in capability:

Participants are reminded that this meeting is public. Notice of the meeting was posted on the NERC website and widely distributed. The notice included the number for dial-in participation. Participants should keep in mind that the audience may include members of the press and representatives of various governmental authorities, in addition to the expected participation by industry stakeholders.

Appendix #4 NERC CIP 002 Critical Asset Methodology Survey: NERC Responses to Comments Received

Summary of Comments Received Regarding Proposed CIP-002 Methodology Data Request:

NERC's proposed CIP-002 Methodology Data Request was posted for industry comment on July 7 for a nineteen-day public comment period. As a result of this public posting, NERC received comments from 65 entities. Summarized below are the overarching issued identified in these comments and NERC's position regarding the issues raised.

Issue Number 1: Nuclear issue

Several entities expressed concern about what appears to be an additional High Impact Rating criterion (1.1. Nuclear Generation Facilities), that has not been present in previous versions of the CIP-002 standard released for comment. Their concern is that this criterion does not seem to be based on any measurable Bulk Electric System impact, but rather on the type of generation fuel utilized, and that this criteria is not an effective method of reliably determining impact to the BES.

NERC response: The main purpose of the Data Request is to obtain information that the CIP Standard Drafting Team can use to determine what assets should be included in the bright line criteria for a proposed CIP-002-4. The Data Request is not proposing to define new criteria. It is merely collecting data so that new criteria can be defined at a later point by the standard drafting team to include in a proposed CIP-002 Version 4 standard.

Issue Number 2: Over counting assets

Several entities were concerned about how to count facilities that may meet multiple criteria. It was expressed that additional instructions for the survey would help to avoid potential erroneous "double counting" of assets that meet certain criteria. For example, facilities that have multiple owners should only be counted once. Facilities that serve multiple entities and/or serve an entity operating in multiple regions should only be counted once. In addition, there was a question about whether the Data Request should be filled out for each NERC Compliance Registry entry, or on an enterprise-wide basis.

NERC response: In response to these comments, the instructions were modified to clarify that each facility should only be counted one time in the survey responses. Furthermore, owners of jointly-owned facilities should coordinate their response so that those facilities are only counted once. The instructions were also modified to stipulate that the Data Request should be

responded to on an enterprise-wide basis, to ensure that internal facilities were also only counted once.

Issue Number 3: Estimate on Burden Imposed to Collect Data

Many entities stated that the time estimate to respond to the Data Request was not high enough. Almost all comments stated that the estimate to respond would take anywhere from 25 to 100 hours to complete.

NERC Response: The estimated time to complete the Data Request was modified to "less than 100 hours" total per entity.

Issue Number 4: Canadian entity issue

One entity noted that this data request is being proposed in accordance with Section 1600 of the NERC Rules of Procedure. This entity stated that "This section clearly states that, within the United States, NERC and regional entities may request data or information that is necessary to meet their obligations under Federal Power Act. This section does not apply to Canadian based entities and we suggest that in the future this is explicitly stated in the text to avoid confusion on the part of Canadian entities."

NERC Response: All NERC registered entities, including Canadian entities, are required to comply with the NERC Rules of Procedure. Section 100 of the NERC Rules provide:

> NERC and NERC members shall comply with these rules of procedure. Each regional entity shall comply with these rules of procedure as applicable to functions delegated to the regional entity by NERC or as required by an appropriate governmental authority or as otherwise provided. Each bulk power system owner, operator, and user shall comply with all rules of procedure of NERC that are made applicable to such entities by approval pursuant to applicable legislation or regulation, or pursuant to agreement.

Therefore, pursuant to applicable legislation, regulation, or agreement among NERC and Canadian provincial authorities, Canadian entities are required to comply with Section 1600 of the NERC Rules of Procedure, including responding to this Data Request upon it becoming mandatory by NERC Board of Trustees approval.

Issue Number 5: High vs. Medium

Several entities expressed concern that high and medium impact levels are included on the Data Request. The concern is that both high and medium impact Critical Assets would be used for CIP-002-4, and all of CIP-003 to CIP-009 would apply to both.

NERC Response: The reason that both high and medium impact levels are included in the Data Request is to assist the Standard Drafting Team in determining whether the bright line between high and medium is set at the correct level. The team intends to use only the high impact level for a bright line for determining Critical Assets that will then be used to determine Critical Cyber Assets. There is no intent to include a medium level in the proposed CIP-002-4.

Issue Number 6: Data use

Several entities questioned whether the following statement could be stated with certainty:

This data will not be used as a basis for determining compliance with the currently enforceable CIP-002 through CIP-009 reliability standards.

NERC Response: As noted in the Data request, the information being collected is only to be used prospectively by the drafting team to evaluate a proposed methodology to be used in a future version of the CIP-002 standard. Therefore, the data being collected will not be used as a basis for determining compliance with the currently enforceable CIP body of standards.

Changes Made to the Survey in Response to Comments and Standard Drafting Team input:

As a result of comments received and additional standard drafting team ("SDT") review, NERC made the following changes to the survey:

- Changed the references to "drafting team data request" to "NERC data request."
- Modified the reference to "Regional Reliability Organization" to "Regional Entity" based on the list of Responsible Entities in CIP-002-2.
- Changes the estimated number of hours to complete the data request from "less than 24" to "less than 100" based on comments received on the Data Request.
- Clarified that NERC registered entities should respond to the data request on an enterprise-wide basis, and that entities with jointly-owned facilities coordinate their responses for such facilities.
- An explanation of the requirements under the current CIP-002-2 standard was added to clarify the information requested in questions 1 and 2.
- A clarification was made to ensure that each element on the list should be counted only one time.
- A clarification was made that each Critical Asset should be counted only once.
- A modification was made that all NERC Compliance Registry (NCR) numbers for the enterprise-wide survey response be included.

- Question 1 and 2 were clarified to state that the responses should be based on each entity's existing Critical Asset list under the currently-effective CIP-002-2 standard.
- The third column heading was changed for the tables in question 2 and question 3 for consistency.
- Question 4 was added to require entities to report all NCR numbers for their enterprise-wide response.
- Attachment 1 Item 1.1 – "Generation" was changed to "generation" to reflect the fact that generation is not a NERC glossary term.
- Attachment 1 Item 1.2 – changed based on input from the Standard Drafting Team (STD).
- Attachment 1 Item 1.3 – changed based on industry comments and input from the SDT.
- Attachment 1 Item 1.4 – changed to add clarity based on industry comments and input from the SDT.
- Attachment 1 Item 1.5 – changed to add clarity based on industry comments and input from the SDT.
- Attachment 1 Item 1.7 – split into two items to add clarity based on input from the SDT.
- Attachment 1 Item 1.9 – changed to add clarity based on industry comments and input from the SDT.
- Attachment 1 Item 1.10 – split into two items to separate FACTS devices from other devices that prevent IROLs based on input from the SDT.
- Attachment 1 Item 1.12 – changed to simplify wording and add clarity based on input from the SDT.
- Attachment 1 Item 1.15 – changed to limit scope to control systems for load shedding based on industry comments and input from the SDT.
- Attachment 1 Item 1.16 – modified to add clarity based on input from the SDT.
- Attachment 1 Item 1.17 – modified to provide MW levels in order to provide the SDT with data to determine bright line levels, if applicable.
- Attachment 1 Item 1.18 – modified to provide kV levels in order to provide the SDT with data to determine bright line levels, if applicable.
- Attachment 1 Item 1.19 – changed to add clarity based on input from the SDT.
- Attachment 1 Item 1.20 – added to allow entities to include additional assets as Critical Assets based on input from the SDT.
- Attachment 1 Item 2.1 – modified to provide consistency with Item 1.2.
- Attachment 1 Item 2.2 – modified to provide consistency with Item 1.3.
- Attachment 1 Item 2.3 – deleted based on modifications to Item 1.4.
- Attachment 1 Item 2.3 (new) – modified to provide consistency with Item 1.7.

- Attachment 1 Item 2.4 – modified to provide consistency with Item 1.8.
- Attachment 1 Item 2.6 – changed to add clarity based on input from the SDT.
- Attachment 1 Item 2.7 – changed to add clarity based on input from the SDT.
- Attachment 1 Item 2.8 – changed to add clarity based on input from the SDT.
- Attachment 1 Low Impact Rating – changed “Critical Assets” to “BES Elements” based on industry comments in order to add clarity.

Appendix # 5- CIP 002-4 Adopted Draft (8-12-10)

Introduction

1. **Title:** Cyber Security — Critical Cyber Asset Identification
2. **Number:** CIP-002-4
3. **Purpose:** NERC Standards CIP-002-4 through CIP-009-4 provide a cyber security framework for the identification and protection of Critical Cyber Assets to support reliable operation of the Bulk Electric System.

   These standards recognize the differing roles of each entity in the operation of the Bulk Electric System, the criticality and vulnerability of the assets needed to manage Bulk Electric System reliability, and the risks to which they are exposed.

   Business and operational demands for managing and maintaining a reliable Bulk Electric System increasingly rely on Cyber Assets supporting critical reliability functions and processes to communicate with each other, across functions and organizations, for services and data. This results in increased risks to these Cyber Assets.

   Standard CIP-002-4 requires the identification and documentation of the Critical Cyber Assets associated with the Critical Assets that support the reliable operation of the Bulk Electric System. These Critical Assets are to be identified through the application of the criteria in Attachment 1.
4. **Applicability:**
   - **4.1.** Within the text of Standard CIP-002-4, "Responsible Entity" shall mean:
     - **4.1.1** Reliability Coordinator.
     - **4.1.2** Balancing Authority.
     - **4.1.3** Interchange Authority.
     - **4.1.4** Transmission Service Provider.
     - **4.1.5** Transmission Owner.
     - **4.1.6** Transmission Operator.
     - **4.1.7** Generator Owner.
     - **4.1.8** Generator Operator.
     - **4.1.9** Load Serving Entity.
     - **4.1.10** NERC.
     - **4.1.11** Regional Entity.
   - **4.2.** The following are exempt from Standard CIP-002-4:
     - **4.2.1** Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.
5. **Effective Date:** The first day of the third calendar quarter after applicable regulatory approvals have been received (or the

Reliability Standard otherwise becomes effective the first day of the third calendar quarter after BOT adoption in those jurisdictions where regulatory approval is not required)

Requirements

R1. Critical Asset Identification — Each Responsible Entity shall develop a list of its identified Critical Assets determined through an annual application of the criteria contained in *CIP-002-4 Attachment I – Critical Asset Criteria*. The Responsible Entity shall review this list at least annually, and update it as necessary.

R2. Critical Cyber Asset Identification — Using the list of Critical Assets developed pursuant to Requirement R1, each Responsible Entity shall develop a list of associated Critical Cyber Assets. For each group of generating units (including nuclear generation) at a single plant location identified in Attachment 1, criterion 1.1, the only Cyber Assets that must be considered are those shared Cyber Assets that could adversely impact the reliable operation of any combination of units that in aggregate exceed Attachment 1, criterion 1.1 within 15 minutes. The Responsible Entity shall review this list at least annually, and update it as necessary. For the purpose of Standard CIP-002-4, Critical Cyber Assets are further qualified to be those having at least one of the following characteristics:

R 2.1 The Cyber Asset uses a routable protocol to communicate outside the Electronic Security Perimeter; or,
R 2.2 The Cyber Asset uses a routable protocol within a control center; or,
R 2.3 The Cyber Asset is dial-up accessible.

R3. Annual Approval — The senior manager or delegate(s) shall approve annually the list of Critical Assets and the list of Critical Cyber Assets. Based on Requirements R1 and R2, the Responsible Entity may determine that it has no Critical Assets or Critical Cyber Assets. The Responsible Entity shall keep a signed and dated record of the senior manager or delegate(s)'s approval of the list of Critical Assets and the list of Critical Cyber Assets (even if such lists are null.)

Measures

M1. The Responsible Entity shall make available its list of Critical Assets as specified in Requirement R1.

M2. The Responsible Entity shall make available its list of Critical Cyber Assets as specified in Requirement R2.

M3. The Responsible Entity shall make available its approval records of annual approvals as specified in Requirement R3.

Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

1.1.1 Regional Entity for Responsible Entities that do not perform delegated tasks for their Regional Entity.

1.1.2 ERO for Regional Entity.

1.1.3 Third-party monitor without vested interest in the outcome for NERC.

1.2. Compliance Monitoring Period and Reset Time Frame

Not applicable.

1.3. Compliance Monitoring and Enforcement Processes

Compliance Audits
Self-Certifications
Spot Checking
Compliance Violation Investigations
Self-Reporting
Complaints

1.4. Data Retention

1.4.1 The Responsible Entity shall keep documentation required by Standard CIP-002-4 from the previous full calendar year unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

1.4.2 The Compliance Enforcement Authority in conjunction with the Registered Entity shall keep the last audit records and all requested and submitted subsequent audit records.

1.5. Additional Compliance Information

1.5.1 None.

2. Violation Severity Levels (To be developed later.)

Regional Variances

None identified.

VERSION HISTORY

Version	Date	Action	Change Tracking
1	January 16, 2006	R3.2 — Change "Control Center" to "control center"	03/24/06
2		Modifications to clarify the requirements and to bring the compliance elements into	

		conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3		Updated version number from -2 to -3	
3	12/16/09	Approved by the NERC Board of Trustees	Update
4	09/?/2010	Modified to provide bright-line criteria for the identification of Critical Assets.	

CIP-002-4 - Attachment I

CRITICAL ASSET CRITERIA

The following are considered Critical Assets:

1.1 A generating unit or group of generating units (including nuclear generation) at a single plant location with an aggregate highest rated net Real Power capability in the preceding 12 months exceeding the lowest Contingency Reserve identified over the preceding 12 months by the Reserve Sharing Group or the Balancing Authority if it is not a member of a Reserve Sharing Group, at the time the CIP-002 is reviewed.

1.2 Any reactive resource or group of resources at a single location (excluding generation Facilities) having aggregate net Reactive Power nameplate rating of 1000 MVARs or greater.

1.3 Generation Facilities that the Planning Coordinator or Transmission Planner designated as required for reliability purposes.

1.4 Each Blackstart Resource identified in the Transmission Operator's restoration plan.

1.5 The Facilities comprising the Cranking Paths and initial switching requirements identified in the Transmission Operator's restoration plan.

1.6 Transmission Facilities operated at 500 kV or higher.

1.7 Transmission Facilities operated at 300 kV or higher at stations interconnected at 300 kV or higher with four or more other stations in the Eastern Interconnection or the Western Interconnection.

1.8 Transmission Facilities operated at 200 kV or higher at stations interconnected at 200 kV or higher with four or more other stations in the Texas Interconnection or the Quebec Interconnection.

1.9 Transmission Facilities that, if destroyed, degraded, misused or otherwise rendered unavailable, violate one or more Interconnection Reliability Operating Limits (IROLs).

1.10 Flexible AC Transmission Systems (FACTS), that, if destroyed, degraded, misused or otherwise rendered unavailable, violate one or more Interconnection Reliability Operating Limits (IROLs).

1.11 Transmission Facilities providing the generation interconnection required to directly transmit generator output to the transmission system that, if destroyed, degraded, misused, or otherwise rendered unavailable, would result in the loss of the assets identified in Attachment 1, criteria 1.1 or 1.3.

1.12 Transmission Facilities identified as essential to meeting Nuclear Plant Interface Requirements.

1.13 Special Protection Systems (SPS), Remedial Action Schemes (RAS) or automated switching systems that operate BES Elements that, if destroyed, degraded, misused or otherwise rendered unavailable, violate one or more Interconnection Reliability Operating Limits (IROLs).

1.14 Common control system(s) that are capable of performing automatic load shedding of 300 MW or more.

1.15 Any control center or control systems, and backup control center or backup control systems, used to perform the functional obligations of the Reliability Coordinator or Balancing Authority or Transmission Operator.

1.16 Any control center, or backup control center, used to control generation that is identified as a Critical Asset, or used to control generation greater than an aggregate of 2300 MWs in a single Interconnection.

Appendix # 6- CIP 002-4 8-10-12, 2010 Discussion Notes and Straw Polls

In Pittsburgh the SDT, after consideration and debate, agreed to delete Criteria 1 related to nuclear industry generation facilities. The SDT in Chicago looked once again at the possible justifications for restoring this deleted criteria and including nuclear generation facilities. Some argued that if one nuclear plant were subject to an attack then all plants might be shut down until they can prove that they do not have the same reliability issue. This would be a fleet issue unique to nuclear generation and reaction to one incident. In addition once a nuclear plant comes off line it will not get it back in 24 hours – investigation will take time and may take out a big block of production. It is also a symbolic target beyond other system assets that plays in Congress or the New York Times and risk protection strategies need to recognize a higher level of scrutiny and perception.

SDT Member and Participant Comments

- **Nuclear facilities.** Agree if higher "value" target then should have more protection, but not because of loss of capacity. No question these plants have high political visibility. However, U.S. has a better, more diverse system of nuclear operation systems. Problems encountered in the past have not shut down all plants.
- We also have the survey to identify which components in nuclear are safety and subject to NRC and which are reliability for NERC – some argue designating all as safety for NRC regulation – may want to designate it all as "high" to avoid issues with NERC.
- NRC has a huge program around cyber security and we are not addressing their issues in the CIP as we are focused on reliability
- Still a fuel question
- Support including – it is optics – high impact, very low probability – but must have standard to address it – exception to calling out a fuel type because of optics
- Communication team needs to explain it was not exempted before but included here – what difference if it is on CA list make any difference in NRC shutting them all down – take exemption out will not affect NRC shutting them down or not for safety
- Would NRC close them all down? Even if they did would do it so as not to affect system reliability – the cyber equipment varies between the nuclear plants, not a common load failure question – this is not a reliability question, only an optics or political question
- We are addressing "impact based" criteria in CIP 002-4 – Hard to reconcile the risk basis for a higher profile for nuclear generation where everything else is impact based, not risk based. This represents a different framework for criteria.
- Political reality – the communication efforts need to point out that we took out the exception for nuclear – if there is a reliability basis, that should be in there – not because it is a nuclear plant.
- Shouldn't matter what the fuel but rather what is the impact on the system. There is a lot of work going on to address the issue within the nuclear industry already.

- Nuclear excluded in Pittsburgh but if exclude 1.1 then may need to add back in – optics must be considered – not mentioning nuclear anywhere will look bad.
- Cyber requirements being developed for nuclear as part of its licensing structure – even though aimed at radiation releases, it is broad and in depth covering the same components for reliability.
- To be consistent it has to be reliability based – but optics that "nuclear" is different or special to those outside the industry.
- How can we focus on reliability of BES but somehow recognize "nuclear"?
- Agree on objectives but how do we get there and arm representatives in Washington – again, in 010-011 some nuclear plants may fall into "low" category – that will not sell – if not including all nuclear then need to explain that NRC is covering under "safety" or other reason – also still believe fleet of nuclear is different and subject to broader potential shut down.
- We will need a clear explanation why any are not included as "critical"
- If use bright line – then many nuclear units will not be included and it will be difficult to defend.
- If put in all nuclear plants now then put in tiered approach later, we may cause confusion – prefer removing exemption and consider the same as others.
- Transmission owner controls substations – most of the nuclear substations are critical even if the generator is not.
- Think we can still say in the next round that all nuclear are "critical"?
- All nuclear generation is addressed by NRC and we say all controls are "high" in our system.
- 1.12 has language already addressing the issue. Nuclear exclusion not there, transmission facilities covered in 1.12 and no distinction by fuel.
- Clarify the shared component is cyber and not just a fence –
- 706b speaks to the issue – anything not covered by NRC is subject to the NERC standards – order by FERC sets out the division of responsibility – no need here to call out the fuel.
- Does not answer if nuclear plant is a CA or a CCA which is necessary to determine 002-009 coverage.
- Either identifying everything inside a common fence, or the common cyber connections
- May help with optics – but the point is to get a list of CCAs – isn't the end result the same – is this plant critical – yes, if it has shared critical cyber asset.
- Have to justify the bright lines you pick to the Commission.
- Trying to in a single section work through an "if, then" set of logic? Single asset for common failure threat or by cyber connection? Just trying to get into the first bucket of identifying as CAs then determine the process for protecting – you seem to be wrestling with both at the same time with the same criteria.
- Will need to show why or how the bright line approach provides better protection
- Any of the alternative language will be "fudgy" and imperfect

- The language in the yellow should be “generation plants” instead of “generation units”?
- Prefer keeping language the same or close to the current CIP version 3
- “For each group of generating units (including nuclear generation) at single plant location identified in Attachment 1 ….”
- Are we saying “only” Cyber Assets that must be considered …? Only shared assets?
- Still needs to be connected by routable protocols – also FERC referred to not enough assets identified, is there a study for that?
- Want to limit the scope to cyber system that controls more than one unit – need to recognize many systems may be interconnected, beyond just the control systems
- In CIP 10 we refocus on cyber systems that impact bright line in 1.1 – here, the clarification smoothes that transition – if we bring everything else in the plant that changes the dynamic – leave this here as is.
- Is there is a concrete definition of adverse impact within 15 minutes – fuzzy, may need discussion later
- Units may talk to each other over some connection – are we considering that a shared system and the only thing we are protecting – what if it is an Ethernet cable without other connections? If it has a switch? What are we trying to get at here? Do we want to protect a cable inside a plant? Are we only looking at “shared”? Does that mean we are protecting cables and switches?
- Tied more to shared systems – it is a connectivity question.
- Shared switch in the middle currently has to be within a protected perimeter.
- Plants surrounded by a fence to be critical only if shared system that impacts the whole site – fence does not define as a critical asset.
- That is not what the standards says – identify those critical to operation of the plant.
- Today protecting assets critical to the unit, not the plant – only those that are shared.
- Can have one cyber asset affecting one unit that then impacts other units – it is the impact on the aggregate of the plant – looking for cyber assets that link the physical assets together – that is what CIP 10 intends to do, but CIP 002-4 does not – find critical assets first through aggregate that exceeds bright line, then for the shared systems.
- Shared systems, not the physical fence
- We should not rely just on the compliance document.
- We had this discussion under “target of production” thirteen months ago
- We should keep the language here or take it out altogether.
- Why does highlighted language not address the issue.
- Switch on the shared network? What needs to be protected? Just the switch?
- Similar problem with EMS – call our control systems as critical.
- How is industry digesting the ambiguity?
- 010-011 addresses the issue, the CIP 002-4 does not.

- The single location is the problem here – I have separated systems and protections even where they are in the same physical location – now trying to introduce a single plant location.
- Delete everything in color – figure out the iron impacted and protect the routable protocols – cannot write something to every entity in the country.
- But we set bright lines and will be held to audits.
- Frustrated because we are trying to define critical asset list when we should focus on the critical cyber asset – this language makes the audits so much more painful.
- Where should we identify the critical asset impact – not critical because it is in the fence but because it impacts reliability.

***Straw Poll*:** Putting in Nuclear as Separate Criteria
Yes – 3 No – 13

- 706b already addresses the issue

***Straw Poll*:** Keep the yellow shaded language in R1remain? (For each group of ...)
Yes – 8 No – 9

Comments after Poll

- Note we did not say we did not want the language but do not want it here.
- Ramification of putting language in the attachment?
- Putting into attachment loop CAs into determination of CCAs
- If in attachment then the plant is not identified as CA lowering the number identified

Criteria 1.1 (newly numbered)

- Wording in 1.1(a) revised to delete 1.1b – (b) was the value if not in a group –
- Value in b sets at smallest value of (a) fluctuating value as a floor.
- (a) was suppose to be RSG and b is if BA is independent – were separated originally
- Thought we said everyone has to be in a group in "a" and eliminated a, b and c
- Can this be accurately explained in a quick manner? Looks as if plants would fluctuate in and out of qualifying
- Is it the lesser of or the greater of? Need to clarify.
- Contingency reserve set differently by region – with guidance from another standard
- Has to be based on a formula
- Standards says there will be a contingency reserve but not prescribe how
- delete "a" and "b"?
- contingency reserve means something to operators – the 2000 is a default number
- Options: delete b, or take 2000 out

- Do we need to put qualifying language back into "a" that was pulled out to make "b"?
- Trying to limit the tracking of different values
- Update as necessary?

***Straw Poll*:** Delete "b", with a and c remaining.
Yes – 15 No– 0

- How do we set how determine the value if it fluctuates?
- Reword "a" – "The lowest contingency reserve identified by the reserve sharing group or balancing authority if it is not a member of a Reserve Sharing Group, at the time the CIP002 is reviewed , or….."
- Why set at lowest level? That is the worst case.
- Those are the periods when most vulnerable as units are most likely down for maintenance.
- The lower the contingency reserve the more units are brought in – the contingency reserve is intended to protect your system.
- What is the current level? About 1800, with lowest around 1400-1500

***Straw Poll*:** Support reworded "a":
Yes – 17 No – 0

- Some areas that do not have contingency reserves? If required why have "c"

***Straw Poll*: Delete "c"?**
Yes - 10 No - 0 Abstain - 6

- Abstainers need to be educated to know how to vote.
- This was intended to catch any entity that was not in a BA or a RSG
- Everyone has to be in a reserve sharing group.
- A plant can be divided up into four regions – but if so, then it may not be critical – do you need a critical value
- Do we still need to keep the 2000 threshold?

1.2

- What group of Facilities within 15 minutes? Need to fix.
- Seems inconsistent with the previous section – this says reactive resource – put comma between compensator and that so we get intent of not associated with Generation Facilities - "any reactive resource not associated with Generation Facilities ….
- If control center controls distribution of cap banks? Combination of all of them could exceed 1000 –
- It makes individual cap banks a CA

- Excluding control centers? It is not a common cyber asset; not sure this sentence says that – change group of facilities to operation of the reactive resources
- Why did we add the "shares a common Cyber Asset or common Cyber Assets"?
- Put period after Cyber Asset and start new sentence?
- Talking about Cyber Assets? Figure out CCAs later
- Any reactive resource at a single location? Excluding generation facilities?
- Any reactive resource or group of reactive resources at a single location (excluding generation Facilities) having aggregated rated net Reactive Power capability of greater or equal to 1000 MVAR
- If no routable protocol or dial up then don't need to worry about shared
- "Nameplate rating"? put back in place of greater or equal to
- Any reactive resource or group of reactive resources at a single location (excluding generation Facilities) having aggregated net Reactive Power name plate rating of 1000 MVARs or greater.
- Take out first "rated"
- Where did we get the 1000 MVARs? Arbitrarily half of 2000 formerly in R1?

1.2 Any reactive resource or group of resources at a single location (excluding generation Facilities) having aggregate net Reactive Power nameplate rating of 1000 MVARs or greater.

***Straw Poll*:** Accept 1.2 as revised above.
Yes – 16 No – 0

1.3

- "Must run"? It has a specific meaning in certain markets. Planning coordinator doesn't determine reliability "must-run" – not sure who still uses the term. Is there a standard for "must-run"? It is a market thing in our area. There are references on NERC site for "must-run" contracts but it is not an official term.
- If planning coordinator says needed for reliability – may need to change the term – "Generation Facilities that the Planning Coordinator identifies as required to be available for reliability purposes."
- "to be available"? "identify as required for reliability purposes."
- Is the planning coordinator the right entity? (yes)
- Planning coordinator can tell you it is a critical asset?
- Think about possible blow-back if saying cannot retire units for purposes of reliability – if cheaper to retire than pay mortgage but now saying cannot take off line?
- Do we run into challenges of PC determining short term operations by requiring continuing for reliability.
- Every bit critical before you decide to retire the unit than after you decide to retire it – why is it not critical before deciding to retire it?

- Not restricting beyond reliability requirement – what if WEC is the designator and the auditor? Is the RRO designating and auditing Critical Assets?
- What is added here not captured in 1.1.
- WEC does have designated "must-runs"
- How do I know what has been identified under this provision? By contract? Then formally designated.
- May not be just a retirement issue.
- Change to "designated" and drop formally?
- What is the time frame? Past, future or current?
- Think it is current when you are audited – that is the way written now.
- Concerned about WEC designating and auditing – seems a conflict of interest, but willing to let industry ballot and comment.
- Add Transmission Planner?
- Care less about who and more about how designated.
- Identified assets we think is critical – let industry decide who and how designated – put out to ballot as written here

"Generation Facilities that the Planning Coordinator or Transmission Planner designated as required to be available for reliability purposes."
Support for 1.3 as revised above:

Straw Poll: Yes: 13 No: 1 Abstaining: 1

1.3

- Transmission operators plan identifies all Blackstart capable units – is that what we intended, to bring in every Blackstart capable unit?
- Need to see what the requirements are for TO to come up with the plan.
- Blackstart is a NERC defined term that may limit – though Blackstart plan includes other resources not included in the term "Blackstart Resources"
- These are not necessarily units you go to first – may need to reach out to drafters of standard to identify the critical assets and not the small units that may be listed in the plans
- "Essential to system restoration" – not everything, but what you would go to first to restore the system – the starting points – restoration plans include anything capable – This needs clarification
- Read NERC definition of Blackstart Unit as background.
- Requirement to test to see if units capable of performing Blackstart function – scheduled test.
- Blackstart units listed to kick in big units – seems clear.
- Large number of permutations for bringing supply back on line? Plan is set out to assure enough capacity is available – blackstart units are declared in current plans.

- Why was "primary" dropped from 1.4? Because there is not distinction or requirement for a "primary" blackstart unit or resource.
- Are we providing incentive to remove assets as blackstart units?

1.4-1.6

- How would Blackstart unit know it is included – need to clarify
- The plan is a catalogue of everything capable of serving as a Blackstart Resource
- Definition of Blackstart Resource is not every capable unit
- There are actual contracts out there for Blackstart Resources and contingencies – we have are resources designated.
- How about "contained" versus "identified"?

1.3 Any Blackstart Resource contained in the Transmission Operator's restoration plan.
1.4 The Facilities comprising Cranking Paths contained in the Transmission Operator's restoration plan.

- Phil Huff will check with Rich Kinas this evening who drafted this section at the last meeting.
- Can we say any Blackstart Resource in the plan is in?
- We had "primary" still in the survey? Significant difference between any and primary – may preliminary survey responses may be all wrong
- Can compile and provide quick overview along with some of the initial industry comment in response to the language in the survey

On Thursday morning, the SDT review any final outstanding issues before seeking to adopt CIP 002-4 for NERC staff review.

- **Criteria 1.1**. Regarding yesterday's question about voltage differences between regions – Scott Mix thought there was a reference possible to an existing standard. After some research it does not seem to be any accepted standard we can rely on for justification for differences by region.
- The idea is to identify where the bulk of BES occurs and hope that if you draw bright lines you will capture the highest impact facilities so the cyber assets connected to them will be protected.
- If bright line is from Vegetation, then it is 200 across regions.
- Trying to provide a clear understanding to a complex situation is something like fitting a square peg into a round hole.
- The 200 level gets both worlds with one standard.
- Losing sight of the fact we need three lines for h-m-l – but not a distinction between regions – lowering to the lesser one may not address need for three later on – ultimately will need more than one bright line.

- This does give us room to pick a medium later.
- Do we need three bright lines? This may be a misapplication of the NIST model. Could we get around this if we do high and everything else? Have been vigorous and gone fairly deep with high here, down into the mediums. Some think high should be much higher than here, more included here than many had expected.
- Suggest sticking with what we have at this point – need additional expertise in the room to help determine the appropriate level.
- Still have capability to tier even if we go with 200 cutoff here.
- Distinctions between interconnection on megawatts but different for voltage levels of transmission
- Went with the number based on Texas using 230 – need to confirm what Texas and Quebec use. Most of Quebec is over 300
- Looking at voltage class – may need to look at capabilities
- Allen Mosher suggested looking at getting subject matter experts from other teams to review our product to make sure it makes sense and help with the justifications
- Want a simple to understand bright line solution or appropriate solution to a complex issue – bright lines do not always fit cleanly or provide perfect solutions
- Do not have enough operational expertise on this group – we got review from others in the past – need to do so again – still think we need to draw clean lines the best we can – comment period will allow experts to weigh in on the line
- Anecdotal evidence says we do not need 1.8 – ask Rod Hardiman for advice
- Justification for separate voltage thresholds for Texas and Quebec? Strike criteria if not, and go with one standard. Quebec has said they want 500.
- Justification for distinction between 1.7 and 1.8? Pointing back to a document that cannot be found. I am nervous to make that distinction without more knowledge. From the southeast perspective I am comfortable for deleting 1.8.There is no justification for the distinction
- Threshold may be important – 300 may be justified

Straw Poll: Test whether to strike 1.8, and Eastern-Western from 1.7?
Favor=15 Oppose=0 Abstain=3

Motion to forward CIP 002-4 with attachment 1 to NERC for staff review
(Huff, Norton 2nd)
Yes=18 No=0

Appendix #7 CIP 002-4 Implementation Plan Discussion Notes

Scott Mix reviewed the a proposed approach for the Implementation Plan with the SDT which is based on utilizing the currently FERC approved CIP implementation plan and included the following components:

Proposed Effective Date Language

- "The first day of the first full calendar quarter after applicable regulatory approvals have been received; or, the first day of the second full calendar quarter after BOT adoption in those jurisdictions where regulatory approval is not required."
- *Assuming* FERC acts within one quarter, issuing an order on March 31, 2011, the effective date would be July 1, 2011 in both the US and Canada.
- Outreach to inform industry to start identification process upon filing.

The Rest of the Standards

- Since we aren't making changes to CIP-003 through CIP-009, the currently approved "Implementation Plan for newly Identified Critical Cyber Assets and Newly Registered Entities" would apply
- This plan was designed to apply to "Newly registered Entities", and was modeled after the Version 1 Table 4.
- Assuming the previous timeline, the starting date for this plan would be July 1, 2011.

Newly Identified CCA Plan Recap

- The Newly Identified CCA Plan allows:
- •24 months for entities without any Version-3 CCAs
- •For entities with Version-3 CCAs:
- Immediate for Policy, Leadership, Exceptions (CIP-003), Awareness (CIP-004)
- 6 months for Information Protection, Access Control, Change Control (CIP-003), Incident Reporting and Response (CIP-008), Recovery Plans, Backup & Restore, Testing Backup Media (CIP-009)
- 12 months for Electronic Security Perimeter (CIP-005), Physical Security (CIP-006), Systems Security Management (CIP-007), Exercises, Change Control (CIP-009)
- 18 months for Training, Personnel Risk Assessment, Access (CIP-004)

Scott Mix reviewed the above proposed approach for the Implementation Plan with the SDT which is based on utilizing the currently FERC approved CIP implementation plan. This approach was presented in Pittsburgh to the SDT and then refined based on that discussion. He noted the schedule assumes for a FERC order on the last day of a quarter and suggested the proposal is aggressive achievable and probably meets FERC's expectations. He suggested that 24 months would not be acceptable to FERC based on past experience.

The Chair suggested that following the review and testing of approaches he would look to forming a drafting team to develop a proposal for review and adoption in Winnepeg.

Member and Participant Discussion Comments on the Proposed Approach

- **Communication plan.** Is there a communication plan for this? Communication is very important

- **FERC Approval**
- Also concerned about FERC approving but asking for changes. Multiple industry avenues to get the information out should be part of the communication plan.
- The SDT is asking FERC to recognize the potential difficulty for implementation if there is an approval that also requests changes. If the industry doesn't know until March 31, then there may be only 3 months to analyze and identify critical assets.
- Can FERC staff take this concept back and ask if this approach is reasonable – can FERC approve in the first quarter of 2011 in order to implement by July 1, 2011.
- FERC staff agreed to discuss and see what other staff (not the Commission) thinks. Still need to address justifications for bright lines, that is the focus of FERC review.
- FERC staff appreciates reliance on already vetted plan – changing effective date to second and third quarter gets us to the current proposal of two full quarters.
- FERC staff suggested that adjusting quarters is a good idea – careful not to open a new can of worms and push approval back past 3-31-1l. Recognize the importance of budget cycles but those are plans, you already have to have every one of the processes listed, just adding items to the process
- This is just for CIP-002 which is only one change. Date could be different than CIP 003-009. Could it be different for CAs and CCAs?
- Can we stagger the implementation of CAs and CCAs? We will significantly increase the number identified and if an entity misses one will they have to self report on July 1?
- Could adjust to second and third full quarters – lock in the end date with interim steps?
- The NERC Board of Trustee approval starts the clock – if FERC request changes, then pushes this back at least 6 months. The pre-work by industry should not be affected. It should be a six-month effort with a nod half way through that the July date is still good.

- **Impact of Bright Lines on Timing.** In terms of the methodology for identifying new assets, we did not anticipate the level of new assets. If an entity identifies a new asset, you have to put new security in place and that will take longer than six months.
- The proposed plan addresses assets that become critical under the new methodology.

- If we propose 24 months for newly identified CAs, this will invalidate the current FERC approved CIP implementation plan.
- In essence, the proposal is the industry gets one year, six months for the approval and six months to implement.
- This may involve implementing a whole new program, not just extending existing program and may be very difficult for the industry to implement.
- As a result of the proposed bright lines, the Industry may have a large increase of CAs and then CCAs. We may need more time for addressing that impact.
- The effective date of any other standard is when you can demonstrate you are in compliance which would be a signed list of CAs and CCAs.
- The six months accounts not just for equipment but also personnel

- **Budgeting for Changes.** Under the existing risk-based approach, you can plan and budget for when an asset comes on or off list. Assuming CIP 002-4 is adopted and approved, you may have to be compliant before you can go through a single budget
  cycle. We should consider allowing for more time in order to budget for compliance.
- We have a fiscal policy but not an unchanging budget. Optically, I believe we cannot push out more than two quarters.
- Understand concern about the budgets, but it sounds like we are afraid because we don't know yet what the impact will be and hopefully will know more once survey results come in, we will have a clearer idea of the impacts.
- Our company is partially regulated in Canada. In the past that we have to wait for approved standards before we can include them in the budget. 12-months may be too dicey

- **Survey Information.** To what extent will completion of survey give industry a heads up? It will tell you something is happening but not what to budget for. The survey does not imply money and there is not implementation plan to reference in completing the survey
- Entities cannot budget based on survey results. The bright lines will require upgrades that may require an outage cycle along with budgeting. Compliance within the timeframe proposed may be very difficult.
- The proposal says time starts once the CA is identified which is July 1, 2011. Having a single date simplifies audits.

- **Newly Identified CCA Plan.** Can we put in the existing implementation in modifications for CCAs? Raises the question of whether we use the newly identified CCA plan or not – if not, then have to redo with new dates.

- **Nuclear Generation.** How do we factor in the nuclear industry? If we address implementation for them, we could leverage that to include new sites.

- If unplugging is detrimental to reliability, we do not want to create reverse incentive to undermine reliability.
- Unplugging may work in some cases but we estimate that we are adding up to twenty plants and possibly $150 million for our company under this proposal. The budget cycle then implementation cycle follows including outages. Unscheduled outages are disruptive, and scheduled outages take time. This is primarily a generation issue with some transmission impacts.
- Consider language similar to the nuclear plans, "no later than X date."
- Need to look at exceptions – what new TFEs need to be in place or filed
- The SDT assign a team to draft new implementation plan and address timing in light of these comments?

1. Implementation Plan Proposed Concept- Revised

Following the discussion above the a revised concept statement was presented by John Lim and Scott Mix:

For the initial implementation of CIP 002-4, CCAs at newly identified CAs will be 24 months (i.e., follow Milestone Category 1 in Table 2, Implementation Milestones for Newly Identified Critical Cyber Assets) in the IPFNICCAANRE (Add 706B items and TFEs)

For subsequent implementations of CIP 002-4 at newly identified CAs, the IPFNICCAANRE will be followed as written

For all implementation of newly identified CCAs at existing CAs will follow the IPFNICCAANRE as written.

Discussion of Revised Concept:

- This covers the one time exemption for 24 months for newly identified CCAs at newly identified CAs – everything else is consistent with existing effort.
- Is implementation the appropriate word? Good intent but is it the right word.
- Still need to factor in 706b and when to file TFEs
- Not changing the newly identified CAs – just a one shot in this particular table
- The other implementation plan is already approved and this represents a one shot /one time exception. Not changing the plan but providing a one-time override? How does this play with the new CIP 005 version?
- Does this cover the need for outages to implement?
- It gives them 24 months to incorporate
- In theory the existing plan did not include that either, this gives more time.
- If not changing plan, do we have flexibility to just say 24 months to give people a clear date?

- Today I have zero time for something new – if build something new, do I have 24 months from commission?
- If did not plan for it to be CA but not online yet but will be a CA once commissioned.
- Suggesting 24 months to bring everything into compliance.
- Concerned if some of us are still confused – once turned over to NERC regions, they may interpret differently – needs to be spelled out as simply as possible to limit the potential interpretation confusion
- Second paragraph – next subsequent application is July 2 as part of update as needed – may need to clarify it is the next annual application, not the "as needed during the first year."
- How do you handle a new CA going into service within the 24 month window – if building it now

Straw Poll on Proposal
Favor proposed approach to drafting implementation plan
Yes=9 Oppose=4 Abstain=5

2. Alternative Approaches to Developing the Implementation Plan

Following the poll the SDT identified and discussed the following potential alternative approaches:

a. Implementation plan that requires identification of CAs within 1 quarter and CCAs in 4 quarters. Existing Newly Identified CCA Plan could be used (but the clock would not start for these new CCAs until 4 quarters (12 months) after approval

Or

b. Develop a new implementation plan that allows
   1. 24 months for Newly Identified CCAs and New CAs and
   2. Uses the existing Newly Identified CCAs for New CCAs at existing CAs
   3. Keep the newly identified CCA

Or

c. Add one quarter to Scott Mix's original plan for effective date.

Or

d. Develop a one-shot/one time exception (for specific circumstances) with a sunset to the existing implementation plan schedule.

Or

e. Provide six months for identifying and 24 months to comply.

Member Discussion of Potential Alternatives

- Don't remember modifying process in 002 to identifying CCAs. The proposal did not modify the definition.

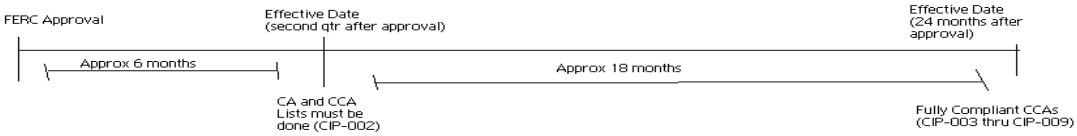
- **Alternative a.** gives a window for plant that does not have a plan.
- in #1 does it buy any time – concerned most about CCA list and identifying when that list has to be in place – having it on the CA list does not necessarily mean it will have CCAs
- **Alternative b.** gives entities time for newly identified, not existing identified assets.
- It uses existing criteria.
- Has to be compliant on day one
- b1.? Does this override one aspect or mean change approved document –
- If 10 and 11 comes in the middle may create issue of overlapping schedules
- FERC staff is nervous about opening up the implementation plan again – would the simple answer be that non-nukes use one plan and nukes another – with exception for more time in specified circumstances?
- Need to leave nuclear open – may come up with a procedure approach
- Concern is mostly about generation rather than transmission? Several transmission stations will also be brought into the mix
- We could move forward with what we have with an addition for exceptions, or build time up front
- What is the time frame for CA and CCA identification and then the time for implementation – when does the race start and how long do you have to finish
- Abstained from the poll because I do not have assets at risk.
- Might also consider from an audit enforcement perspective
- If we do not want to open the implementation plan up then b. and e. are out
- Don't like 24 months which bumps up to the next version and will not fly optically with regulators
- Implementation plan should use the IPFNICCAANRE as it currently exists
- Whatever we use, the visibility is critical to show moving forward on implementation – i.e. a plan that shows we are moving forward with visible dates that can be easily understood.
- What about 18 months? Consider possible TFE for shut down issue?
- Whatever is proposed will need to be justified. It will be easier to justify if tied to something already approved by FERC.
- There seems to be agreement on the concept but we haven't settled on the length for compliance.
- Implementation plain remains as is with a one-time one-shot exception for 18 months, Alternative d. The other half is when to fire the start gun – six months?
- What benefit do we get from all this rather than go with existing plan? Build in buffer
- Use existing implementation plan with process for exceptions if need more time
- Putting in an exception process may take long time to get through legal.
- NERC staff needs some words to take back to compliance director and legal department to see if we can put that into the implementation plan

- Keep in mind time is short to reach agreement on everything to be posted following your September meeting.
- This is offering a one time shot exception – first application of bright line
- Adding in "compliant at 24 months from identification" helps.
- We are talking about CIP 002-009 not just CIP002.
- Should be a date legislators can easily understand and see.

Proposal:

For the initial application of the "bright lines" in CIP 002-4, CCAs at newly identified CAs will be compliant at 24 months from identification (add 706B items and TFEs)

The effective date of the standard (upon the regulatory approval) the registered entity will need to identify CAs and CCAs within six months and xx months to be compliant with 003-009



Discussion Comments

- Effective date is the date FERC approves? It is based on the approval
- There is the issuance date and then effective date. Effective date is the day after auditor can ask for compliance – the date you must have a list with signatures.
- We are looking for the list six months after FERC approval, then 24 months to bring into compliance.
- Move away from the number of months and be sure we have the concept

The Chair and Vice Chair thought there was enough input for a drafting team to develop a new proposal and solicited volunteers for a drafting team to bring back for the SDT's consideration in September.

Implementation Plan Drafting Team Volunteers: Sharon Edwards, Dave Revell, Kevin Sherlin, Scott Rosenberg, Mike Keene (FERC), Dave Norton and Phil Huff

Appendix #8- CIP 010 & 011 Sub-Team Proposal *(Phil Huff)*

Proposal for Sub-Team to Develop Foundational Principles of CIP-011
This proposal was initially presented on Tuesday and discussed in greater detail on Thursday.

The process for the informal comment posting provided little time in developing foundational concepts to applying security controls and industry guidance. Drafting sub-teams must make decisions on applicability according to impact, connectivity and operating environment, but they do not have a common basis for doing so. As CIP-002-4 lacked technical justification for bright-line thresholds, so now CIP-011 lacks a solid basis for determining whether or not a security requirement is appropriate.

Proposal
Form a sub-team to further develop concepts in presenting and scoping cyber security requirements for CIP-011. This would include the form of CIP-011 and basis by which sub-teams write and apply requirements. This would NOT include the actual development of security requirements.
Ideally, team members not heavily involved in the drafting of CIP-002-4 could contribute to this effort. The output of this team would go before the full-team for review and approval once CIP-002-4 has been successfully balloted. The objective of this sub-team would be to further develop concepts in CIP-011 and improve the efficiency of CIP-011 sub-teams.

Issues to Consider
- Impact – what types of security requirements apply at what level?
- Connectivity – How does connectivity factor into applying security requirements?
- Operational Environment – How do different operating environments factor into applying security requirements?
- Type of System Considerations – How do types of systems factor into applying security requirements?
- Technical Feasibility Exceptions – Propose an improved process to allow entities to apply appropriate controls while still satisfying the requirements for transparency and oversight.
- Format – Technically present the Standard in a way that communicates to owners and operators of the BES

Deliverables
- CIP-011 Format Proposal
- Guidance/rationale preamble to CIP-011
  - Description and basis for scoping filters
  - Guidance in reading the CIP-011 format

- Proposal for Technical Feasibility Exceptions

Timeframe: December 2010 Meeting

Appendix # 9 SDT Discussion Notes of CIP 010-011 Schedule and Approach

SDT Member and Participant Comments

On Tuesday the SDT reviewed initially with Allan Mosher the proposed CIP 010-011 schedule and approach. On Thursday, the SDT took up the review of the schedule and tasks for completing its work on the CIP 010 & 011. Phil Huff reviewed with the Team the key highlights of the draft schedule:

- First posting for Formal Comment is proposed for May 31, 2011.
- This assumes an aggressive NERC industry communication campaign to support the effort prior to posting for formal comment.
- By December the SDT will turn its full time attention to CIP 010 & 011.
- By March the SDT will send a package for review with NERC staff, compliance and legal.
- Review in April any edits and Approve in May.

SDT Member and Participant Comments

Stu Langton suggested there was an important discussion of three distinct issues: schedule; preliminary work on next phase; and deeper issue of approach to drafting during the next phase. We may need someone to work on and present a suggestion on the drafting approach for the next phase in Winnipeg.

Schedule & Industry Confusion and Communication

- If we ballot on this schedule and approval in 2012 – period of 2012-13 will be confusing for compliance – anything in this schedule help smooth this for the industry.
- We will be hitting them with ballots just when 002-4 becomes effective
- FERC staff expressed concerns about how aggressive the schedule is – still talking about a draft ready for compliance and legal review by March.
- Howard Gugel noted he is reaching out to communication manager to develop plan – considering series of webinars that look at key components with more focused discussions.
- Are webinars being designed as a one way or two way information process? Allow informal comment or feedback mechanism in the webinars. Once in the ballot phase, it is more difficult to change – you are a representative body of the industry – informal comment lets you hear from the industry and gives you a chance to fix it – need better feedback mechanism from industry.
- Concern with the schedule – did not see any milestone for dealing with inertia of the response to CIP 002-4 – switching back to 010-011 may be a big issue and

difficult sell to industry. Didn't see that dynamic noted in the schedule. As of today, not sure the team is fully behind the change to 010-011. We will need the SDT to come together and a convincing communication plan with the industry of the value to moving toward 010-011.

SDT Deliverables- Short and Long Term

- April 1 is the date that sticks out – that is the last day before turning it over to NERC staff? This version has built in three reviews with the NERC staff.
- This may be aggressive but we have not fully defined the concept. There are bigger issues than just revising standards.

Sub-team Setting Out Proposed Approach for Full Team SDT Review.

- Phil Huff noted he wanted to propose getting a new sub-team to work on material issues between now and December, for example, impact, connectivity, operational environment, type of system considerations, TFEs and format. It could deliver CIP 011 format proposal, guidance and preamble for 011 and a proposal on TFEs for review at the December SDT meeting. They would not look at requirements.
- Understand concept but may also need to consider the overlap of new CIP 005 team. Also heard concerns about potential overlap with 002-4 implementation plan and how aggressive that schedule appears.
- The concept is good idea to compensate for the divergence of CIP 002-4. However still concerned about the fragmentation of the SDT. Once we come together in December we need to reconsider the model of using sub-teams. WE need to go through the requirements as a full team. The results of the proposed effort could give us a start – let this sub-team take a first cut at requirements and house keeping, then starting in December we should focus on full team review given the aggressive schedule – need momentum – feeling numb and disconnected by the current sub-team approach.
- We will need to continue to make changes between meetings – may need to continue a sub-team after December to get pen to paper. The proposal is not to break into subteams during SDT meetings and anticipate full SDT review of work done between meetings.
- Consider using full team webinars between meetings after December.
- Suggest functional areas be assigned for expert drafting to pull together into a strawman that all can review in calls and full team meetings.

SDT Organization in 2011

- As an observer, it appears that the team is good at policy but not at putting pen to paper – use the SDT as a policy group and hire someone to draft the first draft for review by the full group.
- In Sacramento the SDT discussed the need for time. The resulting deal was to work on CIP 002-4 now to December then take another year for 010-011. This draft schedule does that by working back from December 2011 delivery.

- We need to develop and review a more detailed schedule in terms of making sure the resources available. WE cannot manage this project at such a high level of generality and be assured of success.
- We should clarify and adopt clear guidelines for any subteams going forward. Sub-team assignments should be made clear in terms of what to produce and when return to full team.
- Tuesday and Wednesday's work on CIP 002-4 were very productive for this team – everyone understood how we got there.

Overall Approach to CIP

- Dave Norton offered the following thoughts for the SDT to consider in thinking through its schedule for the CIP 010 & 011.
- We are searching for elegant language that covers everything – do not think it is possible to write language that covers our legacy assets and anticipates all the coming changes and challenges. Our product needs to be amenable to changes we have not even seen –
- Our friendly regulator is concerned that we have written one requirement that applies in a binary way based on the size of the iron and not on the risk based approach of NIST which applies no matter the size, then adds more specific language for specific challenges such as data centers. FERC staff urged us to have base layers and add specific requirements for serial, wireless, routability, etc.. That is, protect bastions with physical security, but parse the problem – not one issue with a binary solution. If we don't do this, NERC should expect to face remand.
- Our largest organizations, IOUs, have a weighted impact in terms of ballots as they have the largest investments in the most complex programs, policies and compliance programs in place that have been oriented to the existing 003-009 categories. They are not happy about putting it all into a single 011 standard. Access control is an example.
- The SDT also needs to address "defense in depth" – there is network defense and host defense – more elegant to address access control holistically but most in industry are not prepared to do so. There is a fear that industry will vote it down because they don't like it. An incremental change would be to use the current structure and build off of that.
- 33% of requirements apply to low end is a challenge for FERC review. We need to focus on routable as the vector that needs the most protection – regulator doesn't like 011 and industry doesn't like 011 – schedule is relevant only to extent you identify the path.
- Politics not addressed are the quality of the product you put out – bad optics if industry rejects but almost as bad if you are simply self-reporting constantly – this is too complicated not to have a base for discussion and editing – too long to argue over every word – need to run this as a project – fix it right the first time or just do 706 in the 003-009 frame.

- Have to break this down – this is only drafting team that has to formally use tents – originally intended to break this group into multiple teams – many say they will never create a team this big – cannot solve this problem with everyone sitting in the room – have to have teams break off and use ballot body to comment.
- The question is whether 011 is the right product in FERC's view. There are two core problems with current 002 model: 1) the initial mistake to eliminate the communication links which has now have created islands and failing standards. You don't know what you are protecting – in federal framework we are protecting base and work from there – working backwards from sites and assets. We need clarity on what we are protecting – fix what we are protecting. We may be on the wrong path and facing remand. We haven't clarified what are we protecting against. We have to move to a new model.
- Clearly, as a team, we have problems with the underlying concepts for some on the team, but that doesn't mean we should just scrap work to date. There are still some key questions for team to work out before jumping back into the requirements. Yet we still need to provide a schedule.
- Is the team ready to agree on a schedule? If we don't know what we can deliver how can we know when.
- We've heard and had the same arguments before regarding approaches.
- After robust debate, we agreed on the concept and worked on it. We are now close to where the whole team can work on requirements. All this was forged through a stringent voting requirement that got us to this point. We should consider whether to move on to finish the product or scrap it?
- We are still not looking at security protection and industry view. The major driver is keeping the financial cost and risk low – not on what should we be protecting.
- Cost, however, is a legitimate part of the SDT's consideration.
- We don't know what it will cost in a risk based system.
- We should focus on 706 orders and incremental improvements in the past – but is the product out of date and do we need something completely different? What we have today does not address the problem. We may need to build a new product that works – redefine the problem before we can set the schedule
- Members have to make proposals and if it does not get team support then you have to move forward with the team. It is good to discuss and test these, but we have to move forward as a team – once argument is made and then direction chosen then have to move forward.
- FERC staff: Mike Peters speaks for himself, not the FERC commission or staff – staff and commission said the NERC/SDT should create a baseline then consider specialized protection as needed. CIP 011 is a step in the right direction to applying appropriate protections to different levels. There is no reason the CIP 011 structure cannot fit. One statement cannot fit all – what it is, where it is and how it is protected. I think team can do it, has been productive in Pittsburgh and here in fleshing out Attachment 1 which was, by the way, drafted by a small group. Our

observation is that the small group approach is a valid approach as long it comes back for review, refinement and adoption by the SDT.

- Need to attack our task ahead as a project. We have had no one place to draw on as a source. CIP 003-009 can still work as a base or root stock and we can apply the sub-team work to that frame, use 706 to provide incremental improvement – and we can absolutely make it work by mid year.
- Team is split into I.T. and power engineers – problem in philosophy and finding a mutual mid point we can agree on.
- Take what we have and fix based on 706 request – two glaring issues with current: doesn't cover enough and doesn't cover communications. We are working on the former with CIP 002-4 and the latter can be added by this group. We can do it, it is aggressive but doable. If we don't in six months it will be taken away from us.
- We keep working through different perspectives and appreciate each others talents – still think there are foundational issues that a sub-team can look at between now and December to give us the starting point.
- We have some issues – sub-team needs figure it out and then six months to work as full team
- In Sacramento we said March was doable. With the CIP 002-4 delay, I think that May is doable
- From NERC's perspective, there has been a considerable investment of money and time in developing consensus around 011. The SDT was then were diverted from outside. The SDT needs to decide if investment can be applied to create value. You need to give us a schedule on a solution not just CIP 010-011. You need to ask yourselves if CIP 010-011 is the right approach, and if yes, then go forward and bring it to the industry. If not, then the SDT needs to develop an alternative plan and get to the job.
- Feedback we are receiving from industry to posting is that the High/Medium/Low represents a significant change. Regulators seem to say you need a baseline to build on. Appears that the industry and regulators are at odds and team is trying to walk the line and please both. Taking away 003-009 was too much for industry to digest. Learning to making changes to 003-009 based on 706 – from day one with this team we developed camps about protecting systems. Somehow we keep coming back to feeling among some that the validity of there position has not been addressed.
- This is the elephant in the room – keep 003-009 or come up with a new solution – if we have a quorum, lets decide and move forward.
- We have a target audience and regulators with different expectations and the SDT is between a rock and hard spot – trying to build a consensus between big iron and systems – need to tailor approaches up from a base up, not a top down approach because we continue to get different results from the two models.
- We did vote on the concept, and with less than the 75% support decided to go with 010-011 in order to get the industry comment, refined and got simple majority again/

- Thought we got over hump of the systems approach – don't quite get if we apply 10-11 approach, where are we missing the point, a flawed approach?
- The substance in CIP 011 is not wrong but what is the gain? Is it cosmetic only?
- To clarify issue. If what we have in 011 today is wrong in terms of its content, then we have a threshold issue and problem. On the other hand, if it is the issue of format and having it all in one standard, that should be much easier issued to resolve.
- Concerned about motions and deciding this evening. The proposal to form a team to look at this was a correct approach. Its like we voting against taxes and then asking a team to develop a tax plan.
- In discussing the schedule we didn't start by figuring out requirements and resources then agree on a schedule, instead we have been told what date will be done. However we need to take the date seriously or the job will be taken away not just from the SDT but from the industry.
- The SDT is still not discussing what to protect – format is not substantial issue – we do not have glue between 010 and 011 – still don't have an approach to controls – break up controls based on how they are applied, not by the existing standards – if whole new paradigm then break them out – schedule is good because we do not have any choice
- FERC and congress would be happy with control centers and protect BES and be done. continue the CIP 002 approach that leads to a test program. We worked on and got super majority (75%+) on not using CIP 003-009 structure. There was simple majority support on 011, important concepts in there – naysayers continue to wait and continue to revisit – we can't go back to what we have. However, not in favor of a yea/nay vote today.
- Is there problem with the work on 011 so far? I am pleased with much of that work – keep in mind how far we can move the industry and still move toward the objective – do not want to lose that work, still needs to be vetted – I voted against 010-011, but as a team player I support moving forward and retain good work so far.
- We have power plants that do not affect the system – we would shut them down rather than spend the money to protect them – unintended consequence of protecting everything – some equipment doesn't need to be protected – ask industry what they think – you asked them a million questions and got a million answers –
- FERC staff perspective: industry and regulators may sound like opposites, but not sure that is true. The problem may be more about how to write these concepts into the standards – much of your work facilitates getting the basics out there. John Van Boxtel's format model may offer unique opportunities as the tables did not have sufficient detail. His model proposed making the tables the minimum and then look at extra schedules for specific elements. The SDT is poised to make a necessary paradigm shift to a protection culture. O10 & 011 are looking for protections of assets appropriate to the risk of reliability of BES with appropriate

controls to be applied to address risk to BES. It is less important if in one clump or separate pots.

- My urge for a motion today is just to move forward is born out of frustration of revisiting issue at end of a long day. In Atlanta, we did have super majority (75%) to abandon the CIP 003-009 going forward and we made that call despite industry reaction. The separation of transmission, generation and control centers is not the issue, rather it is the control systems across all of them. The technology based system controls are the issues we need to look at, but we are being told, and have agreed, to provide in the interim a bright line that not a risk based system.
- The SDT was put together to address order 706 and to look at and consider NIST as we modify existing standards based on 706 as a base for future changes. We decided to go to High-Medium-Low. The industry may not yet be ready for a change.
- NERC staff is facilitating rather than managing. Maybe we need to manage, first nail down scope – we have been subject to "scope creep", of plan B and multiple versions to address outside issues. We looked at the structural problems presented by multiple standards and chose to move toward combining into one. We still need a common lexicology too – we should focus on function technological system approach – on h-m-l looking at control systems. Congress does not distinguish between different systems whether corporate, market or control systems . We need to move toward a result based system – compliance and fear of costs is currently driving our process. Going back to to CIP 002-009 will not solve the problem. The industry's comfort with the old system and the sunk costs should not drive our process.
- Many of these comments highlight the issue of communication with the industry – much higher potential for external entry from a connected 25 mw unit than an older 1000 mw unit without connection – communication allows you to tunnel to fifty sites – it is about the control, not the size of the unit.
- So the result may be that the weak link will be shut down as not economic and you may have just degraded the reliability of the network and the grid.
- Some things being proposed still fit into the existing system. We have disagreements on approaches and formats but there has been good quality work to date.
- Back to the discussion of the schedule the proposed schedule on the table to post 010-011 at end of May and passed by end of the year by Board of Trustees

On Friday morning, John Lim reminded team members of importance of working together as a team. He then withdrew his motion on the CIP 010-011 schedule from day before for sake of offering another motion that may be clearer and reflect the good discussion points. Phil Huff noted he will put two motions forward that will describe a process for moving forward on foundational concepts discussed yesterday. The motion moves the posting date for formal comments back to July, 2011 and suggests taking time in front end to set foundation before launching into the requirements in January 2011 providing three more

months for the foundation discussion. Phil Huff made the following motion which was seconded by Dave Norton:

1st Motion for CSO706 SDT Project Schedule

The CSO706 SDT will prepare a complete package for initial posting to the industry for consideration and ballot in July 2011, in response to FERC Order 706, ~~including the requirements, implementation plan, guidance documentation, and other related documents and~~ with the expectation of ballot body approval and filing to FERC by the end of the year 2011. This is contingent upon the SDT being allowed to complete this work without major redirection of SDT efforts. ~~ancillary assignments.~~

16 in Support; 1 opposed (94%)

- Concerned regarding the management of the Team's effort moving forward

Discussion of Motion

- Finite amount of time – before setting out on work take a check point on where we are – a check point restart
- Agree need to review but concerned about targeting completion in middle of next year – resources set for this effort, schedule set, then only thing to adjust is scope – seems a little backwards
- Concern we do not know where we are going and are setting a date – don't know yet what success looks like – make industry happy or the government.
- Politically and optically we need to deliver timely or this process will not exist – time and resources are finite
- We said we would do it right – responsive to 706 and industry – we can put package together by July but not FERC by end of year – we don't control last half of the year.
- Have to deliver something. This is a reasonable motion to move us forward.
- This is not throwing away all the work to date – but still foundational issues to tackle – this reflects time to do that.
- Two paragraphs are tightly linked – need foundation set by December – also concerned that this hits at same time 002-4 adopted in mid summer.
- Why pick a date before we know what we are going to do? Standards Committee requested a date for completing the project – may know better in December the actual date.
- We took a year to do other work – then hit by "plan B" by end of year – that is why we are dealing with this – now they want a stake in the ground for completion – we should focus on 010-011 (if no more curves can we finish?) – Yes, but concerned that 002-4 will set industry into its ways and bolster opposition to 010-011.

- Do I think team can meet July deadline? Yes but we have to educate the industry with a communication plan before presenting for ballot?
- I can provide my time as necessary but what is the scope and time demand on members – a yes vote is a commitment to make this happen – can others meet that commitment.
- Need to provide by end of 2011 – 002-4 will further entrench current methodology – concerned this proposal will support return to 003-009.
- Does not mean we have chosen which direction – second part of motion says we will look at direction – sub-team will not be looking at 011.
- Are we freezing 003-009 in place? Uncomfortable with that possibility.
- Look at language offered here and IT seems going back to earlier discussions of format – are we going back to revisit that? Implying 011 does not stand, revisiting the issue?
- Phil Huff noted that was not the intent. Not about redeveloping concepts but there are many we have not looked at yet.
- Looked at catalogue and developed concept – language here implies sub-teams rewrite sections – some here think fractious conversation is due to lack of full team review – resetting in January?
- If commit to dates and SC. They must make a commitment not to throw us any more curves. Recount to them how many diversions they have made for us. They need to leave us alone to do our work – bilateral commitment.
- Second issue – why take until December to line up our ducks – I volunteer to lead it in two months.
- We have to respond to comments to 002-4 – December the first chance to devote full time to the next stage. We may have time in October to look at it too?
- On the second motion – sub-teams have come back with different formats and content including factors on controls – need more uniform method of targeting those – not redoing the controls but improve targeting to hit those most important.
- July is the team's concern – after July it is on NERC and industry trade associations – critical for NERC to educate the industry on the concepts for industry support. Team can produce quality by July and fails due to lack of communication then that rests with NERC and industry trade associations. We can deliver quality product for industry review in July.
- What we are doing about 002-4 now? What is the communication plan for that? There is confusion in the industry as to what we are doing and why- the ask what happened to 010-011, also, risk to schedule is March 31 response from FERC on 002-4 that asks us to do something else with it.
- Concerned about filing to FERC by end of 2011 – make it "with the expectation of ballot body approval and filing to FERC …." – we control up this up to July, 2011.
- Put period after July 2011 then new sentence: "This schedule would provide the industry with the opportunity to …"
- PH – concerned about the last suggestion – still part of the schedule even if not in our control

- Still responding to the formal comments – prefer "with expectation"
- Complete package implies the subparts will be included – "initial posting to the industry for consideration and ballot in July 2011 with the expectation of ballot body approval and filing to FERC by the end of the year 2011. This is contingent upon the SDT being allowed to complete this work without any ancillary assignments.
- Concern about setting end date you do not control if FERC asks for more in March
- Language assumes FERC does not ask for any additional work on CIP 002-4.
- Question about assignments and distractions – need to include communication or NERC leadership on what we are doing and going – turbulent waters will get muddy in January when CIP 002-4 is posted, also say we want communications that have been missing.
- NERC hears this loud and clear but this team cannot dictate. If this team produces a standard proposal in July, 2011, the ballot body approval will not happen without communication. Communication does not impact team's work but assignments would.
- If additional risks pop up, we should assume it will throw us off schedule.
- Keep struck words referring to 706.
- We know what ancillary assignments are but will others – "without additional major redirection of teams effort."
- Last time it was a request to redirect not an ancillary assignment
- Sounds a little catty – we accepted last assignment and did it and rescheduled
- We have become a standing committee on anything cyber – yes, nested and have to hang together – but this group is not the normal approach to standards development – let us finish before giving us anything else – take out additional to avoid catty?

Phil Huff proposed and Dave Norton seconded a second motion (second paragraph)

2nd Motion Process for Implementing CIP 010-011 Schedule- Framework Sub-Team

The CSO706 SDT will form a sub-team to develop a framework for presenting and scoping cyber security requirements for preliminary delivery in October 2010 and completion in December 2010. This would include the form of the standards and the basis by which the requirements are written and applied. The output of this team would go before the full-team for review and approval. This task would not include the actual development of security requirements.

In Favor of the Motion
Yes=17 No=0 Unanimous

Member Discussion of the Motion before the Vote

- Agree with the intent it should be clear to those writing the requirements as to how to write them. Go together as a framework that will need joint discussion. The Sub-team should take an initial stab at writing initial requirements.
- Should it take it to point of filing in the blanks? By October should present the direction to the SDT and then finalize in December. Cut and paste what we have and let full group redirect in October and December as needed
- Concerned about waiting with the current Sub-teams. We cannot afford to wait – would continue subteam work on requirements then full team review –
- Drop "sub-teams" and just say "by which the requirements are written and applied."
- This proposal draws on the essence from Phil's first proposal (*See Appendix 8)*. Much of that detail is in the original to set framework for hanging the requirements – it offered specific suggestion of issues to look at from our earlier questions – something of a quality check-list.
- We need to talk about the fundamental framework and logic for attacking the requirements. –A style guide is a good description but may need some refinement first.
- Concern with first half – we often break down when concepts brought back to full group an get lost in the woods of word-smithing deferring the more foundational discussion which now must happen in order to set our core message.
- Specific deliverable for this Sub-team should not be a concept paper. Perhaps it should say framework. A**c**cept amendment for framework instead of concept
- Intent is to "develop a framework" not "further"
- The intent is it incorporate and not disregarding the raw material have worked on to date – preliminary delivery in October to the full team and presentation to the full SDT in December for refinement and adoption.

The Chair asked for volunteers for the Framework Sub-Team and the following members and participants responded.:

- Dave Norton (Lead)
- John von Boxtel
- Joe Doetzl
- Dave Revill
- Doug Johnson
- Phil Huff
- Jon Stanford

Other volunteers included:

- Mike Keane
- Scott Mix
- Joe Bucciero (Facilitator)

It was agreed that Joe Bucciero would send a note to those members of the SDT not present asking for others who might want to volunteer

Following the vote the SDT agreed on the following direction to the current CIP-011 Sub-Teams: We need the output from the sub-teams on responses to industry comments and workshop comment summaries so they can be posted in October and recognize industry's investment into those comments.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Agenda
Cyber Security Order 706 SDT — Project 2008-06

Thursday, August 26, 2010 | 12:00 – 4:00 p.m. EDT
ReadyTalk Phone Number: 1-866-740-1260
Conference Code: 9815445

1. **Roll Call and Anti-Trust Guidelines**

2. **Progress reports on:**
   - Implementation Plan for CIP-002-4 (Scott Mix/Dave Revill)
   - Guidance Document for CIP-002-4 (John Lim)
   - Any additional input on CIP-002-4 Draft (All)

3. **Summary Response for Attachment 2, CIP-010 (Jackie Collett)**

4. **Updates from Subteam Leads on Response to Industry Comments and Dallas Workshop Comments**
   (Jay Cribb, Sharon Edwards, David Revill, Doug Johnson, Scott Rosenberger, Scott Mix)

5. **CIP 005-4 Urgent Action SAR Posting & Impact on the CSO706 SDT Work (EDWARDS)**

6. **Framework Subteam Progress Report (Norton)**

7. **Review of Action Items**

8. **Schedule for Next CSO706 SDT Meeting (Winnipeg, Manitoba)**

9. **Other Topics**

10. **Adjourn**

116-390 Village Blvd.
Princeton, NJ 08540
609.452.8060 | www.nerc.com

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Minutes
Cyber Security Order 706 SDT — Project 2008-06

August 26, 2010 |12:00 p.m. - 2:00 p.m.

Joe Bucciero welcomed members and other participants, took roll call and provided the Anti-trust guidance. 14 members of the SDT joined on the call. Chair John Lim set forth the agenda noting it was not a decision-making meeting but a review of progress on the CIP 002-4 documents that need to be reviewed and adopted by the Team for posting.

Dave Revill provided an overview of the CIP 002-4 Implementation Plan sub-team's work since the Chicago meeting and answered questions regarding the proposal. John Lim provided an overview of the draft of the CIP 002-4 Guidance Document that will be refined for presentation at the CSO706 SDT meeting in Winnipeg. Joe Doetzl suggested that a different title for the CIP 002-4 Guidance Document be considered as to avoid confusion with the "Identifying Critical Cyber Assets" guidance document that was recently released by CIPC and approved.

John Lim noted the CIP 002-4 NERC standards and legal edits have been circulated. It was noted an additional criteria in Attachment 1, 1.16 (Any facility declared critical by a regulatory agency) was added by NERC staff and will need to be reviewed as part of the document approval process in Winnipeg to determine whether it will remain in the standard text as part of the posting. Also the control center vs. control room discussion, including their geographical locations, which is part of the CIPC guidance document should be considered.

Jackie Collett noted she was developing the Summary Response for Attachment 2, CIP-010 for the purpose of filing with the CIP-002-4 documents and would circulate a draft in advance of Winnipeg. Updates from each of the CIP-011 Sub-team Leads (Phil Huff for Jay Cribb, Sharon Edwards, David Revill, Doug Johnson, Tom Stevenson for Scott Rosenberger) were provided, and each discussed their progress regarding preparation of a summary response to the Industry Comments and Dallas Workshop Comments. It was agreed that the sub-teams will complete the review of the Dallas Workshop transcript by the Winnipeg meeting, so that it can be posted on the NERC project site for Project 2008-06 (CSO706). The sub-teams will also complete the summary response to the Industry comments received with the informal posting of CIP-010, since these requirements are very close to those in CIP-002-4. The SDT will continue to work on the responses to the CIP-011 comments, and will finalize the summary response to those comments following the adoption of the Framework sub-team's work for CIP-011. The target is to post these responses to comments along with the posting of the revised CIP-010 and CIP-011 standards in 2011.
The Framework sub-team, appointed in Chicago and led by Dave Norton, reported on their first meeting noting they have established a meeting schedule and will be ready to present their preliminary approach

at the October meeting in Toronto. He noted that the SDT will need to clarify early on what protecting ourselves means. What are we trying to protect, and what are we trying to protect against?

Howard Gugel and Scott Mix provided an update on the CIP 005-4 Urgent Action SAR Posting & Status. Pre-ballot review of the SAR is scheduled to complete on September 17, 2010.

It was noted that the Chicago draft meeting summary has been circulated to the SDT and will be reviewed in Winnipeg. The Winnipeg agenda will be circulated following the Leadership Team Call scheduled for next Tuesday (August 31).

The meeting adjourned at 1:55 p.m.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

CSO706 SDT Full Team Conference Call
August 26, 2010
Agenda

1. Roll Call and Anti-Trust Guidelines

2. Progress reports on:
   - Implementation Plan for CIP-002-4 (Scott Mix/Dave Revill)
   - Guidance Document for CIP-002-4 (John Lim)
   - Any additional input on CIP-002-4 Draft (All)

3. Summary Response for Attachment 2, CIP-010 (Jackie Collett)

4. Updates from Subteam Leads on Response to Industry Comments and Dallas Workshop Comments
   (Jay Cribb, Sharon Edwards, David Revill, Doug Johnson, Scott Rosenberger, Scott Mix)

5. CIP 005-4 Urgent Action SAR Posting & Status

6. Framework Sub-Team Progress Report (Norton)

7. Review of Action Items

8. Schedule for Next CSO706 SDT Meeting (Winnipeg, Manitoba)

9. Other Topics

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

SDT Members Attending via ReadyTalk and Phone

1. Rob Antonishen	Ontario Power Generation
2. Jim Brenton	ERCOT
3.Jackie Collett	Manitoba Hydro
4.Joe Doetzl	Kansas City Pwr. & Light Co
5. Sharon Edwards	Duke Energy
6. William Gross	NEI
7. Jeff Hoffman	U.S. Bureau of Reclamation, Denver
8. Phillip Huff, Vice Chair	Arkansas Electric Coop Corporation
9. Doug Johnson	Exelon Corporation – Commonwealth Edison
10. John Lim, Chair	Consolidated Edison Co. NY
11. David Norton	Entergy
12. David S. Revill	Georgia Transmission Corporation
13. Tom Stevenson	Constellation Energy
14William Winters	Arizona Public Service, Inc.
Scott Mix	*NERC*
Howard Gugel	*NERC*
Joe Bucciero	*NERC/Bucciero Consulting, LLC*
Robert Jones	*FSU/FCRC Consensus Center*
Stuart Langton	*FSU/FCRC Consensus Center*
Hal Beardall	*FSU/FCRC Consensus Center*

SDT Members Not Participating

Jay S. Cribb	Southern Company Services
Gerald S. Freese	America Electric Pwr.
Rich Kinas	Orlando Utilities Commission
Patricio Leon	Southern California Edison
Scott Rosenberger	Luminant
Kevin Sherlin	Sacramento Municipal Utility District
Jonathan Stanford	Bonneville Power Administration
Keith Stouffer	National Institute of Standards & Technology
John Van Boxtel	WECC
John D. Varnell	Technology Director, Tenaska Power Services Co
Bradley Yeates	Southern Nuclear Operating Company

Other Participants

Dave	Batz	dbatz@eei.org
David	Gordon	dgordon@mmwec.org
Rod	Hardiman	rchardim@southernco.com
Ashu	Mukherji	ashu.mukherji@pseg.com

Peter	Brown	peter.brown2@pgnmail.com
David	Jeon	djeon@semprageneration.com
Barry	Lawson	barry.lawson@nreca.coop
Roger	Fradenburgh	rfradenburgh@netsectech.com
Matt	Dale	matthew.dale@ferc.gov
Travis	Borrini	tborrini@ameren.com
andres	lopez	andres.lopez@usace.army.mil
Mike	Keane	micahel.keane@ferc.gov
Robert	Green	robert.green@pseg.com
Justin	Kelly	Justin.Kelly@ferc.gov
Bill	Glynn	bill.glynn@westarenergy.com
Hoang	Ngo	hngo@rrienergy.com
Ingrid	Rayo	ingrid.rayo@constellation.com
Nathan	Mitchell	nmitchell@appanet.org
James	Fletcher	jrfletcher@aep.com
Dan	King	daking@sempra.com

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

26th Meeting Summary
Cyber Security Order 706 SDT — Project 2008-06

Adopted Unanimously by the SDT on October 14, 2010

Winnipeg Manitoba

September 8, 2010, Wednesday - 8 AM to 6 PM CDT
September 9, 2010, Thursday - 8 AM to 6 PM CDT
September 10, 2010, Friday - 8 AM to 10 AM CDT

Robert Jones, Stuart Langton, and Hal Beardall
Facilitation and Meeting Design
FCRC Consensus Center, Florida State University

Joe Bucciero, Bucciero Consulting, LLC

http://www.nerc.com/filez/standards/Project_2008-06_Cyber_Security.html

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

CSO706 SDT September 8-10, 2010 Meeting Summary Contents

Cyber Security Order 706 SDT- Project 2008-06
26TH MEETING
September 8-10, 2010
Winnipeg, Manitoba

EXECUTIVE SUMMARY

On Wednesday morning, John Lim, Chair & Phil Huff, Vice Chair of the CSO 706 SDT welcomed members and other participants to Winnipeg and thanked Jackie Collett and Manitoba Hydro for hosting the meeting. Jackie reviewed the logistics for the meeting. Joe Bucciero conducted a roll call of members and participants in the room and on the conference call. Mr. Bucciero also reviewed the need to comply with NERC's Antitrust Guidelines each day of the meeting, and reminded all participants that the meeting has been publicly noticed and is open to the public. The meeting began with a quorum of 15 members in the room and 3 members participating by ReadyTalk conference call. John Lim reviewed the proposed meeting objectives; facilitator Bob Jones reviewed and the SDT agreed to the proposed timed agenda.

On Thursday morning, the SDT unanimously adopted the August 10-13, 2010 Chicago SDT meeting summary and the August 26, 2010 SDT Conference Call Summary.

Vice Chair Phil Huff reviewed the note that the SDT leadership sent to Standards Committee Chair, Allen Mosher, regarding the schedule for CIP 010 & CIP-011, which was adopted by the SDT during the Chicago meeting in August 2010. The note calls for a NERC-led communications and industry outreach effort along with a posting of the CIP-010/CIP-011 standards in July 2011 and adoption of the standards by the NERC Board of Trustees in December 2011.

He also reviewed the CIP 002-4 schedule noting a Webinar has been scheduled for September 29, a week after the scheduled CIP 002-4 posting for a 45 day formal comment period. The SDT reviewed the Webinar preparation on Friday morning. In October the SDT will meet in Toronto and will be taking an initial look at the work of the Framework Sub-Team led by David Norton. During the November meeting in Baltimore, the SDT will be reviewing and responding to industry comments and determining what changes to make to CIP 002-4 before posting for the 2nd ballot. In December, the SDT will be reviewing the recommendations from the Framework Sub-Team and determining the course for the further development of the CIP standards in 2011.

The SDT heard industry updates and discussed the following: the process for the urgent action CIP 005; the CAN 7 revision and review; the formation of a national electric sector cyber security organization called NESCSO at NETL; the final release of the NIST IR7628 (termed as a "guideline" but treated in the Federal sector like a standard); the DHS Cyber Security Roadmap for critical infrastructure activities; and the October NERC annual standards meeting in St. Louis.

John Lim provided an overview of the work done by the CIP-002-4 drafting sub-team in refining the draft CIP 002-4 standard text following the Chicago meeting. The SDT reviewed and analyzed industry responses to the NERC Data Request as input to Attachment 1 of the CIP-002-4 standard, and reviewed and refined several associated documents including: an implementation plan, a guidance/reference document including rationales for Attachment 1 and a summary of industry informal comments on CIP-010 Attachment 2, on which CIP-002-4 Attachment 1 is based. Howard Gugel reviewed the process for posting CIP-002-4.

The SDT discussed the schedule for urgent action CIP-005, and it was clarified that it will be balloted separately, but will run in parallel with CIP-002-4. The revision to CIP-005-3 was posted for a 30-day pre-ballot review on August 18, 2010, and the draft CIP-005-4 standard is scheduled for a 10-day ballot period beginning on September 17, 2010. No recirculation ballot is planned.

On Wednesday morning, NERC staff (Howard Gugel) reviewed with the SDT the initial analysis of industry responses to the draft NERC Data Request. Following some further clarification and discussion with several Data Request respondents, Howard reviewed with the SDT on Thursday the adjusted results in the number of assets in the low impact category (from around 1300 to around 530).

The SDT reviewed each section of the CIP 002-4 draft, and as needed, conducted straw polls on the acceptability of the language.

CIP 002-4 SDT Straw Polling and Decisions on Motions	***Yes***	***No***	***Abstain***	***%***
Requirements				
R2 as proposed by the Drafting Team	**20**	**0**		**100%**
Attachment 1 Criteria				
1.1 as proposed by the Drafting Team	10	5	4	
1.1 Alternative ("…aggregate highest rated net Real Power capability of the preceding 12 months equal to or exceeding 2000 MW."	13	6	2	
1.1 Choice #1 ("Use a numerical MW value that approximates the reserve sharing for each NERC region.")	7	9		44%
1.1 Choice #2 ("Use numerical MW value that approximates an average of the reserve sharing amounts across all regions")	12	6		67%
1.1 Choice #3 (Use the Reserve Sharing concept, rather than a MW value, but include additional descriptions supplied by Control Center experts	13	4		76%
1.1 Choice #4 ("Use the Reserve Sharing concept, rather than a number, as it was proposed at the start of this meeting.")	10	5	4	
1.1 "Each group of generating units (including nuclear generation) at a single plant location with an aggregate highest rated net Real Power capability of the preceding 12 months equal to or exceeding 1500 MW.	**19**	**0**		**100%**
1.2 Each generation Facility that the Planning Coordinator or Transmission Planner designates as required for reliability purposes."	**13**	**2**	**4**	
1.5 As proposed by the Drafting Team	**11**	**3**	**5**	
1.5 Alternative *(Rich Kinas language)*	**1**	**17**	**0**	

1.5 *As rewritten*-The Facilities comprising the Cranking Paths and initial switching requirements from the Blackstart Resource to the unit(s) to be started, as identified in the Transmission Operator's restoration plan up to the point on the Cranking Path where multiple path options exist.	**16**	**1**	**3**	
1.7 As proposed by the Drafting Team	**17**	**0**	**2**	
1.8 As proposed by the Drafting Team	**17**	**0**	**3**	
1.8 Alternative language (proposed by Jason Marshall)	0	18		
1.9 As proposed by the Drafting Team	19	0		
1.10 As proposed by the Drafting Team	18	0	3	
1.11 As proposed by the Drafting Team	20	0		
1.12 As proposed by the Drafting Team	20	0		
1.13 As proposed by the Drafting Team	18	2		
1.14 As proposed by the Drafting Team	16	2	2	
1.15 As proposed by the Drafting Team	15	2	2	
1.15 Delete "in an single interconnection"	6	12	1	
1.16 "Any facility declared by a regulatory agency to be critical to national security."	0	19	0	
1.17 "Any additional assets that the Responsible Entity deems appropriate to use."	17	3	0	
Motion to Approve Attachment 1 as Revised *(S. Edwards; 2nd D. Johnson)*	**18**	**1**		**95%**
Implementation Plan Timeline- Overall 24 months (6 months for identification of critical assets and 18 months for critical assets in compliance)	**18**	**0**	**0**	
Motion to Approve to Implementation Plan as Revised	**18**	**0**		
Motion to Approve CIP 002-4 Reference Document	**18**	**0**	**1**	
VSLs/VRFs as revised	**19**	**0**		
Cover Letter and Comment Form as revised	**19**	**0**		

The SDT reviewed a draft agenda and proposed assignments for an industry webinar on September 29 from 11:00 a.m. -1 p.m. on the CIP 002-4 filing, which the Chair outlined. Allen Mosher, Chair of the NERC Standards Committee will provide some introductory remarks in terms of the context and recent history of the SDT's efforts. It was noted that the presentations would be at a relatively high level with the intention of leaving sufficient time of the Webinar devoted to Q & A. There will also be a short presentation by an industry representative member of the CIP 005 urgent action work group on the substance and procedure for that draft standard.

Dave Norton, Sub-Team lead, reported on the two meetings the Framework Sub-Team has convened. He suggested the context is that some in the industry stakeholders did not like what they saw with CIP-011, and the regulator doesn't think we have approached things consistently with the NIST 800-53 framework, thereby establishing a baseline at the outset. The Sub-Team has agreed that the SDT needs to answer the question, "what are we protecting and from who?" There are threats, vulnerabilities and impacts to consider but threats are hard to be clear on, and impacts have a lot of permutations. The Sub-Team is initially focusing on known vulnerabilities in the open information sources and posing the question: how can we use known vulnerabilities to link to specific standards (e.g., NIST IR volume 3, Chapter 7 treatment of vulnerabilities). The original CIP standard team learned that it is very difficult to write CIP requirements that address the old and new at the same time,

resulting in overkill for the old and leaving modern vulnerabilities unaddressed. The output should be a justification and rationale underpinning the standards, not the standards themselves. They are starting with a framework for the CIP standards, and not a format. Ultimately this should lead to a format.

Dave Revill noted that when the SDT developed CIP-011, we identified requirements at the high impact level and forced the scoping elements on them. The Framework Sub-Team's idea is to start from the bottom and work up.

The Chair noted that the Framework Sub-Team will have a significant amount of agenda time during the Toronto SDT Meeting in October to bring the SDT up to date and engage them in discussion of the key issues. These discussions should provide guidance as the Sub-Team continues its efforts to bring back a framework that the SDT can review, refine, and adopt at its December 2010 meeting that will guide its work in 2011.

On Friday morning, the SDT reviewed the progress being made by the CIP-010 and CIP-011 sub-teams in summarizing industry responses and the Dallas workshop comments. The Chair thanked those sub-groups who had completed their tasks and asked all the sub-groups to complete their summaries by the SDT October meeting

The Chair reviewed the schedule for a SDT conference call meeting on Wednesday, September 15 from 10:00 a.m.-12:00 p.m. (eastern time) to review the final documents for posting that were not adopted at this meeting and to determine whether the SDT members, following review with their corporate senior management, wanted to revisit the SDT's previous decisions on whether to specifically include all nuclear generation as a criterion for assessment in CIP-002-4 Attachment 1.

The Toronto agenda was discussed and SDT member and host Rob Antonishen described the Toronto, Ontario venue for the meeting.

Meeting adjourned at 9:45 a.m. Friday, September 10, 2010

_____

Cyber Security Order 706 SDT- Project 2008-06
26TH MEETING SUMMARY
September 8-10, 2010
Winnipeg, Manitoba

I. AGENDA REVIEW, WORKPLAN SCHEDULE AND UPDATES

A. Agenda Review and Adoption of Meeting SDT Summaries

John Lim, Chair & Phil Huff, Vice Chair of the CSO 706 SDT welcomed members and other participants to Winnipeg and thanked Jackie Collett and Manitoba Hydro for hosting the meeting. Jackie covered logistics and noted a tour of the new energy efficient Manitoba Hydro building at the end of the day. Joe Bucciero conducted a roll call *(See Appendix #2)* and reviewed the antitrust and public meeting guidelines *(See Appendix #3)* with the meeting participants at the outset on each day. On Thursday morning, the SDT unanimously adopted the August 10-13, 2010 Chicago meeting summary and the August 26 SDT Conference Call Summary. The meeting began with a quorum of 15 members in the room and 3 members participating by Readytalk conference call. John Lim reviewed the proposed meeting objectives, the facilitator Bob Jones reviewed and the SDT agreed to the proposed timed agenda.

B. Update on the CIP 002-4 and the 010 and 011 Development Schedule

Vice Chair Phil Huff reviewed the note that the SDT leadership sent to Standards Committee Chair, Allen Mosher, regarding the schedule for CIP 010 & CIP-011, which was adopted by the SDT during the Chicago meeting in August 2010. The note calls for a NERC-led communications and industry outreach effort along with a posting of the CIP-010/CIP-011 standards in July 2011 and adoption of the standards by the NERC Board of Trustees in December 2011.

He also reviewed the CIP 002-4 schedule noting a Webinar has been scheduled for September 29, a week after the scheduled CIP 002-4 posting for a 45 day formal comment period. The SDT reviewed the Webinar preparation on Friday morning. In October the SDT will meet in Toronto and will be taking an initial look at the work of the Framework Sub-Team led by David Norton. During the November meeting in Baltimore, the SDT will be reviewing and responding to industry comments and determining what changes to make to CIP 002-4 before posting for the 2nd ballot. In December, the SDT will be reviewing the recommendations from the Framework Sub-Team and determining the course for the further development of the CIP standards in 2011.

C. Updates on other related cyber security initiatives- *NERC Staff and SDT Members*

The SDT discussed the schedule for urgent action CIP-005, and it was clarified that it will be balloted separately, but will run in parallel with CIP-002-4. The revision to CIP-005-3 was posted for a 30-day

pre-ballot review on August 18, 2010, and the draft CIP-005-4 standard is scheduled for a 10-day ballot period beginning on September 17, 2010. No recirculation ballot is planned.

Scott Mix also noted that the CAN 7 was under review and was being prepared for review by NERC legal staff next week. Jim Brenton noted that CAN 5 is on track for implementation in October and that there are likely to be a lot of concern in the industry about this CAN.

The SDT heard industry updates and discussed the following: the process for the urgent action CIP 005; the CAN 7 revision and review; the formation of a national electric sector cyber security organization called NESCSO at NETL; the final release of the NIST IR7628 (termed as a "guideline" but treated in the Federal sector like a standard); the DHS Cyber Security Roadmap for critical infrastructure activities; and the October NERC annual standards meeting in St. Louis.

Keith Stouffer reported that last Thursday the NIST IR 7628 was finalized and is now available on the website for down load. He noted that while it is termed as a "guideline" it is treated in the Federal sector like a standard.

Gerry Freese noted the DHS Cyber Security Roadmap which provides guidance for critical infrastructure activities has been released for comment and indicated some concerns with load issues, interdependencies and other issues. It was noted that it was on the agenda for discussion at next week's CIPSE meeting. Sharon Edwards had read it and suggested there is some overlap with the work of the SDT. Scott Mix noted that Section 215 addresses the areas for which NERC can write enforceable standards.

Howard Gugel noted that at the October NERC annual standards meeting in St. Louis, he will make a presentation on the evolving work of the SDT on CIP-010 and CIP-011.

II. SDT CIP 002-4 DOCUMENT REVIEW

A. Overview and Process

John Lim provided an overview of the work done by the CIP-002-4 drafting sub-team in refining the draft CIP 002-4 standard text following the Chicago meeting. The SDT reviewed and analyzed industry responses to the NERC Data Request as input to Attachment 1 of the CIP-002-4 standard, and reviewed and refined several associated documents including: an implementation plan, a guidance/reference document including rationales for Attachment 1 and a summary of industry informal comments on CIP-010 Attachment 2, on which CIP-002-4 Attachment 1 is based. Howard Gugel reviewed the process for posting CIP-002-4.

Howard Gugel reviewed the process for posting CIP-002-4:

- The documents will be posted for 45-day formal comment period during which the first 30 days a ballot pool will be formed. On the 35th day, there will be a concurrent ballot for 10 days.
- Any comments received will require responses. With the short turnaround, NERC staff will assist the SDT in drafting strawman response document.
- The SDT will review the responses and determine whether to change any provision CIP-002-4 in Baltimore in November. NERC standards and legal staff will review and the response document will be posted.
- The 2nd ballot period will run for 10 days.
- The Team will respond to comments and post for a 3rd ballot in December

The SDT discussed the schedule and clarified whether urgent action CIP 005 will be a part of the CIP 002-4 etc posting. There will be a separate ballot on urgent action CIP 005-4 which will run parallel with CIP-002-4 and the ballot will open on September 20 for 10 days with no recirculation. If CIP-005 is turned down, then NERC would publish CIP 005-3 with conforming changes from CIP-002-4.

B. Briefing on the NERC Data Request Results

On Wednesday morning, NERC staff (Howard Gugel) reviewed with the SDT the initial analysis of industry responses to the draft NERC Data Request. *(See Appendix #4)* Following some further clarification and discussion with several Data Request respondents, Howard reviewed with the SDT on Thursday the adjusted results in the number of assets in the low impact category (from around 1300 to around 530). He also pointed out the new provision added to the Attachment #1 (the new 1.16) would be supported by the number of assets included in this category in the survey.

C. Review and Refinement of the CIP 002-4

The SDT reviewed each section of the CIP 002-4 draft, and as needed, conducted straw polls on the acceptability of the language. The final adopted text is included in Appendix #5. Below is a list of the straw polls and decisions reached by the SDT on the CIP 002-4 documents:

CIP 002-4 SDT Straw Polling and Decisions on Motions	*Yes*	*No*	*Abstain*	*%*
Requirements				
R2 as proposed by the Drafting Team	**20**	**0**		**100%**
Attachment 1 Criteria				
1.1 as proposed by the Drafting Team	10	5	4	
1.2 Alternative ("…aggregate highest rated net Real Power capability of the preceding 12 months equal to or exceeding 2000 MW."	13	6	2	
1.2 Choice #1 ("Use a numerical MW value that approximates the reserve sha each NERC region.")	7	9		44%
1.2 Choice #2 ("Use numerical MW value that approximates an average of the sharing amounts across all regions")	12	6		67%
1.2 Choice #3 (Use the Reserve Sharing concept, rather than a MW value, but additional descriptions supplied by Control Center experts	13	4		76%
1.2 Choice #4 ("Use the Reserve Sharing concept, rather than a number, as it was proposed at the start of this meeting.")	10	5	4	
1.3 "Each group of generating units (including nuclear generation) at a single plant location with an aggregate highest rated net Real Power capability of the preceding 12 months equal to or exceeding 1500 MW.	**19**	**0**		**100%**
1.3 Each generation Facility that the Planning Coordinator or Transmission Planner designates as required for reliability purposes."	**13**	**2**	**4**	
1.5 As proposed by the Drafting Team	**11**	**3**	**5**	
1.5 Alternative *(Rich Kinas language)*	**1**	**17**	**0**	
1.5 *As rewritten*-The Facilities comprising the Cranking Paths and initial switching requirements from the Blackstart Resource to the unit(s) to be started, as identified in the Transmission Operator's restoration plan up to the point on the Cranking Path where multiple path options exist.	**16**	**1**	**3**	
1.7 As proposed by the Drafting Team	**17**	**0**	**2**	
1.8 As proposed by the Drafting Team	**17**	**0**	**3**	
1.8 Alternative language (proposed by Jason Marshall)	0	18		
1.9 As proposed by the Drafting Team	19	0		
1.10 As proposed by the Drafting Team	18	0	3	
1.11 As proposed by the Drafting Team	20	0		
1.12 As proposed by the Drafting Team	20	0		
1.13 As proposed by the Drafting Team	18	2		
1.14 As proposed by the Drafting Team	16	2	2	
1.15 As proposed by the Drafting Team	15	2	2	
1.15 Delete "in an single interconnection"	6	12	1	
1.16 **"**Any facility declared by a regulatory agency to be critical to national securi	0	19	0	
1.17 "Any additional assets that the Responsible Entity deems appropriate to use."	17	3	0	
Motion to Approve Attachment 1 as Revised *(S. Edwards; 2nd D. Johnson)*	**18**	**1**		**95%**
Implementation Plan Timeline- Overall 24 months (6 months for identification of critical assets and 18 months for critical assets in compliance)	**18**	**0**	**0**	
Motion to Approve to Implementation Plan as Revised	**18**	**0**		
Motion to Approve CIP 002-4 Reference Document	**18**	**0**	**1**	
VSLs/VRFs as revised	**19**	**0**		
Cover Letter and Comment Form as revised	**19**	**0**		

1. CIP 002-4 Requirements

R1. Critical Asset Identification — Each Responsible Entity shall develop a list of its identified Critical Assets determined through an annual application of the criteria contained in *CIP-002-4 Attachment I – Critical Asset Criteria*. The Responsible Entity shall review this list at least annually, and update it as necessary.

SDT Comments

- R1 and R2- "updated as necessary"? What is the metric? "Where appropriate"? "Based on the annual review." A: "one calendar quarter after discovery of a new asset."
- "Annual" has been a thorn for the SDT for a long time.
- We should keep it the way it is using the "minimalist" rule for CIP 002-4.
- This also appears and would need to be changed in CIP 003-009.
- It is frustrating when we can make a simple change and improve the standards but don't.
- Have language in CIP 10 as well. Identified and addressed.
- Note that the SDT voted last time 17-0 to accept this language.
- The SDT should be careful of scope creep: on 002-4. Will fix and do correctly.

Howard Gugel 9/28/10 4:36 PM
Comment: Actually, we addressed the low hanging fruit initially.

R2. Critical Cyber Asset Identification — Using the list of Critical Assets developed pursuant to Requirement R1, each Responsible Entity shall develop a list of associated Critical Cyber Assets. The Responsible Entity shall review this list at least annually, and update it as necessary. For each group of generating units (including nuclear generation) at a single plant location identified in Attachment 1, criterion 1.1, the only Cyber Assets that must be considered are those shared Cyber Assets that could adversely impact the reliable operation of any combination of units that in aggregate exceed Attachment 1, criterion 1.1 within 15 minutes. For the purpose of Standard CIP-002-4, Critical Cyber Assets are further qualified to be those having at least one of the following characteristics:

R2.1 The Cyber Asset uses a routable protocol to communicate outside the Electronic Security Perimeter; or,

R2.2The Cyber Asset uses a routable protocol within a control center; or,

R 2.3The Cyber Asset is dial-up accessible.

SDT Comments on R2

- The drafting team added back" performing a function essential to the operation of the Critical Asset."
- R2 "Each" Place qualification ("within 15 minutes) at R2.4
- 15-minute criteria only applies to generation units.

- One of the following characteristics- place in a footnote? 'the only Cyber Assets that must be considered are those shared Cyber Assets that could adversely impact the reliable operation of any combination of units that in aggregate exceed Attachment 1 criterion 1.1 within 15 minutes.
- Intent of sub requirements- applied to the asset's identify at the generator. If below or equal they won't apply.
- A change will require changing all the numbering.
- All comfortable with proceeding with it as proposed?

SDT Straw Poll on R2 As Written

Yes	***No***	***Abstain***
20	**0**	**0**

2. Attachment 1 Criteria

Criterion 1.1

John Lim reviewed the minor changes made in 1.1 since Chicago. The SDT discussed and were polled for their support for 1.1 as written.

> **1.1. A generating unit or group of generating units (including nuclear generation) at a single plant location with an aggregate highest rated net Real Power capability in the preceding 12 months exceeding the lowest Contingency Reserve identified over the preceding 12 months by the Reserve Sharing Group or the Balancing Authority if it is not a member of a Reserve Sharing Group, at the time the CIP-002 is reviewed.**

SDT Straw Poll on 1.1 As Written

Yes	***No***	***Abstain***
10	**5**	**4**

The SDT's initial discussion of the proposed language in 1.1 noted concerns about: utilizing the concept of reserve sharing as a threshold value; the unintended consequence of placing pressure on entities to no carry additional reserve; referencing a term that will fluctuate over time; the difficulty to finding the number as demonstrated in the NERC date request responses; and introducing a new operational term ("planned Contingency Reserve") that does not appear in other standards.

Several potential options were identified including: gigawatt hours per year produced; tie to name plate ratings but address capacity using the test results required to run to demonstrate capacity referencing proposed Mod 24 standard); use contingency reserve to come up with a defensible number, but don't tie the 1.1 to a contingency reserve.

Following the ranking, the SDT discussed that if the contingency reserve is the value we are comparing then it needs clarification in terms of what it is and how it is determined and how to define a "group of generating units."

The SDT then reviewed concerns and support for the following alternative 1.1 language including: this is using the concept to derived a value; this figure is based on disturbance not reliability; having a bright line across each region may not make sense; this is an indirect way to identify critical assets; and bright lines should be readily available and clear for each entity. The SDT then polled support for the following:

> **Alternative 1.1: "Each group of generating units (including nuclear generation) at a single plant location with an aggregate highest rated net Real Power capability of the preceding 12 months equal to or exceeding 2000 MW."**

SDT Straw Poll on 1.1 As Re-written

Yes	***No***	***Abstain***
13	**6**	**2**

Sharon Edwards agreed to draft options for the SDT consideration on Thursday based on the discussion on Wednesday. She summarized the following four options for the SDT's consideration and recommended consideration of Options 1 and 3 to begin with. It was suggested that the SDT needs to make a decision on this and seek industry input through the comment and balloting process.

Choice #1 – Use a numerical MW value that approximates the reserve sharing for each NERC region: Each group of generating units (including nuclear generation) at a single plant location with an aggregate highest rated net Real Power capability of the preceding 12 months equal to or exceeding the amount designated in the following table:

FRCC	900 MW	MW Value approximates the Reserve Sharing amount for that region *(Kinas)*
MRO	2200 MW	MW Value approximates the Reserve Sharing amount for that region (Collect)
NPCC	1200 MW	MW Value approximates the Reserve Sharing amount for that region *(Lim)*
RFC	2000 MW	MW Value approximates the Reserve Sharing amount for that region *(Marshall)*
SERC	1200 MW	MW Value approximates the Reserve Sharing amount for that region *(Revill)*
SPP	TBD *(KP)*	MW Value approximates the Reserve Sharing amount for that region *(Perry)*
ERCOT	2300 MW	MW Value approximates the Reserve Sharing amount for that region *(Brenton)*
WECC	TBD*(JVB)*	MW Value approximates the Reserve Sharing amount for that region

Sharon noted that this option allows regional flexibility in setting specific MW value but it is difficult to calculate for each region. The table figures were presented as initial approximations for region based on available information.

SDT Straw Poll on Choice #1

Yes	***No***	
7	**9**	**= 44%**

Comments on Choice #1before Poll

- The numbers are set by Reserve Sharing Group not by regions.
- The NPCC # doesn't reflect number for other areas within the NPCC.
- Need a number that does not change over time. Choice # 3 is more preferable if we can get away from new terms not seen yet by the industry.
- Concerns raised by members may make this problematic. Is 900 MW always critical?
- The table is intended to offer average approximations that can serve as the basis for bright lines. They do not represent an average of every BA in the region.
- 2300 may not be the ERCOT number.
- In favor of the table yesterday. Would still vote for that approach.

Choice #2 – Use numerical MW value that approximates an average of the reserve sharing amounts across all regions: Each group of generating units (including nuclear generation) at a single plant location with an aggregate highest rated net Real Power capability of the preceding 12 months equal to or exceeding 1500 MW.

SDT Comments on Choice #2 before poll

- This is similar to approach with 2000MW. 1500-1600 MW table in Choice 1. Question of the values served by this. Over 900 doesn't work in Florida.
- 1500 MW will capture about 1/3 of generation in US.
- We have used 2000 so far here and elsewhere?
- To address the concern regarding FRCC, it can adopt a more stringent value based on their regional need.

SDT Straw Poll- Choice #2

Yes	***No***	
12	**6=**	**67%**

Comments after poll

- What is the basis of the table. It is a way of drawing a line in the sand.
- Here's how we drew the line.
- Get number out to industry to get reaction.

Choice #3 – Use the Reserve Sharing concept, rather than a MW value, but include additional descriptions supplied by Control Center experts. (*Note: No new definitions are being proposed.)* Each ~~generating unit or~~ group of generating units (including nuclear generation) at a single plant location with an aggregate highest rated net Real Power capability in the preceding 12 months within the Reserve Sharing Group, or a Balancing Authority if it is

not a member of a Reserve Sharing Group, exceeding the lowest planned contingency reserve (Spinning plus Operating Reserves plus additional reserves) over the preceding 12 months at the time the Responsible Entity reviews its list of Critical Assets.

SDT Comments on Choice #3 before the poll

- Based on the SDT discussion yesterday, a little clarification/information (spinning plus) was added to the reserve sharing concept.
- There is a problem with ("spinning plus operating reserves). Concerned with defining this term.

SDT Straw Poll on Choice #3

Yes	***No***	
13	**4=**	**76%**

Comments on Choice #3 after poll

- Why can't we use the nameplate rating here? A: Nameplate is not always the operating capacity.
- How much precision do we need?
- Nameplate is like horsepower of a car.

Choice #4 – Use the Reserve Sharing concept, rather than a number, as it was proposed at the start of this meeting: Each ~~generating unit or~~ group of generating units (including nuclear generation) at a single plant location with an aggregate highest rated net Real Power capability in the preceding 12 months exceeding the lowest Contingency Reserve identified over the preceding 12 months by the Reserve Sharing Group or the Balancing Authority if it is not a member of a Reserve Sharing Group, at the time the Responsible Entity reviews its list of Critical Assets.

SDT Comments on Choice #4 before the poll

- This is the proposal reviewed and polled at start of meeting yesterday with the following results:

Yes	***No***	***Abstain***
10	**5**	**4**

The facilitators noted that both Choice #2 and Choice #3 garnered more than 2/3's support from the SDT. The SDT then voted between their preference as between Choice # 2 and Choice #3 and Choice #2 received greater than 2/3s of the members votes. The SDT agreed that the following should become 1.1:

> **1.1 *(Final)* Each group of generating units (including nuclear generation) at a single plant location with an aggregate highest rated net Real Power capability of the preceding 12 months equal to or exceeding 1500 MW.**

Criterion 1.2
- No changes

Criterion 1.3

"Each generation Facility that the Planning Coordinator or Transmission Planner designates as required for reliability purposes."

SDT Comments before Polling
- Since Chicago the drafting team developed editorial changes.
- EEI suggested language "maintaining the stability and reliability of the BES."
- Does this refer to all units? Broad brush statement will confuse planning and coordination planners
- It needs to be more specific or it shouldn't be incorporated.
- Concept was to try to keep the idea in here.
- 12 units classified reliability must run up to 43 for Data Request Q3.
- Shutting down for security? No for reliability. They want to retire it and you'll require them to
- Go to R&R then goes to market. If it falls out of R&R, will shut down
- Unintended consequence may be a less reliable BES.
- This may work in a market but not in a non-market area. Have to be careful. Some language that- "retirement delayed" Auditors may ask, "Where is your study for every unit?"

Howard Gugel 9/28/10 4:49 PM
Comment: Not sure it is appropriate to include this

SDT Straw Poll on 1.3 As Written

Yes	***No***	***Abstain***	
13	**2**	**4=**	**68%**

Criterion 1.4
- No changes

Criterion 1.5:

"The Facilities comprising the Cranking Paths and initial switching requirements identified in the Transmission Operator's restoration plan."

SDT Straw Poll on 1.5 As Written

Yes	***No***	***Abstain***
11	**3**	**5=**

The SDT comments before polling touched on the following issues: seeking to get to the more the primary or initial cranking path; cranking path can be anything to get to any unit; data request indicated that 438 that will be identified as critical assets with 53 additional sub-stations; will this

bring in a disincentive to designate black start with multiple cranking paths; 1.5 and 1.9 taken together will bring in 627 transmission facilities + 250 generators as critical assets; concern every resource mentioned in operators restoration plan; does the current language enable a stop from 5 to 20 MW; and, generating facilities (keeping the turbine generator on and turning gear going) will have to come off of turning gear.

Following the poll, the SDT discussed: the problem with moving from low MW up to several higher levels; the term "facilities" is not specific to transmission or generation; the fact that 1.5 picks up from 1.4 and follows cranking paths till it reaches multiple path options. An ad hoc drafting group brought back the following language after a lunch break which the SDT agreed to:

> **1.5** *(Rewritten)***The Facilities comprising the Cranking Paths and initial switching requirements from the Blackstart Resource to the unit(s) to be started, as identified in the Transmission Operator's restoration plan up to the point on the Cranking Path where multiple path options exist.**

SDT Straw Poll on 1.5 As Re-written

Yes	***No***	***Abstain***
16	**1**	**3**

The Chair agreed to review draft alternative language that Rich Kinas offered to develop. The following language was reviewed on Thursday by the SDT.

> **1.5 Alternative** *(Rich Kinas)* **"All facilities (transmission and generation) identified in the Transmission Operator's restoration required to start generation and re-establish a minimum of one synchronized tie with a neighbor."**

SDT Straw Poll on Alternative 1.5

Yes	***No***	***Abstain***
1	**17**	**0**

Criterion 1.7

"Transmission Facilities operated at 300 kV or higher at stations interconnected at 300 kV or higher with four or more other stations."

SDT Comments

- There is a substantial drop in CA (70%) when at 4. Drop to 3.
- Dropping the phrase "or generating" addresses his issues.

Howard Gugel 9/28/10 5:18 PM
Comment: Who is his?

SDT Straw Poll

Yes	***No***	***Abstain***
17	**0**	**2**

Criterion 1.8

"Transmission Facilities at a single station location that, if destroyed, degraded, misused or otherwise rendered unavailable, violate one or more Interconnection Reliability Operating Limits (IROLs)."

SDT Straw Poll

Yes	***No***	***Abstain***
17	**0**	**3**

Comments on 1.8

- Need to protect bus breakers on both ends of that line, i.e. at 2 stations not one. Take out "at a single station"?
- Without this we will have compliance issues, could have to deal with multiple locations. Don't believe the SDT has words on 1.8 right. Not going to violate an IROL. Jason Marshall will take a crack at different words for the SDT to consider.
- The Chair suggested we would come back to alternative language if it can improve its acceptability.

*Jason Marshall's alternative 1.8 language reviewed on 9-9. "***Transmission facilities that if destroyed, degraded, misused, or otherwise rendered unavailable, cause a reduction in an IROL magnitude or cause a new IROL to be identified."**

SDT Straw Poll

Yes	***No***
0	**18**

SDT Comments before the poll

- Do I have to evaluate all transmission facilities? That was why we had the language "at a single station location."
- How are TOP and planners to make these determinations? We may need examples for each of the key functions?
- We can go back to highlight resources we used initially in the drafting team in the guidance document. Works for ISOs.
- TOP and other transmission people may have trouble with this.

Criterion 1.9

"Flexible AC Transmission Systems (FACTS) at a single station location, that, if destroyed, degraded, misused or otherwise rendered unavailable, violate one or more Interconnection Reliability Operating Limits (IROLs)."

SDT Comments

- No changes
- There were 0 assets on the survey.
- Intent to capture future- criticality for BES. If no purpose do we need this? Why called out? A: Because they have huge cyber systems which are easy to attack.
- **SDT Agreed to leave 1.9 in Attachment #1**

Criterion 1.10

"Transmission Facilities providing the generation interconnection required to directly connect generator output to the transmission system that, if destroyed, degraded, misused, or otherwise rendered unavailable, would result in the loss of the assets described in Attachment 1, criterion 1.1 or 1.3."

SDT Straw Poll

Yes	*No*	*Abstain*
18	**0**	**3**

SDT Comments

- For criteria 9,10 and 12, "Misuse" different from the others
- "Misuse" –in order to cause a problem with the IROL. This is already covered.
- **SDT Agreed to leave 1.10 in Attachment #1**

Criterion 1.11

"Transmission Facilities identified as essential to meeting Nuclear Plant Interface Requirements."

SDT Comments

- No changes
- This is a nuclear safety deal, vs. reliability issue.
- Tied to Nuc 001- in terms of safety.
- **SDT Agreed to leave 1.11 in Attachment #1**

Criterion 1.12

"Each Special Protection System (SPS), Remedial Action Scheme (RAS) or automated switching system that operates BES Elements that, if destroyed, degraded, misused or otherwise rendered unavailable, violate one or more Interconnection Reliability Operating Limits (IROLs)."

SDT Comments

- Consistency editorial change by the Drafting Group.
- **SDT Agreed to leave 1.12 in Attachment #1.**

Criterion 1.13.

"Common control system(s) capable of performing automatic load shedding of 300 MW or more within 15 minutes."

SDT Comments before polling

- The SDT found the NERC edits acceptable.
- "common"= shared?
- Language was taken out of Version 3.
- Because of the development of smart grid this is a bigger issue than it was in Version 1, 2 and 3.
- Put in 15 minute or real time. It is now pre-programmed into the device in the firm ware of the thermostat.
- This could be a problem without a time element.
- "Simultaneous" or "within a 15 minute period"?
- Issues with the smart grid are longer term. For this CIP 002-4 interim standard let's keep it simple.
- Used 15 minute in other criteria. "within 15 minutes"?
- "Under frequency" vs. "automatic" load shedding confusion. This doesn't apply to "manual load shedding."
- We may have a hard time in the future changing
- "designated for" vs. "responsible for."
- Used capable- due to compromise or misuse
- Is "capable through misuse" designated for automatic?
- Smart grid- distribution providers are out of scope? Going forward we will be better able to define it.
- Automatic load shed not manually initiated load shed.
- "Capability"- support keeping that concept in this criterion.
- "If misused could shed 300 mw or more within 15 minutes.
- Consider pulling automatic out- discrepancy between 2000 and 300 MK.
- The justification for 300MW is in DOE 317, Version 2.

Howard Gugel 9/28/10 5:21 PM
Comment: ??

SDT Straw Poll on 1.13 as written

Yes	***No***	***Abstain***
18	**2**	**0**

Comments after the rating

- Jim Bretton disagreed with putting time in.
- Bring in all DMS systems with removal of automatic if they have load-shedding capability.

- Rich Kinas noted this significantly changes the number of assets and prompts us to lose focus as to why we are here.
- Manual initiated operation- of cyber device- protection. EMS already considered.

Criterion 1.14

"Each control center, control system, backup control center, or backup control system used to perform the functional obligations of the Reliability Coordinator, Balancing Authority, or Transmission Operator."

SDT Straw Poll

Yes	***No***	***Abstain***
16	**2**	**2**

Comments before Polling

- The drafting team and NERC offered only editorial changes.
-
- Should we drop this one?
- Control systems in 1.14.
- If combined we don't have a criteria of 2300 MW. Will be covering a lot of entities without the bright line.
- New advanced persistent threats at layer 7 at application layers are a concern. These are not being picked up by firewalls. Understand this creates a burden on these small entities but they and we need protection at the same level. Size doesn't matter when it comes to attack vectors.
- Control systems need to be protected.
- On control center criteria- don't understand survey results and why it didn't result in dropping a lot off the list? How did we lose 5 RCs? While these are close enough they are not reliable data figures and need more analysis.
- "Connectivity and size doesn't matter." IP is everything and everywhere. Controls should be inadequate for the control system. Can't buy the argument that connectivity is all that matters.
- Look at just this standard. If you put them all in it will be a huge impact. Can't solve all the problems with this standard.
- Consider changing "every" to "each"?
- Can't afford to ignore. Can't imagine that FERC would allow us to get away with 2300. It is there and it is a vulnerability.
- We are mixing 1.14 and 1.15 in our discussion. Threshold for control generation- control centers = 2 of more physical assets.
- Entities as GOPs are designating. GOP in 1.14?
- That is an "or" in 1.15.
- Can't worry about connectivity. Worried about letting it come into language. Some GOPs have control centers controlling few MW and 1 or 2 plants.

Howard Gugel 9/28/10 5:22 PM
Comment: Does not pertain to this language

Howard Gugel 9/28/10 5:23 PM
Comment: Not sure what this means.

Howard Gugel 9/28/10 5:25 PM
Comment: Not sure of context

Howard Gugel 9/28/10 5:26 PM
Comment: Context?

Howard Gugel 9/28/10 5:26 PM
Comment: What does this mean?

- 1.14 is based on EOP 008 which doesn't include GOP.
- We don't have a definition of control centers in 002-4.
- 1.14- can't rely on EOP 008- not required to have a back up control center. Lots of ways of meeting standards. It may be problematic to call this out as a reason.
- This is because we don't have concrete definition for control center. Focus on the control systems.
- Back up control centers- doesn't say you have to have a back up center, but if you do you must secure.
- EOP 008 doesn't have qualifications so we don't need them either. We need a justification.
- EOP 008 not referenced in the guidance.

Criterion 1.15:
"Each control center or backup control center used to control generation identified as a Critical Asset, or used to control generation greater than an aggregate of 2300 MWs in a single Interconnection."

SDT Straw Poll on 1.15 as presented.

Yes	*No*	*Abstain*	
15	**2**	**2=**	**79%**

The SDT discussed the criterion which links back to 1.1 and discussed it as presented and identified the following concerns: this will probably get this sent back from FERC; need to clarify why 1.1 uses 2000 MW and this uses 2300 MW; should "control systems" be added to be consistent with 1.15; there may be control systems that are computerized but that are not connected; control centers appear in CIP versions 1, 2 & 3 so removing the focus on control centers would need to be justified; this is a transition to a function focus of CIP 010 & 011; control room vs. control center doesn't have to be analyzed separately from asset it controls; control centers operated by generation operators with no transmission but just control and dispatch; what about renewables or variable generation; and what does control generation mean? 1.15: centers being used to control generation- don't control breakers, just establishing a set point. Easy for it to be taken off until they are sure it is the right signal they should be following. 2300 explanation good break point.

Howard Gugel 9/28/10 5:27 PM
Comment: Should this be in here?

SDT Straw Poll- delete "in a single interconnection"

Yes	*No*	*Abstain*	
6	**12**	**1=**	**32%**

Criterion 1.16
"Any facility declared by a regulatory agency to be critical to national security."

Howard Gugel presented the criterion that was not proposed by the SDT CIP 002-4 drafting team but proposed by NERC staff. He noted the NERC data request showed that only 17 nuclear generation facilities are included in the existing risk-based methodology. If nuclear generation is added as a specific criterion, that number rises to 88. The SDT reviewed the statement noting the following concerns: this is a overbroad statement and a back handed way to get nuclear in; NERC is a reliability

Howard Gugel 9/28/10 5:29 PM
Comment: Not sure this should be a matter of record

organization and the SDT is working on a reliability standard; other regulators have their own processes, this doesn't belong here; there are 57 bills in the U.S. Congress giving power to the President and others to declare emergency, but until the industry get these directives from Congress and then FERC and NERC it is premature to address.

The SDT unanimously decided not to include this criterion statement in Attachment 1.

Criterion 1.17
"Any additional assets that the Responsible Entity deems appropriate to use."

The SDT discussed adding this statement back into Attachment 1 that had been removed in Chicago. The NERC data request shows 307 critical assets would be identified under this criteria. While this may be primarily an optics issues there would be no down side and it might help fund some security investment.

Howard Gugel 9/28/10 5:34 PM
Comment: Not sure the discussion considered funding. It revolved arould justifying existing Critical Asset methodology that captured assets not identified in the new criteria.

SDT Straw Poll

Yes	***No***	***Abstain***
17	**3**	**0**

Nuclear Generation Criterion

John Lim noted that the NERC president, Gerry Cauley, met with EEI executives who agreed that it would be a prudent thing to add nuclear generation as a critical asset criterion. Given the timing, the Chair proposed that members consult with their management to get additional feedback and that this issue would be up for review and possible adoption by the SDT at its September 15 conference call. It was noted that lowering 1.1 to 1500 MW will bring in more nuclear generation facilities.

A motion to adopt Attachment 1 as revised was offered by Sharron Edwards and seconded by Doug Johnson.

SDT Member Vote on Attachment #1 as Revised

Yes	**No**	
18	**1=**	**95%**

Jim Brenton voted no and offered the following explanation of his vote. "Draft CIP 002 Version 4, Attachment 1, does not require that nuclear generation plants be designated as Critical Assets per CIP-002-4. Generation Operator Control Centers and Control Systems are not designated as Critical Assets per Draft CIP 002 Version 4, Attachment 1. Many of these facilities are interconnected via real time network connections and cyber security exploits at

the application level can transverse between trusted nodes only protected at Layer 4 (firewalls and Router ACL). An insufficient number of Generation Units will be designated as Critical

Assets with the criteria in Attachment 1, Criterion 1.1 set at 1500 MW. The draft CIP 002 Version 4, Attachment 1 language related to IROLs is vague and will cause problems for TOP, TP and other registered entities in making CA determinations—it is not a bright line or a deterministic metric—since the values may change dynamically. I generally support the language provided. However, the team had an opportunity but failed to address the nuclear generation issue and the need for including sufficient generation facilities under the proposed standards, both of which I consider show stoppers, as I articulated to all during the meeting.

Howard Gugel, NERC staff, noted he would check with NERC management but that he agrees with the SDT's approach to delay the vote until members can check with their management team. If, however, the SDT agreed to post without nuclear generation included as critical assets in it, the public document posting will occur in the middle of election season in the U.S.

Howard Gugel 9/28/10 5:36 PM
Comment: I do not believe that I stated that I agreed with the approach to not include nuclear.

D. CIP -002-4 Implementation Plan

Following the Chicago meeting, SDT member Dave Revill led a lead a team (Sharon Edwards, Phil Huff, Dave Norton, Scott Rosenberg, and Kevin Sherlin. Mike Keane FERC and Scott Mix NERC, Joe Bucciero, facilitator) to develop a new draft of the implementation plan based on the Chicago input. It was presented to the SDT on the August 26 conference call. He noted the proposed sliding 18 month window for new assets not identified in the first application that are identified as a result of an update ("update as necessary") during the first 12 months. This in effect meant entities may have anywhere from 12 to 30 months to be compliant. R2 locks in which cyber assets we are talking about and those "critical cyber assets "associated with" critical assets newly identified by CIP 002-4.

The SDT discussed regarding the proposal including: confusion between FERC approval vs. effective date; given the doubling the generation and transmission facilities in scope (not Version 2 and 3 didn't anticipate the doubling of assets) 18 months is not that long a time; if we can't meet schedules because vendors are not ably to supply we must self report unless there is an exception process; if newly identified asset or control entity that hasn't dealt with before -24 months; in accelerating schedule for few requirements we have made this more complicated without really gaining much; we will also be introducing concept of CIP 010 and 011 during same period; consider a phased approach given the number of assets that need to be addressed; can regional entities deal with an exceptions process; if we just make it 24 months across the board then simplify some of these exceptions; and the regulator perspective may be that 18 months is too long a timeframe.

Following the discussion the drafting group met over lunch and came back with a proposal for a timeline which intended to provide an 18 month plus 6 months window and removed the 12 month window and made it instead a separate exception. They noted that they were not recommending an exception process because of the challenge in standing it up for this interim standards with the appropriate oversight, change the NERC rules of procedure and difficulty of implementing at the regional level. From 2006-2009 the industry identified over 4500 critical assets in 3 years with no

previous experience. This proposal would add around another 2000 critical assets (or an additional 50%) in two years. This could also be part of the feedback from the industry in the comment form.

The SDT and participants discussed the proposal offering the following points and concerns: just because it would be hard to create an exception process, doesn't justify setting the industry up for failure; power plants are very different and more complex than substations; Q 1.2 responses from the NERC data request suggests about 370 generation or a 93% increase nearly doubling existing numbers; this generation asset doubling may provide justification for the 24 vs. 18 months; version 1-FERC 706 beginning of 2008 was in essence a 24 month implementation plan; the implementation timeline for nuclear assets is 2 years with allowance for outages; though each Province varies, in general, NERC standards for Canadian entities are effective upon NERC board approval, however the effective implementation takes place upon FERC approval; should generation assets get 24 months and all others 18 months.

The SDT then polled the following implementation timeline:

Implementation Timeline- Overall 24 months (6 months for identification of critical assets and 18 months for critical assets in compliance)

Straw Poll on Timeline

Yes	No	Abstain
18	**0**	**0**

Motion to Approve the Implementation Plan as Revised with friendly amendments *("18 months after effective date") (See Appendix #)* Dave Revill with Sharon Edwards 2nd.

Yes	*No*
18	**0**

E. CIP 002-4 Reference (Guidance) Document

The Reference Document (formerly "guidance document") was initially reviewed at the August 26 SDT conference call and on Wednesday afternoon. On Thursday afternoon the SDT reviewed the reference document noting that there will be conforming edits based on the agreements reached by the SDT on CIP 002-4 and Attachment 1 and on the implementation plan. The SDT and participant discussion of the document included the following points: put some of the survey results into the guidance document supporting how this is protecting the public; use "reliable operation" which is from the standard vs. the terms "reliability or operability"; change facilities to "designated as a facility"; stay away from the term control room/facilities; guidance for CIP 2 1-3.Where does that guidance fit relative to CIP 4? Is it going away, should be considered and mentioned; critical asset identificaiton guideline becomes largely irrelevant because of the removal of the risk based approach; Critical Assset identification guidelines are still relevant; John did a good job explaining without

expanding; take out the "one button" in the rationale for 1.13 to avoid confusion with automatic load shedding."

Following the SDT review and discussion Sharon Edwards made a motion to accept the Reference Document as revised and David Revill seconded the motion with the proviso that this will be brought back to the SDT conference call on September 15 for final adoption.

Yes	No	Abstain
18	0	1

F. VSLs/VRFs

Howard Gugel reported on the draft VSLs and VRFs. He noted in the interest of minimal changes, the subR format is still being used here.

Howard Gugel 9/28/10 5:40 PM
Comment: These were not reviewed in Chicago

Members offered the following points in the review of the draft VSLs: add R2- "performing a function essential"; delete "list" and "as per requirement after operation of the Critical Asset; consider changing to bullets; consider rolling up the SubRs under severe R2; and, without an exception process as discussed yesterday in the implementation plan, how many in violation when entity did a self-reporting.

Members offered the following points in the review of the draft VRS; keep these as separate sub Rs on this table because they have different impact levels; is it a double jeopardy issue if you are in violation of a lower and a high when you have separate Sub Rs; when you have a high level requirement R2 that has a VRF with it and the Sub Rs have vrfs are at a lower level, if there is a violation of 2.1 is it also a violation of R2; auditors can't discuss VRF and VRS, they simply find a violation and findings on an audit are always rolled up to the highest level; then it becomes an enforcement issue determined by an enforcement team at a sub component; there are many requirements wrapped into R2; take the definitional parts and have as bullet points.

The SDT unanimously approved the VSL and VRS documents as revised.

G. Cover Letter and Comment Form

Howard Gugel reviewed with the SDT a draft Cover Letter and Comment form. The Vice Chair drafted and the SDT agreed to add two paragraphs that referenced the CIP 010 and 011 development and its relation to the CIP 002-4. Howard clarified that the CIP 003-009 version 4 package would be posted with CIP 002-4 with conforming references and applicability section changes. It was suggested that VSLs and VRFs be referenced as 2 separate questions.

Doug Johnson made a motion and Jay Cribb seconded to adopt the Cover Letter and Comment Form as revised for posting with CIP 002-4.

Yes	No
19	0

H. Preparation for CIP 002-4 September 29, 2010 Webinar

The SDT reviewed a draft agenda and proposed assignments for an industry webinar on September 29 from 11:00 a.m. -1 p.m. on the CIP 002-4 filing, which the Chair outlined. Allen Mosher, Chair of the NERC Standards Committee will provide some introductory remarks in terms of the context and recent history of the SDT's efforts. It was noted that the presentations would be at a relatively high level with the intention of leaving sufficient time of the Webinar devoted to Q & A. There will also be a short presentation by an industry representative member of the CIP 005 urgent action work group on the substance and procedure for that draft standard.

There will also be a short presentation by an industry representative member of the CIP 005 urgent action work group on the substance and procedure for that draft standard. It was agreed that a power point template would be circulated and a dry run will take place on September 20 with the slides to NERC by September 22.

III. PROGRESS REPORT ON CIP FRAMEWORK SUB-TEAM

Dave Norton, Sub-Team lead, reported on the two meetings the Framework Sub-Team has convened (See, Appendix 8). He suggested the context is that some in the industry stakeholders did not like what they saw with CIP-011, and the regulator doesn't think we have approached things consistently with the NIST 800-53 framework, thereby establishing a baseline at the outset. The Sub-Team has agreed that the SDT needs to answer the question, "what are we protecting and from who?" There are threats, vulnerabilities and impacts to consider but threats are hard to be clear on, and impacts have a lot of permutations. The Sub-Team is initially focusing on known vulnerabilities in the open information sources and posing the question: how can we use known vulnerabilities to link to specific standards (e.g., NIST IR volume 3, Chapter 7 treatment of vulnerabilities). The original CIP standard team learned that it is very difficult to write CIP requirements that address the old and new at the same time, resulting in overkill for the old and leaving modern vulnerabilities unaddressed. The output should be a justification and rationale underpinning the standards, not the standards themselves. They are starting with a framework for the CIP standards, and not a format. Ultimately this should lead to a format.

The Sub-team is currently pulling nuggets out from others have done before. The output should be a justification and rationale underpinning the standards, not the standards themselves. They are starting with a framework not a format. Ultimately this should lead to a format.

Dave Revill noted that when the SDT developed CIP-011, we identified requirements at the high impact level and forced the scoping elements on them. The Framework Sub-Team's idea is to start from the bottom and work up.

Member and Participant Comments

- Think about differences between serial line with an operating system vs. embedded software systems on serial lines. Different vulnerabilities. We have to think of the differences- need people who understand on how the code works.
- CIP 11 security controls lacked a basis to come back to what the measure of success was.
- We should identify threats and ask is it "appropriate" based on operating environment and the characteristics of the device.
- As a model of identifying a baseline and incorporating appropriate NIST features, can you get there without dealing with the issue with the present compliance model? If no reward system in addition to the punitive system of compliance will this work?
- As far as possible, it will be advantageous to maintain the current structure and modify a bit, then we can be responsive to that faction in the ballot pool.
- What ever appears to work will come naturally if we start at what are we trying to protect and let the structure come to that.
- E.g. on format, big middle and little. Impact classes of assets within each a category of cyber assets?
- Acknowledge the differences between a generation vs. transmission mindset.
- Agree on the "appropriate" mantra, but need to pin down what this means. Have to drill down.
- The model that we have may be ok. The implementation of the model (over zealousness of some of the audit staff and unevenness of the quality) is where the problem arises. The industry is not complaining about audits, but about the process as implemented that is not true to standards and fair and equitable across the regions.
- The Sub-teams hope is that they can get to more granular statements that are specific to technology so we can minimize TFEs.
- VRF/VSLs- 0 tolerance is problem for compliance. Gradual incremental improvement.
- From NERC and FERC the view is that self-reports are a good thing or at least a better thing than hiding it. Industry executives don't view it that way.
- FERC is looking for the industry to define what appropriate is. It doesn't mean none, has to meet some rational tests.
- In a compliance based standard context, lawyers and management see it differently from those who are trying to fix things and make them more secure. Impossible to write a standard that covers everything. FERC order 693 requires audit to the requirements.
- The Sub-team will be reviewing again what exactly does 706 say to do.

The Chair noted that the Framework Sub-Team will have a significant amount of agenda time during the Toronto SDT Meeting in October to bring the SDT up to date and engage them in discussion of the key issues. These discussions should provide guidance as the Sub-Team continues its efforts to bring back a framework that the SDT can review, refine, and adopt at its December 2010 meeting that will guide its work in 2011.

IV. NEXT STEPS AND ASSIGNMENTS

On Friday morning the SDT reviewed the progress being made by the CIP 010 and 011 sub-teams in summarizing industry responses and the Dallas workshop comments. The Chair thanked those sub-groups who had completed their tasks and asked all the sub-groups to complete their summaries by the SDT October meeting

The Team reviewed the preparations for the CIP 002-4 Webinar *(see Section II. H above)* which will take place on September 29 from 11:00 a.m.- 1:00 p.m.

The Chair reviewed the schedule for a SDT conference call meeting on Wednesday, September 15 from 10:00 a.m.-12:00 p.m. (eastern time) to review the final documents for posting that were not adopted at this meeting and to determine whether the SDT members, following review with their corporate senior management, wanted to revisit the SDT's previous decisions on whether to specifically include all nuclear generation as a criterion for assessment in CIP-002-4 Attachment 1.

The Toronto agenda was discussed and SDT member and host Rob Antonishen described the Toronto, Ontario venue for the meeting.

The meeting adjourned at 9:45 a.m. on Friday, September 10.

Appendix # 1— Meeting Agenda
Project 2008-06 Cyber Security Order 706 SDT
Draft 26th Meeting Agenda
September 8, 2010, Wednesday- 8:00 AM to 6:00 PM CDT
September 9, 2010 Thursday- 8:00 AM to 6:00 PM CDT
September 14, 2010 Friday- 8:00 AM to 10:00 AM CDT
Manitoba Hydro Place
360 Portage Ave., Winnipeg, Manitoba, Canada

NOTE: 1. Agenda Times May be Adjusted as Needed during the Meeting
NOTE: 2. Drafting Sub-team Meetings May Not Have Access to Telephones and Ready Talk

Proposed Meeting Objectives/Outcomes:

- To review, clarify, refine and adopt the draft CIP-002-4 standard, Implementation Plan and Guidance Document for posting
- To review and discuss the implications of the NERC Mandatory Data Request results for the CIP 002-4 draft
- To review agenda and assignments for CIP-002-4 September 29 Webinar
- To review progress of the Frameworks Sub-team, and the sub-teams draft responses to industry and Dallas workshop comments
- To agree on next steps and assignments

Wednesday, September 8, 2010 8:00 a.m. - 6:00 p.m.

- Introduction, welcome, and opening and guest remarks -*(Morning)*
- Receive updates on other related cyber security initiatives- *NERC Staff and SDT Members (Morning)*
- Review NERC comments on draft CIP-002-4 standard *(Morning)*
- Review and refine draft CIP 002-4 standard and related documents (including CIP-002-4, VSL/VRFs, Implementation Plan, Guidance document for CIP 002-4) *(Morning)*
- Review of NERC Data Request responses for consideration in CIP-002-4 Attachment #1 Criteria *(Afternoon)*

Thursday, September 9, 2010 8:00 a.m. - 6:00 p.m.

- Finalize draft of CIP 002-4 standard *(Morning)*
- Discuss related documents (including VSL/VRFs, Implementation Plan, and Guidance document for CIP 002-4, Comment Form, Cover Letter) *(Morning and Afternoon)*
- Adoption of CIP 002-4 documents for posting *(Afternoon)*
- Review Summary Response Documents for Attachment 2, CIP-010 *(Afternoon & Evening)*

Friday, September 10, 2010, 8:00 a.m. - 10:00 a.m.

- Review Preparation for CIP 002-4 September 29 Webinar *(Morning)*
- Review Progress report on CIP Framework sub-team (*Morning)*
- Review progress reports on Sub-teams' draft summaries of industry and Dallas workshop comments
- Review SDT October12-14, 2010 Toronto Meeting Agenda (*Morning)*

Appendix # 2 Attendees List
September 8-10, 2010 Winnipeg

Attending in Person — SDT Members and Staff

1. Rob Antonishen	Ontario Power Generation
2. Jim Brenton	ERCOT
3. Jackie Collett	Manitoba Hydro
4. Jay S. Cribb	Southern Company Services
5.Joe Doetzl	Kansas City Pwr. & Light Co
6. Sharon Edwards	Duke Energy
7.Gerald S. Freese	America Electric Pwr.
8. Jeff Hoffman	U.S. Bureau of Reclamation, Denver
9. Phillip Huff, Vice Chair	Arkansas Electric Coop Corporation
10. Doug Johnson	Exelon Corporation – Commonwealth Edison
11. John Lim, Chair	Consolidated Edison Co. NY
12. David Norton	Entergy
13. David S. Revill	Georgia Transmission Corporation
14. Tom Stevenson	Constellation
15. Keith Stouffer	National Institute of Standards & Technology

SDT Members Attending via ReadyTalk and Phone

16. Scott Rosenberger	Luminant Energy (W/Th)
17.Rich Kinas	Orlando Utilities Commission (W/Th)
18. John D. Varnell	Technology Director, Tenaska Power Services Co. (W/Th)
19. John Van Boxtel	WECC (W)
20 William Winters	Arizona Public Service, Inc. (W/Th)
21.William Gross	Nuclear Energy Institute (W/Th)
22.Kevin Sherlin	Sacramento Municipal Utility District (Th)
Scott Mix	*NERC*
Howard Gugel	*NERC*
Brian Harrell	*NERC*
Roger Lampila	*NERC*
Joe Bucciero	*NERC/Bucciero Consulting, LLC*
Robert Jones	*FSU/FCRC Consensus Center*
Stuart Langton	*FSU/FCRC Consensus Center*

Howard Gugel 9/28/10 5:42 PM
Comment: I do not think these entries belong in this table. We were in person, not on ReadyTalk

SDT Members Not Participating

Patricio Leon	Southern California Edison
Jonathan Stanford	Bonneville Power Administration

Others Attending in Person

Justin Kelly	FERC
Greg Fraser	G.J. Fraser Consulting
Joel Garmen	Next Era Energy (FPL) (T/W/Th)
Robert Preston Lloyd	Southern California Edison
Michael Keane	FERC
Nathan Mitchell	APPA
Brian Newell	American Electric Power
Mark Simon	Encari
Tom Alrich	Matrikon
Guy Zito	NPCC (T/W)

Howard Gugel 9/28/10 5:57 PM
Comment: Allen did not attend this meeting

Others Attending via Readytalk and Phone

September 8, 2010, Wednesday

Bryn	Wilson	wilsonwb@oge.com
andres	Lopez	andres.lopez@usace.army.mil
Roger	Fradenburgh	rfradenburgh@netsectech.com
Amir	Hammad	amir.hammad@constellation.com
jan	Bargen	jan.bargen@ferc.gov
Monte	Moorehead	mpmoorehead@midamerican.com
matt	Jastram	matt.jastram@pgn.com
Robert	Ford	robert.w.ford@usace.army.mil
David	Batz	dbatz@eei.org
Jason	Marshall	jmarshall@midwestiso.org
Patricia	Lynch	patricia.lynch@nrgenergy.com
Larry	Camm	larry_camm@selgs.com
Tom	Alrich	tom.alrich@matrikon.com
Bob	Case	Bob.Case@blackhillscorp.com
Rod	Hardiman	rchardim@southernco.com
Vincent	Le	vincent.le@ferc.gov
Maggy	Powell	margaret.powell@constellation.com
Russell	Noble	rnoble@cowlitzpud.org
Annette	Johnston	AJJohnston@midamerican.com
Drew	Kittey	Drew.Kittey@ferc.gov
David	Gordon	dgordon@mmwec.org

Al	Mendoza	patricio.leon-alvarado@sce.com
Roger	Fradenburgh	rfradenburgh@netsectech.com
Ingrid	Rayo	ingrid.rayo@constellation.com
Sharla	Artz	sharla_artz@selgs.com

September 9, 2010, Thurssday

Bob	Case	Bob.Case@blackhillscorp.com
Russell	Noble	rnoble@cowlitzpud.org
Jan	Bargen	jan.bargen@ferc.gov
Stephen	Thomas	Stephen.J.Thomas@constellation.com
Bill	Keagle	william.a.keagle.jr!@bge.com
Rod	Hardiman	rchardim@southernco.com
Sharla	Artz	sharla_artz@selgs.com
David	Gordon	dgordon@mmwec.org
Larry	Camm	larry_camm@selgs.com
Dave	Batz	dbatz@eei.org
Tom	Alrich	tom.alrich@matrikon.com
Vincent	Le	vincent.le@ferc.gov
Drew	Kittey	Drew.Kittey@ferc.gov
Jason	Marshall	jmarshall@midwestiso.org
Robert	Ford	robert.w.ford@usace.army.mil
Ingrid	Rayo	ingrid.rayo@constellation.com
Bryn	Wilson	wilsonwb@oge.com

September 10, 2010, Friday

Larry	Camm	larry_camm@selgs.com
Bill	Keagle	william.a.keagle.jr@bge.com
Ingrid	Rayo	ingrid.rayo@constellation.com
Sharla	Artz	sharla_artz@selgs.com
Tom	Alrich	tom.alrich@matrikon.com
Rod	Hardiman	rchardim@southernco.com
jan	bargen	jan.bargen@ferc.gov
Bryn	Wilson	wilsonwb@oge.com
Russell	Noble	rnoble@cowlitzpud.org

Appendix #3 NERC Antitrust Compliance Guidelines

See Antitrust Compliance Guidelines read at the beginning of each day's session at:

(NEED LINK)

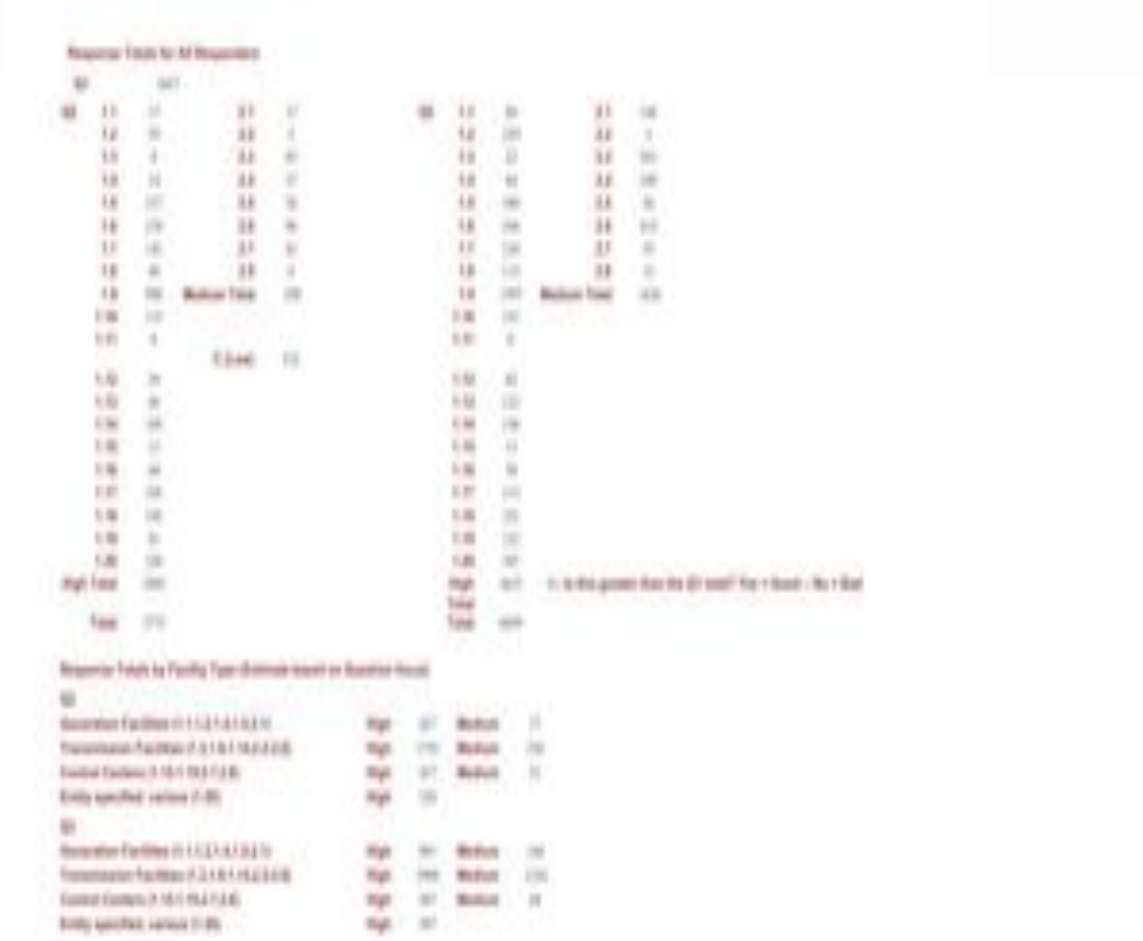
The NERC reminder below was read at the beginning of each day's session.

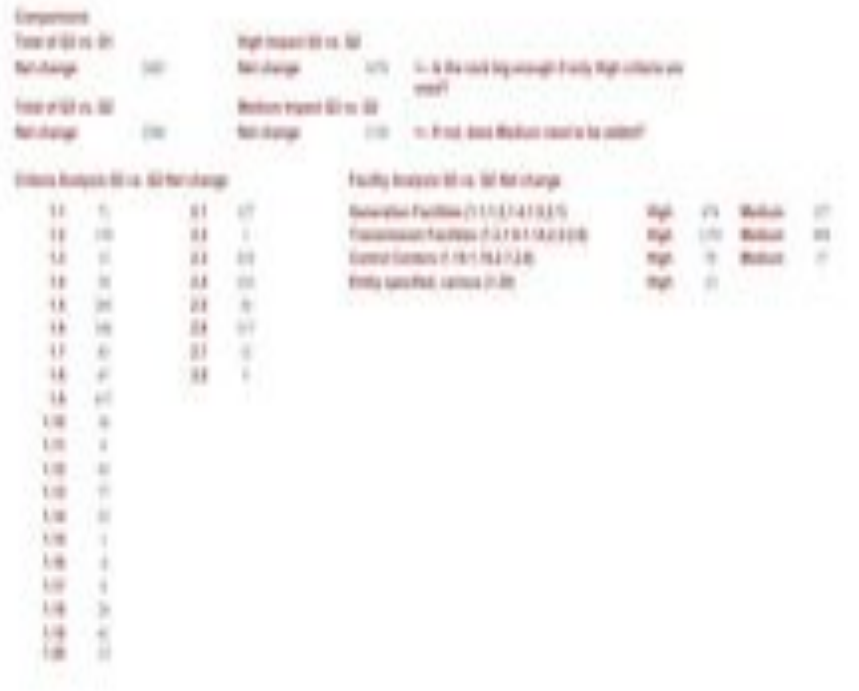
NERC REMINDER FOR USE AT BEGINNING OF MEETINGS AND CONFERENCE CALLS THAT HAVE BEEN PUBLICLY NOTICED AND ARE OPEN TO THE PUBLIC

For face-to-face meeting, with dial-in capability:

Participants are reminded that this meeting is public. Notice of the meeting was posted on the NERC website and widely distributed. The notice included the number for dial-in participation. Participants should keep in mind that the audience may include members of the press and representatives of various governmental authorities, in addition to the expected participation by industry stakeholders.

Appendix # 4- Raw Results- NERC Data Request





Appendix # 5- CIP 002-4 Adopted Draft (9-9-10)

Introduction

1. **Title:** Cyber Security — Critical Cyber Asset Identification

2. **Number:** CIP-002-4

3. **Purpose:** NERC Standards CIP-002-4 through CIP-009-4 provide a cyber security framework for the identification and protection of Critical Cyber Assets to support reliable operation of the Bulk Electric System.

   These standards recognize the differing roles of each entity in the operation of the Bulk Electric System, the criticality and vulnerability of the assets needed to manage Bulk Electric System reliability, and the risks to which they are exposed.

   Business and operational demands for managing and maintaining a reliable Bulk Electric System increasingly rely on Cyber Assets supporting critical reliability functions and processes to communicate with each other, across functions and organizations, for services and data. This results in increased risks to these Cyber Assets.

   Standard CIP-002-4 requires the identification and documentation of the Critical Cyber Assets associated with the Critical Assets that support the reliable operation of the Bulk Electric System. These Critical Assets are to be identified through the application of the criteria in Attachment 1.

4. **Applicability:**

   4.1. Within the text of Standard CIP-002-4, "Responsible Entity" shall mean:

   4.1.1 Reliability Coordinator.

   4.1.2 Balancing Authority.

   4.1.3 Interchange Authority.

   4.1.4 Transmission Service Provider.

   4.1.5 Transmission Owner.

   4.1.6 Transmission Operator.

   4.1.7 Generator Owner.

   4.1.8 Generator Operator.

   4.1.9 Load Serving Entity.

   4.1.10 NERC.

4.1.11 Regional Entity.

4.2. The following are exempt from Standard CIP-002-4:

4.2.1 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

5. **Effective Date:** The first day of the third calendar quarter after applicable regulatory approvals have been received (or the Reliability Standard otherwise becomes effective the first day of the third calendar quarter after BOT adoption in those jurisdictions where regulatory approval is not required)

Requirements

R1. Critical Asset Identification — Each Responsible Entity shall develop a list of its identified Critical Assets determined through an annual application of the criteria contained in *CIP-002-4 Attachment I – Critical Asset Criteria*. The Responsible Entity shall review this list at least annually, and update it as necessary.

R2. Critical Cyber Asset Identification — Using the list of Critical Assets developed pursuant to Requirement R1, each Responsible Entity shall develop a list of associated Critical Cyber Assets performing a function essential to the operation of the Critical Asset. For each group of generating units (including nuclear generation) at a single plant location identified in Attachment 1, criterion 1.1, the only Cyber Assets that must be considered are those shared Cyber Assets that could adversely impact the reliable operation of any combination of units that in aggregate exceed Attachment 1, criterion 1.1 within 15 minutes. Each Responsible Entity shall review this list at least annually, and update it as necessary. For the purpose of Standard CIP-002-4, Critical Cyber Assets are further qualified to be those having at least one of the following characteristics:

R2.1 The Cyber Asset uses a routable protocol to communicate outside the Electronic Security Perimeter; or,
R2.2 The Cyber Asset uses a routable protocol within a control center; or,
R2.3 The Cyber Asset is dial-up accessible.

Annual Approval — The senior manager or delegate(s) shall approve annually the list of Critical Assets and the list of Critical Cyber Assets. Based on Requirements R1 and R2 the Responsible Entity may determine that it has no Critical Assets or Critical Cyber Assets. The Responsible Entity shall keep a signed and dated record of the senior manager or delegate(s)'s approval of the list of Critical Assets and the list of Critical Cyber Assets (even if such lists are null.)

Measures

M1. The Responsible Entity shall make available its list of Critical Assets as specified in Requirement R1.

M2. The Responsible Entity shall make available its list of Critical Cyber Assets as specified in Requirement R2.

M3. The Responsible Entity shall make available its approval records of annual approvals as specified in Requirement R3.

Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

1.1.1 Regional Entity for Responsible Entities that do not perform delegated tasks for their Regional Entity.

1.1.2 ERO for Regional Entity.

1.1.3 Third-party monitor without vested interest in the outcome for NERC.

1.2. Compliance Monitoring Period and Reset Time Frame

Not applicable.

1.3. Compliance Monitoring and Enforcement Processes

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints

1.4. Data Retention

1.4.1 The Responsible Entity shall keep documentation required by Standard CIP-002-4 from the previous full calendar year unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

1.4.2 The Compliance Enforcement Authority in conjunction with the Registered Entity shall keep the last audit records and all requested and submitted subsequent audit records.

1.5. Additional Compliance Information

1.5.1 None.

2. Violation Severity Levels (To be developed later.)

Regional Variances

None identified.

VERSION HISTORY

Version	Date	Action	Change Tracking
1	January 16, 2006	R3.2 — Change "Control Center" to "control center"	03/24/06
2		Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3		Updated version number from -2 to -3	
3	12/16/09	Approved by the NERC Board of Trustees	Update
4	09/20/10	Modified to provide bright-line criteria for the identification of Critical Assets.	

CIP-002-4 - Attachment I

CRITICAL ASSET CRITERIA

The following are considered Critical Assets:

1.1. Each group of generating units (including nuclear generation) at a single plant location with an aggregate highest rated net Real Power capability of the preceding 12 months equal to or exceeding 1500 MW.

1.2. Each reactive resource or group of resources at a single location (excluding generation Facilities) having aggregate net Reactive Power nameplate rating of 1000 MVARs or greater.

1.3. Each generation Facility that the Planning Coordinator or Transmission Planner designates as required for reliability purposes.

1.4. Each Blackstart Resource identified in the Transmission Operator's restoration plan.

1.5. The Facilities comprising the Cranking Paths and initial switching requirements from the Blackstart Resource to the unit(s) to be started, as identified in the Transmission Operator's restoration plan up to the point on the Cranking Path where multiple path options exist.

1.6. Transmission Facilities operated at 500 kV or higher.

1.7. Transmission Facilities operated at 300 kV or higher at stations interconnected at 300 kV or higher with three or more other transmission stations.

1.8. Transmission Facilities at a single station location that, if destroyed, degraded, misused or otherwise rendered unavailable, violate one or more Interconnection Reliability Operating Limits (IROLs).

1.9. Flexible AC Transmission Systems (FACTS) at a single station location, that, if destroyed, degraded, misused or otherwise rendered unavailable, violate one or more Interconnection Reliability Operating Limits (IROLs).

1.10. Transmission Facilities providing the generation interconnection required to directly connect generator output to the transmission system that, if destroyed, degraded, misused, or otherwise rendered unavailable, would result in the loss of the assets described in Attachment 1, criterion 1.1 or 1.3.

1.11. Transmission Facilities identified as essential to meeting Nuclear Plant Interface Requirements.

1.12. Each Special Protection System (SPS), Remedial Action Scheme (RAS) or automated switching system that operates BES Elements that, if destroyed, degraded, misused or otherwise rendered unavailable, violate one or more Interconnection Reliability Operating Limits (IROLs).

1.13. Common control system(s) capable of performing automatic load shedding of 300 MW or more within 15 minutes.

1.14. Each control center, control system, backup control center, or backup control system used to perform the functional obligations of the Reliability Coordinator, Balancing Authority, or Transmission Operator.

1.15. Each control center or backup control center used to control generation identified as a Critical Asset, or used to control generation greater than an aggregate of 1500 MWs in a single Interconnection.

1.16. Any additional assets that the Responsible Entity deems appropriate to include.

CIP-002-4	R1.	Critical Asset Identification — Each Responsible Entity shall develop a list of its identified Critical Assets determined through an annual application of the criteria contained in CIP-002-4 Attachment 1 – Critical Asset Criteria. The Responsible Entity shall review this list at least annually, and update it as necessary.	N/A	N/A	The Re Entity h develop Critical the list been re updatec as requ	
CIP-002-4	R2.	Critical Cyber Asset Identification — Using the list of Critical Assets developed pursuant to Requirement R1, each Responsible Entity shall develop a list of associated Critical Cyber Assets performing a function essential to the operation of the Critical Asset. For each group of generating units (including nuclear generation) at a single plant location identified in Attachment 1, criterion 1.1, the only Cyber Assets that must be considered are those shared Cyber Assets that could adversely impact the reliable operation of any combination of units that in aggregate exceed Attachment 1, criterion 1.1 within 15 minutes. Each Responsible Entity shall review this list at least annually, and update it as necessary. For the purpose of Standard CIP-002-4, Critical Cyber Assets are further qualified to be those having at least one of the following characteristics:	N/A	N/A	The Re Entity h develop associa Cyber A perform functio to the o the Crit but the been re updatec as requ	

CIP-002-4	R2.1	The Cyber Asset uses a routable protocol to communicate outside the Electronic Security Perimeter; or,	N/A	N/A	N/A	
CIP-002-4	R2.2.	The Cyber Asset uses a routable protocol within a control center; or,	N/A	N/A	N/A	
CIP-002-4	R2.3.	The Cyber Asset is dial-up accessible.	N/A	N/A	N/A	
CIP-002-4	R3.	Annual Approval — The senior manager or delegate(s) shall approve annually the list of Critical Assets and the list of Critical Cyber Assets. Based on Requirements R1 and R2, the Responsible Entity may	N/A	N/A	The Re Entity have a dated r senior delegat	

		determine that it has no Critical Assets or Critical Cyber Assets. The Responsible Entity shall keep a signed and dated record of the senior manager or delegate(s)'s approval of the list of Critical Assets and the list of Critical Cyber Assets (even if such lists are null.)			annual the list Assets. OR The Re Entity have a dated re senior delegat annual the list Cyber (even i are null	

Appendix #6 Implementation Plan (Final)

Implementation Plan for Version 4 of

Cyber Security Standards CIP-002-4 through CIP-009-4

Prerequisite Approvals

There are no other reliability standards or Standard Authorization Requests (SARs), in progress or approved, that must be implemented before this standard can be implemented.

Applicable Standards

The following standards are covered by this Implementation Plan:
CIP–002–4 —Cyber Security — Critical Cyber Asset Identification
CIP–003–4 — Cyber Security — Security Management Controls
CIP–004–4 — Cyber Security — Personnel and Training
CIP–005–4 — Cyber Security — Electronic Security Perimeter(s)
CIP–006–4 — Cyber Security — Physical Security
CIP–007–4 —Cyber Security — Systems Security Management
CIP–008–4 — Cyber Security — Incident Reporting and Response Planning
CIP–009–4 — Cyber Security — Recovery Plans for Critical Cyber Assets

These standards are posted for ballot by NERC together with this Implementation Plan. When these standards become effective, all prior versions of these standards are retired.

Compliance with Standards

Once these standards become effective, the Responsible Entities identified in the Applicability section of the standard must comply with the requirements. These Responsible Entities include:

- Reliability Coordinator
- Balancing Authority
- Interchange Authority
- Transmission Service Provider
- Transmission Owner
- Transmission Operator
- Generator Owner
- Generator Operator
- Load Serving Entity
- NERC
- Regional Entity

Proposed Effective Date for CIP-002-4

Responsible Entities shall be compliant with the requirements of CIP-002-4 on the Effective Date specified in the Standard.

Proposed Effective Date for CIP-003-4 – CIP-009-4

Critical Cyber Assets Already in Compliance with CIP-003-3 – CIP-009-3

Critical Cyber Assets identified by CIP-002-4 R2 that are already compliant with CIP-003-3 through CIP-009-3 shall be compliant with the requirements of CIP-003-4 through CIP-009-4 on the Effective Date specified in each version 4 Standard.

Critical Cyber Assets Associated with Critical Assets Newly Identified by CIP-002-4

U.S. Nuclear Power Plant Facilities

For Owners and Operators of U.S. Nuclear Power Plants, Critical Cyber Assets associated with U.S. Nuclear Power Plants identified as Critical Assets which are newly identified by CIP-002-4 R1 within the first 18 months following the Effective Date of CIP-002-4 shall be compliant with CIP-003-4 through CIP-009-4 by the latter of (i) 18 months after the Effective Date of CIP-002-4 or (ii) 6 months following the completion of the first refueling outage beyond 18 months from the Effective Date of CIP-002-4 for those requirements requiring a refueling outage.

All Facilities Other Than U.S. Nuclear Power Plant Facilities

For Responsible Entities who previously identified Critical Cyber Assets under CIP-002-1 R3, CIP-002-2 R3, or CIP-002-3 R3; Critical Cyber Assets associated with Critical Assets which are newly identified by CIP-002-4 R1 within the first 18 months following the Effective Date of CIP-002-4 shall be compliant with CIP-003-4 through CIP-009-4 18 months after the Effective Date of CIP-002-4.

All Other Critical Cyber Assets

For all cases not identified above, Critical Cyber Assets shall be compliant with the requirements of **CIP-003-4 through CIP-009-4** by the latter of (i) the Effective Date specified in each Version 4 Standard or (ii) the compliance milestones in the *Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities* based on the earliest date of identification of the Critical Cyber Asset from CIP-002-1 R3, CIP-002-2 R3, CIP-002-3 R3, or CIP-002-4 R2.

Implementation Plan for Newly Identified Critical Cyber Assets and

Newly Registered Entities

Concurrently submitted with version 4 of Cyber Security Standards CIP-002-4 through CIP-009-4 is a separate Implementation Plan document that would be used by the Responsible

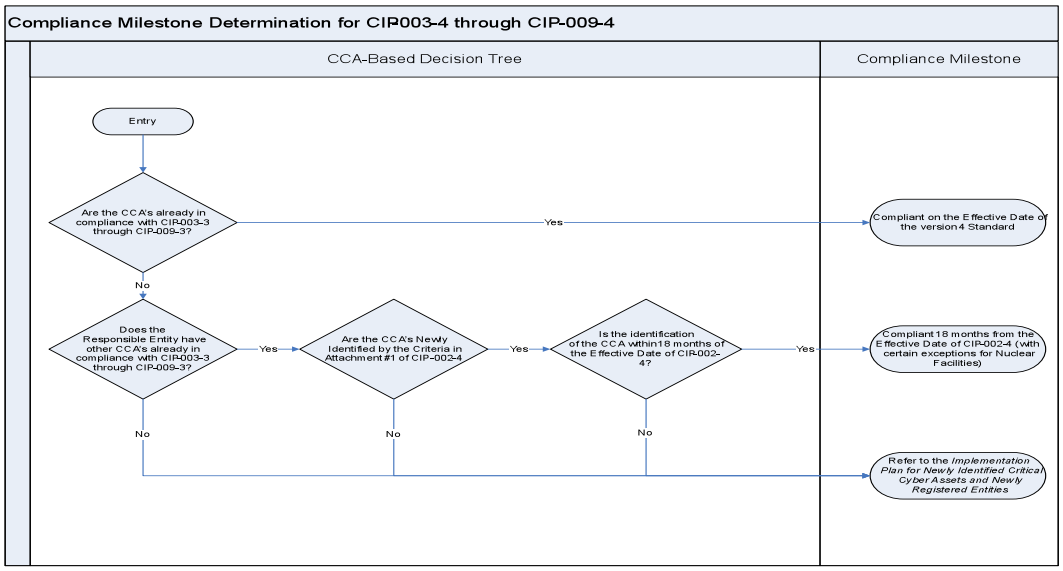
Entities to bring any newly identified Critical Cyber Assets into compliance with the Cyber Security Standards, as those assets are identified. This Implementation Plan would apply based on the situations identified in the above section, *Proposed Effective Date*. This Implementation Plan closes the compliance gap created in the Version 1 Implementation Plan whereby Responsible Entities were required to annually determine their list of Critical Cyber Assets, yet the implication from the Version 1 Implementation Plan was that any newly identified Critical Cyber Assets were to be immediately 'Auditably Compliant', thereby not allowing Responsible Entities the necessary time to achieve the Auditably Compliant state.

The Implementation Plan for newly identified Critical Cyber Assets provides a reasonable schedule for the Responsible Entity to achieve the 'Compliant' state for those newly identified Critical Cyber Assets.

The Implementation Plan for newly identified Critical Cyber Assets also addresses how to achieve the 'Compliant' state for: 1) Responsible Entities that merge with or are acquired by other Responsible Entities; and 2) Responsible Entities that register in the NERC Compliance Registry during or following the completion of the Implementation Plan for Version 4 of the NERC Cyber Security Standards CIP-002-4 to CIP-009-4.

Prior Version Standard Retirement

Standards CIP-002-3 – CIP-009-3 shall be retired upon the Effective Date of the corresponding Version 4 Standard.



NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Appendix #7 Letter and Comment Form

September 20, 2010

TO: INDUSTRY STAKEHOLDERS

RE: **REQUEST FOR COMMENTS REGARDING THE DRAFT OF CIP-002-4 THROUGH CIP-009-4**

Ladies and Gentlemen:

In 2008, FERC Order 706 paragraph 236 directed the ERO to develop modifications to Standard CIP-002-1 Cyber Security – Critical Cyber Asset Identification to address their concerns regarding: (1) the need for ERO guidance regarding the risk-based assessment methodology; (2) the scope of critical assets and critical cyber assets; (3) internal, management approval of the risk-based assessment; (4) external review of critical assets identification; and (5) interdependency analysis.

A Standards Drafting Team (SDT) was appointed by the NERC Standards Committee on August 7, 2008 to develop these modifications as part of Project 2008-06 – Cyber Security Order 706. The SDT has been charged to review each of the CIP reliability standards and address the modifications identified in the FERC Order 706. The SDT began meeting in October 2008.

Prior to this posting, the SDT developed CIP-002-2 through CIP-009-2 to comply with the near-term specific directives of FERC Order 706. This version of the Standards was approved by FERC in September of 2009 with additional directives to be addressed within 90 days of the order. In response, the SDT developed CIP-003-3 through CIP-009-3, which FERC approved in March 2010.

Throughout this period, the SDT has continued efforts to develop an approach to address the remaining FERC Order 706 directives. Most recently, CIP-010 and CIP-011were posted for informal comment in May of 2010. After reviewing and analyzing responses from the industry, the SDT determined it was infeasible to address all of the concerns and achieve industry consensus on CIP-010 and CIP-011 by the planned target date of December 2010. Consequently, the SDT limited the scope of requirements in this posting of CIP-002 through CIP-009 as an interim step to address the more immediate concerns raised in FERC Order 706, paragraph 236. The approach to address the remaining FERC Order 706 directives continues to be developed.

The SDT believes the NERC Standards CIP-002-4 through CIP-009-4 provide a cyber security framework for the identification and protection of Critical Cyber Assets to support reliable operation of the Bulk Electric System. These standards recognize the differing roles of each entity in the operation of the Bulk Electric System, the criticality and vulnerability of the assets needed to manage Bulk Electric System reliability, and the risks to which they are exposed.

Standard CIP-002-4 requires the identification and documentation of the Critical Cyber Assets associated with the Critical Assets that support the reliable operation of the Bulk Electric System. These Critical Assets are to be identified through the application of the "bright-line" criteria contained in *Attachment 1 – Critical Asset Criteria* of the draft CIP-002-4 standard.

The draft CIP-002-4 standard and requirements provide a foundation for effective cyber security to protect the systems that support a reliable Bulk Electrical System (BES). After months of deliberation and industry input, the SDT is continuing to evolve the Reliability Standards addressing cyber security by presenting a draft standard *CIP 002-4 – Cyber Security – Critical Cyber Asset Identification* that identifies BES Cyber Systems according to "bright-line" criteria associated with the impact on reliable operation of the BES. The *CIP-002-4 Cyber Security - Critical Asset Identification - Rationale and Implementation Reference Document* provides clarifying notes and rationale of the SDT. The draft CIP-003-4 through CIP-009-4 standards include conforming changes to match the versioning of CIP-002-4.

A separate ballot is being conducted on CIP-005-4, and if the proposed standard is approved it will be filed with CIP-003-4 to CIP-009-4. If the proposed CIP-005-4 is rejected, then the present CIP-005-3 will be modified with conforming changes and filed with CIP-003-4 to CIP-009-4. The team is continuing to work on subsequent cyber security standards that will establish impact levels and define associated cyber security controls at levels appropriate to their BES impact.

The Team is seeking industry feedback and suggestions on this draft of CIP 002-4. The industry feedback will be considered by the SDT in revising and refining CIP 002-4 requirements and related documents.

The SDT has provided a form for industry participants to offer their comments on this draft of CIP-002-4.

Questions

Your responses to the following questions will assist the SDT for Project 2008-06 Cyber Security Order 706 in finalizing the work for CIP-002-4 through CIP-009-4 relative to the proposed modifications summarized above. For each question, please indicate whether or not you agree with the modification being proposed. If you disagree with the proposed modification, please explain why you disagree and provide as much detail as possible regarding your disagreement including any suggestions for altering the proposed modification that would eliminate or minimize your disagreement. The SDT would appreciate responses to as many of these questions as you are willing to supply.

1. CIP-002-4 Attachment 1 contains criteria that define elements that must be classified as Critical Assets. Do you have any suggestions that would improve the proposed criteria? If so, please explain and provide specific suggestions for improvement.

   ☐ Yes
   ☐ No
   Comments:
2. Requirement R1 of draft CIP-002-4 states, "Critical Asset Identification — Each Responsible Entity shall develop a list of its identified Critical Assets determined through an annual application of the criteria contained in *CIP-002-4 Attachment 1 – Critical Asset Criteria*. The Responsible Entity shall review this list at least annually, and update it as necessary." Do you agree with the proposed Requirement R1? If not, please explain why and provide specific suggestions for improvement.

   ☐ Yes
   ☐ No
   Comments:
3. Requirement R2 of draft CIP-002-4 states, "Using the list of Critical Assets developed pursuant to Requirement R1, each Responsible Entity shall develop a list of associated Critical Cyber Assets performing a function essential to the operation of the Critical Asset. For each group of generating units (including nuclear generation) at a single plant location identified in Attachment 1, criterion 1.1, the only Cyber Assets that must be considered are those shared Cyber Assets that could adversely impact the reliable operation of any combination of units that in aggregate exceed Attachment 1, criterion 1.1 within 15 minutes. Each Responsible Entity shall review this list at least annually, and update it as necessary. For the purpose of Standard CIP-002-4, Critical Cyber Assets are further qualified to be those having at least one of the following characteristics". The requirement then lists characteristics using the same text that is contained in the existing CIP-002-3 R3. Do you agree with the proposed Requirement R2? If not, please explain why and provide specific suggestions for improvement.

   ☐ Yes
   ☐ No
   Comments:
4. Do you agree with the proposed Violation Risk Factors? If not, please provide suggested improvements on the proposed VRFs.

   ☐ Yes
   ☐ No
   Comments:

5. Do you agree with the proposed Violation Severity Levels? If not, please provide suggested improvements on the proposed VSLs.

☐ Yes
☐ No
Comments:

6. Do you agree with the proposed implementation plan? If so, please explain and provide specific suggestions for improvement.

☐ Yes
☐ No
Comments:

Appendix # 8 Framework Team September 2 Meeting Results

Structure and Composition of CIP Version 5

1) In order to be responsive to: 1) the industry in general; 2) a large industry voting block with far-reaching established programs; and, 3) FERC 706; we need to:

   a) Maintain a size-based paradigm for organizing grid assets. As such, we would define "Classes" of grid assets:
      i) Class A – large ("bright line" CIP-002-4; sans control/data centers)
      ii) Class B - medium sized assets (scope TBD)
      iii) Class C - small sized assets (scope TBD)
      iv) Class D – Control/ Data Centers

   b) Use the NIST paradigm for building requirement-sets; i.e., first establish minimum baseline requirements for all Asset Classes and Categories (see #2 below) for each subject area contained in the CIPs; then augment as criticality increases (i.e., for Class B Categories and Class A Categories)

2) To obtain granularity in requirements desired, establish "Asset Categories" within each Asset Class, and write Requirements appropriate for each:

   a) Generation Category – within each Class A, B, and C
   b) Transmission Category – within each Class A, B, and C
   c) Control/Data Center Category – within each Class A, B, and C
   d) Others?

   [Note movement of control/data centers out of CIP-002 for treatment as a Category]

Drafting Work Process

1) Initially, create separate sub-teams (STs) to work individually on the controls and technical issues that we need to address. Let's not address the governance issues at first, but hold them until we have the framework better defined. [If additional Standards are determined to be necessary, create additional STs.]

2) Define "*What are we defending against*?" As the first step in the process, each ST will research and specify generic known vulnerabilities that CIP Standards' requirements are aimed to mitigate. This is needed to provide foundational rationale for a more granular approach to Requirements-writing, with the aim of avoiding the pitfalls of a "one size fits all" approach under which we currently operate. This approach should reduce both the number of TFE and variability in interpretation.

3) With an eye toward the issues its working on, each ST conducts a review and captures:
   a) specific instructions contained in the CS_706 SAR
   b) specific FERC 706 directives, ensuring coverage of "Post V4" topics

4) Using the list of vulnerabilities from Item #2 work just above, and directives culled from work under Item #3 just above, each ST will begin crafting baseline Requirements for each Asset Category within each Asset Class, using the following resources:
   a) Draft CIP-011 language, regardless of prior organization of material
   b) DHS Catalog
   c) NIST SP800-53 and SP800-82
   d) ??? NISTIR V2 SG Cyber Security WG
   e) ??? ISA99

5) Using the same resources as in Item #4 just above, each ST would then augment the "Baseline Requirements" created under Item #4 just above, with more "Advanced Control and Countermeasure Requirements" as appropriate for each Asset Category beneath Asset Class B, and Asset Class A respectively.

6) As each ST creates Requirements, it must take note of the potential need for coordination/rationalization of language in the Standard it is working on with other Standards being worked by other ST. [CIP could remain "nested" to a certain degree]

7) After 'rationalization' of language across Standards, either task a new ST or have the entire SDT take up the umbrella governance issues.

II/III Outstanding items needing further consideration

1) Data Communications – Do we:
   a. Create a new Standard?
   b. Treat it as a Category of Asset beneath each Asset Class?
   c. Just enhance the existing approach?
2) Can "Baseline Requirements" be:
   a. Strictly "organizational controls" (largely processes and procedures)? Or,
   b. Also additionally technical countermeasures (equipment, SW, etc.)
3) Shall we have different "Baseline Requirements":
   a. Across each Asset Class? [Class A more rigorous than B, and B more than C]
   b. Across each Category within each Class? [Same logic as 3a.]
4) Other areas the Framework Team members want to discuss at this time?

How much farther than this do we want to go before gaining full SDT agreement in principle that this approach is acceptable?

Appendix #9 Sub-Team Roster

Sub-Team	
CIP 010 BES System Categorization	John Lim (Lead), Rich Kinas, Jim Brenton, Dave Norton *(Observer Participants: Rod Hardiman, Jim Fletcher) (FERC: Mike Keane, Peter Kuebeck)*
Personnel and Physical Security	Doug Johnson (Lead), Rob Antonishen, Patrick Leon, Kevin Sherlin *(FERC: Drew Kittey)*
System Security and Boundary Protection	Jay Cribb (Lead), Jackie Collett, John Varnell, John Van Boxtel, Philip Huff *(Observer Participant: Brian Newell) (FERC: Justin Kelly)*
Incident Response and Recovery	Scott Rosenberger (Lead), Joe Doetzl, Tom Stevenson (*Observer Participant: Jason Marshall) (FERC: Dan Bogle)*
Access Control	Sharon Edwards (Lead), Jeff Hoffman, Jerry Freese, Bill Winters *(Observer Participants: Roger Fradenburgh, Robert Preston Lloyd) (FERC: Mike Keane)*
Change Management, System Lifecycle, Information Protection, Maintenance, and Governance	Dave Revill (Lead), Jon Stanford, Keith Stouffer, Bill Winters *(Observer Participant: Brian Newell) (FERC: Jan Bargen, Matthew Dale)*
CIP 002-4 Drafting Team	John Lim (Lead), Jim Brenton, Jackie Collett, Jay Cribb, Sharon Edwards, Doug Johnson, Rich Kinas, Dave Norton, Dave Revill, and Bill Winters *(Observer Participants: Rod Hardiman; Jim Fletcher; Bryn Wilson) (FERC: Mike Keane, Peter Kuebeck; NERC: Scott Mix)*
Implementation Plan CIP 002-4	Dave Revill (Lead), Sharon Edwards, Kevin Sherlin, Scott Rosenberg, Dave Norton and Phil Huff *(FERC: Mike Keane; NERC: Scott Mix)*
Framework CIP 010 &011	Dave Norton (Lead), Jim Brenton, Jay Cribb, Joe Doetzl, Phil Huff, Doug Johnson, Dave Revill, Jon Stanford, and John Van Boxtel. *(FERC: Mike Keane; NERC: Scott Mix)*

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Agenda
Cyber Security Order 706 SDT - Project 2008-06

September 8, 2010 | 8:00 AM to 6:00 PM CDT
September 9, 2010 | 8:00 AM to 6:00 PM CDT
September 10, 2010 | 8:00 AM to 10:00 AM CDT

Manitoba Hydro Place
360 Portage Ave., Winnipeg, Manitoba, Canada

Proposed Meeting Objectives/Outcomes:

- To review, clarify, refine and adopt the draft CIP-002-4 standard, Implementation Plan and Guidance Document for posting
- To review and discuss the implications of the NERC Mandatory Data Request results for the CIP 002-4 draft
- To review agenda and assignments for CIP-002-4 September 29 Webinar
- To review progress of the Frameworks Sub-team, and the sub-teams draft responses to industry and Dallas workshop comments
- To agree on next steps and assignments

Wednesday, September 8, 2010 8:00 a.m. - 6:00 p.m.

- Introduction, welcome, and opening and guest remarks -*(Morning)*
- Receive updates on other related cyber security initiatives- *NERC Staff and SDT Members (Morning)*
- Review NERC comments on draft CIP-002-4 standard *(Morning)*
- Review and refine draft CIP 002-4 standard and related documents (including CIP-002-4, VSL/VRFs, Implementation Plan, Guidance document for CIP 002-4) *(Morning)*
- Review of NERC Data Request responses for consideration in CIP-002-4 Attachment #1 Criteria *(Afternoon)*

Thursday, September 9, 2010 8:00 a.m. - 6:00 p.m.

- Finalize draft of CIP 002-4 standard *(Morning)*
- Discuss related documents (including VSL/VRFs, Implementation Plan, and Guidance document for CIP 002-4, Comment Form, Cover Letter) *(Morning and Afternoon)*
- Adoption of CIP 002-4 documents for posting *(Afternoon)*
- Review Summary Response Documents for Attachment 2, CIP-010 *(Afternoon & Evening)*

116-390 Village Blvd.
Princeton, NJ 08540
609.452.8060 | www.nerc.com

Friday, September 10, 2010, 8:00 a.m. - 10:00 a.m.

- Review Preparation for CIP 002-4 September 29 Webinar *(Morning)*
- Review Progress report on CIP Framework sub-team (*Morning)*
- Review progress reports on Sub-teams' draft summaries of industry and Dallas workshop comments
- Review SDT October12-14, 2010 Toronto Meeting Agenda (*Morning)*

Second page...

CSO706 SDT FULL TEAM CONFERENCE CALL SUMMARY
September 15, 2010
10:00 a.m. - 12:00 p.m. EDT
Adopted by the SDT on October 14, 2010

Following roll call and a review of the anti-trust guidelines, the Chair reviewed the objectives and agenda for the call. When a quorum of at least 17members was achieved, NERC Standards Committee Chair Allen Mosher addressed the SDT thanking them for their continuing efforts. He expressed appreciation for their sense of humor indicating he understood their frustration in doing this difficult job. He asked them to do the right thing for reliability of the BES while keeping in mind the different visions on what that is and the broader policy context of the CIP. He acknowledged the challenge for companies in the industry to address these high impact/low frequency events. He reminded members that CIP was different from other standards and was viewed through a different lens, noting both the significant external pressures felt within the industry and beyond as well as the heightened attention to the reality of being probed daily on cyber security threats.

Howard Gugel, NERC reported that there were no NERC staff edits of the CIP 002-4 that was adopted by the Team in Winnipeg. He mentioned that he had deleted one of the measures from the old requirement.

John Lim opened the SDT discussion on the possibility of adding a new criterion to CIP 002-4 Attachment 1 to include all nuclear generation facilities. He noted that in Winnipeg the Team agreed that members would discuss and receive input from their senior management in light of the EEI CEOs meeting of last week.

After extended discussion of a proposal for adding a new Attachment 1 criterion addressing nuclear generation and potential related changes for CIP 002-4 in the applicability and requirements sections, a motion was made by John Lim to test support for the following change to the Applicability Section, 4.2.1 failed to get a second:

> 4.2.1 Proposal: ~~All BES facilities under NERC jurisdiction those s~~Structures, components, equipment and systems ~~of facilities~~ within a nuclear generation plant ~~not~~ regulated by the U.S. Nuclear Regulatory Commission or the Canadian Nuclear Safety Commission.

Jim Brenton then made a motion that the following new criterion be included in Attachment 1, with Dave Norton seconding the motion with the friendly amendment substituting facility for unit:

> 1.1. "Each nuclear generation ~~facility~~ unit."

There was discussion following the motion and Jim Brenton and Dave Norton agreed that if the motion passed to include a new 1.1, there would be conforming changes to 1.2 and in 4.2 to reinstate the exclusion and make the following change in R2:

1.1. Each group of generating units (excluding ~~including~~ nuclear generation) at a single plant location with an aggregate highest rated net Real Power capability of the preceding 12 months equal to or exceeding 1500 MW.

"R2. Critical Cyber Asset Identification — Using the list of Critical Assets developed pursuant to Requirement R1, the Responsible Entity shall develop a list of associated Critical Cyber Assets essential to the operation of the Critical Asset. For each group of generating units ~~(including nuclear generation)~~ at a single plant location identified in Attachment 1, criterion 1.~~1~~ 2, the only Cyber Assets that must be considered are those shared Cyber Assets that could adversely impact the reliable operation of any combination of units that in aggregate exceed Attachment 1, criterion 1.~~1~~ 2within 15 minutes. The Responsible Entity shall review this list at least annually, and update it as necessary."

Some members offered concerns that this language had not been reviewed in advance and vetted in terms of possible impacts or unintended consequences; that with the changes in Winnipeg the current R1.2 brings in many more nuclear facilities (e.g. all Duke's nuclear generation will come in as critical assets); why nuclear as a fuel is treated differently for reliability than other types of fuel (hydro, coal, etc) and that safety systems are regulated by other regulatory bodies (e.g. NRC); that inclusion of this criteria is purely an optic for criticality which establishes a bad precedent and is indefensible in terms of reliability; the possible impact of the changes on 1.11; that the SDT hasn't excluded nuclear and is covered in new last criterion added in Winnipeg; concern that the "unit" term take us to safety systems and possibly puts them in double jeopardy; this was excluded in Pittsburgh in order to avoid the FERC and NRC issue.

The chair called for a vote on the motion, noting there was a quorum present and that it would require at least 13 of the 19 members present support to pass with 2/3's support of the SDT:

- **In support of the motion= 9 members = 47%**
- **Opposed to the motion=10 members**

Following the vote there was discussion as to whether there was anything short of removing the criteria that might move those voting no to vote yes. Some members noted their reasons for not supporting the motion that included: the current 1.1 at 1500 MW and other changes in the criteria made in Winnipeg were sufficient; there needs to be a reliability basis for including nuclear generation; concern about the confusion in terms of NRC jurisdiction; better to submit the draft from Winnipeg to the industry and see what happens in balloting process; considering this a the last minute without the ability to sort out possible unintended consequences.

The Chair noted that based on this vote, the CIP 002-4 that had been approved by the SDT in Winnipeg would be posted for the 45 day formal comment period.

The Team agreed to post the Reference (formerly the Guidance) Document that had been revised and circulated to the Team on September 13 based on the Winnipeg input. Members editorial redline comments on the document would be considered following the review of the Industry comments and first ballot. Since the Summary Industry Response document for the relevant sections of Attachment 2, CIP-010 was not ready it would not be posted with CIP 002-4.

The Team briefly reviewed the preparation for the September 29 webinar and the meeting adjourned at 12:00 p.m.

Appendix #1 Agenda

CSO706 SDT Full Team Conference Call
September 15, 2010
10:00 a.m.- 12:00 p.m. EST

Objectives

- To review and consider acceptance of any NERC staff edits to CIP 002-4
- To review and consider adoption for a new Attachment #1 criterion on nuclear generation facilities
- To review and adopt the Reference Document for posting with CIP 002-4
- To review and adopt the Summary Response to relevant parts of Attachment 2, CIP 010 for posting with CIP 002-4; and
- To review next steps including the September 29 Webinar.

Draft Agenda

The agenda for today's conference call includes:

- Roll Call, Quorum Test (17 SDT members) and Objectives and Agenda Review
- Anti-Trust Guidelines
- Review of the CIP 002-4 Posting Schedule
- Review of CIP 002-4 NERC Staff Edits
- Discussion and Possible Motion to Add to Attachment #1 a new Criterion designating as Critical Assets all nuclear generation Facilities
- Review and Adopt the Reference Document for CIP-002-4 *(John Lim)*
- Review and Adopt Summary Response for Attachment 2, CIP-010 *(Jackie Collett)*
- Review of the September 29 Webinar on CIP 002-4
- Next Steps and Assignments

Appendix #2 Participant List
SEPTEMBER 15, 2010 SDT CONFERENCE CALL, 10 A.M- LLEREP.M. EST

SDT Members Participating

1. Rob Antonishen	Ontario Power Generation
2. Jim Brenton	ERCOT
3. Jackie Collett	Manitoba Hydro
4. Jay S. Cribb	Southern Company Services
5.Joe Doetzl	Kansas City Pwr. & Light Co
6. Sharon Edwards	Duke Energy
7. Gerald S. Freese	America Electric Pwr.
8.William Gross	Nuclear Energy Institute
9. Jeff Hoffman	U.S. Bureau of Reclamation, Denver
10. Phillip Huff, Vice Chair	Arkansas Electric Coop Corporation
11. Doug Johnson	Exelon Corporation – Commonwealth Edison
12. John Lim, Chair	Consolidated Edison Co. NY
13. David Norton	Entergy
14.Kevin Sherlin	Sacramento Municipal Utility District
15. Tom Stevenson	Constellation
16. Keith Stouffer	National Institute of Standards & Technology
17. Scott Rosenberger	Luminant Energy
18. John D. Varnell	Technology Director, Tenaska Power Services Co.
19 William Winters	Arizona Public Service, Inc.

Members Unable to Participate

Rich Kinas	*Orlando Utilities Commission*
Patricio Leon	*Southern California Edison*
David S. Revill	*Georgia Transmission Corporation*
Jonathan Stanford	*Bonneville Power Administration*
Brad Yates	
John Van Boxtel	*WECC*

Scott Mix	*NERC*
Howard Gugel	*NERC*
Joe Bucciero	*NERC/Bucciero Consulting, LLC*
Robert Jones	*FSU/FCRC Consensus Center*
Stuart Langton	*FSU/FCRC Consensus Center*

Ready Talk Participants (other than members)

Drew	Kittey	Drew.Kittey@ferc.gov
Andres	Lopez	andres.lopez@usace.army.mil
Herb	Schrayshuen	herb.schrayshuen@nerc.net

John	Fridye	jfridye@rrienergy.com
Ray	Bernard	RayBernard@go-rbcs.com
Rod	Hardiman	rchardim@southernco.com
Gerry	Cauley	gerry.cauley@nerc.net
Robert	Preston Lloyd	robert.lloyd@sce.com
Justin	Kelly	Justin.Kelly@ferc.gov
Paul	Ackerman	paul.ackerman@constellation.com
Monte	Moorehead	mpmoorehead@midamerican.com
Roger	Fradenburgh	rfradenburgh@netsectech.com
Nathan	Mitchell	nmitchell@appanet.org
Chris	Earls	cee@nei.org
Allen	Mosher	amosher@appanet.org
Michael	Keane	michael.keane@ferc.gov
Rod	Hardiman	rchardim@southernco.com
Jan	Bargen	jan.bargen@ferc.gov
Vincent	Le	vincent.le@ferc.com
James	Fletcher	jrfletcher@aep.com
Peter	Brown	peter.brown2@pgnmail.com
Robert	Schaffeld	raschaff@southernco.com
Scott	Mix	scott.mix@nerc.net

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

27th Meeting Summary
Cyber Security Order 706 SDT — Project 2008-06

Adopted by the SDT November 18, 2010

Toronto, Ontario

October 12, 2010, Tuesday - 8 AM to 6 PM EDT
October 13, 2010, Wednesday - 8 AM to 6 PM EDT
October 14, 2010, Thursday - 8 AM to 6 PM EDT

Robert Jones, Stuart Langton, and Hal Beardall
Facilitation and Meeting Design
FCRC Consensus Center, Florida State University

http://www.nerc.com/filez/standards/Project_2008-06_Cyber_Security.html

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

CSO706 SDT October 12-14, 2010 Meeting Summary Contents

Cyber Security Order 706 SDT- Project 2008-06
27TH MEETING
October 12-14, 2010
Toronto, Canada

EXECUTIVE SUMMARY

John Lim, Chair of the CSO 706 SDT welcomed members and other participants to Toronto and thanked Rob Antonishen at Ontario Power Generation for hosting the meeting. Howard Gugel, NERC, conducted a roll call and reviewed the antitrust and public meeting guidelines. On Wednesday morning, the SDT unanimously adopted the September 8-11, 2010 Winnipeg meeting summary and the September 15, 2010 SDT Conference Call Summary. On Wednesday at noon, the Chair, on behalf of the SDT, bid Jackie Collett a fond farewell and thanked her for her leadership and contributions. She will be taking a new position with Manitoba Hydro and will step down from the SDT in December 2010.

Bob Jones briefly reviewed the schedule for CIP 010 & CIP-011, which was adopted by the SDT during the Chicago meeting and sent to the Standards Committee in September. The schedule calls for a draft standard for formal comment to the industry by July 2011. In December, the SDT will be reviewing the recommendations from the Framework Sub-Team and determining the course for the further development of the CIP standards in 2011. He also reviewed the CIP 002-4 schedule. During the November meeting in Baltimore, the SDT will be reviewing and responding to industry comments and determining what changes to make to CIP 002-4 before posting for the 2nd ballot.

In updates, Scott Mix, NERC noted the comments received were substantial for CIP 005-4 (over 200 pages) and he summarized common themes. The SDT is treating the posting as an informal comment process and plans to have revisions to the proposed standard by next week and a guidance document was posted in the meantime during the ballot period. The intent is to have this out for ballot along with CIP 002-4. Scott also noted that Jim Brenton, a member of the CAN-5 team, was not able to participate in the Toronto meeting and offered a brief report on the efforts to date. Finally he noted that the CAN-7 is technically completed. Dave Norton reported on NESCSO/NETL this new organization that has been funded by DOE and formed to address best practices with an academic flavor. Apparently two organizations have received DOE 3- year funding: EPRI and Energy Sec a small organization that meets once a year and has established a portal and secure chat facility. Howard Gugel reported on the NERC annual standards meeting in St. Louis and his presentation on the CIP work of the SDT. He noted there were questions about protecting assets (E.g. 69 KV in swamp) and small entities expressed concerns about the thresholds and he suggested that the SDT consider including information on why were are making transition to protecting all cyber assets on this up front in their next posting. Scott Mix reported that FERC has issued an order accepting the TFEs with some clean up and additional obligations and NERC will file another compliance filing in the next 90 days (Docket # RR 10-1-001). Howard Gugel reported that CIP 002-1 Declaration of Critical Assets, Balloting for Interpretation had closed but results not yet available.

The SDT reviewed the questions posed regarding CIP 002-4 on the September 29 Webinar and reviewed and refined responses for each question as a way to prepare for the challenge in responding to industry comments on the first ballot of CIP 002-4 in November. Howard Gugel, NERC staff, reviewed with the SDT a few changes agreed to by the SDT in that were inadvertently left off of the formal 45 day comment filing and he proposed, and the SDT agreed, to post a new CIP 002-4 version with errata corrected for balloting.

Dave Norton provided a review of the Framework Team's efforts to date, including several conference call meetings since it was created at the August SDT Chicago meeting. Their charge was to develop a framework strawman for the CIP framework going forward in 2011. He noted that the Team has begun to develop some documents including: a draft communications plan (Dave Revill), a rationale paper (Phil Huff), a spreadsheet with current requirements (Jay Cribb and Phil Huff) and a set of critical issues (Dave Norton).

Dave Norton presented a power point with six draft premises designed to stimulate SDT discussion on a framework going forward. The Team discussed and provided some potential responses for each of the premises:

- Premise #1, focusing on whether to assess the threats and risks or applying best practices against known vulnerabilities included discussion of: what threats are we defending against; reliability standards; audit-ability the nature of the framework; controls and "considering" the NIST; requirements and controls; and risk Assessment. In discussing this premise, the SDT concluded their approach will continue to be apply best practices against known vulnerabilities.
- Premise #2, focused on whether to take a minimalist or a transformative approach to the CIP standards concluded that this is not "either/or" but rather "both/and."
- Premise #3, focused on how the Team should respond to the directive to "consider" the NIST security risk management framework, and the discussion covered topics of: requirements language, TFEs, programmatic approach to standards drafting; compensating measures and a lesson learned culture. The Team concluded that this, like premise #2, may not be "either/or" but rather "both/and" and that "consideration" of NIST is not the same as adoption of NIST. The industry and the SDT should consider what aspects of the NIST approach fit the requirements model and whether adopting a programmatic approach to drafting standards will help to address the consideration of NIST.
- Premise # 4 focused on categorization of critical assets and the SDT generally concluded that both electrical impact and cyber security views should inform the standards and that trying to distinguish between high, medium and low may not be the best approach to providing cyber protection of the BES. The differences between transmission, generation and control centers may prove be more important than distinguishing H/M/L.
- Premise #5, focused on characterization of asset classes for protection and the SDT discussed physical security and its relationship to the characterizations and generally conclude that the three set paradigm should be the one to build on for the CIP.
-

- Premise #6 focused on whether and how standards should address the different genre and age of control equipment in terms of vulnerability, device class or technology.

On Thursday the Team developed a set of framework guidance statements based on the discussion. Phil Huff offered an initial draft of statements which the Team reviewed, refined and agreed to. Below are the final statements.

Ultimately, we need more structure in the requirement drafting process. The Framework Sub-Team's deliverable in December should be very concrete and clear in the proposed direction moving forward.

1. The Framework Sub-Team will develop a framework (e.g. style guide) for writing program-based requirements, where appropriate. This framework should include:
   - Minimizing zero-defects in compliance requirements
   - Guidance for rationale statements for individual requirements that speak to the vulnerabilities they address.
2. The Framework Sub-Team will develop a high-level narrative to answer the foundational question of "What are we trying to protect against?"
3. The Framework Sub-Team will develop a model which applies a baseline set of requirements for all BES Cyber Systems which allows for enhanced requirements for:
   - High impact
   - Specifications for generation, transmission, and control centers
   - Specifications for legacy vs. state-of-the-art equipment
   - Connectivity considerations
4. The Framework Sub-Team will consider developing a framework for incorporating vulnerability assessments into the current standards for the purpose of allowing flexibility in applying security controls.

Following the discussion of the premises and prior to refining and finalizing the guidance statements, the SDT discussed the following issues related to the development of the framework: manage security like reliability; change the zero-defect approach; change the industry approach to self reports; improve uniformity of audits.

The Framework Team has been asked to provide a draft answer the question of the organization of the CIP going forward and has been developing a clearer documentation of the rationale for the changes reflected in the draft CIP 10 and 11. The Chair asked each SDT member, through a round-robin review, to describe their current thinking on the format for the CIP. He noted that at its Sacramento meeting the SDT was nearly evenly split on the format question. Several members noted they had changed their earlier position supporting the use the existing CIP 003-009 format and many now said that form should follow function and that either format approach, or even another format approach would be acceptable. The facilitate summarized the results of the exercise suggesting there was in evidence a lot more openness

around this issue than in Sacramento and a shared value of getting the requirements right first and then organizing the format and that the Framework Team could focus on the goal of eliminating or reducing cross-linking in the standard requirements and TFEs. The Chair suggested the Framework Team continue its efforts in preparing a strawman for the December, 2010 meeting in Orlando. He also noted that the communication plan for industry outreach and education that the Team is developing will be critical to the success of the SDT.

The Team reviewed the steps and assignments coming into the Baltimore meeting. The SDT agreed to engage in a series of conference call meetings (Monday-Friday, 11:00 a.m.-3:00 p.m.) the week before the Baltimore meeting to review industry comments and review and refine a set of strawman SDT responses to the comments. Tom Stevenson provided an overview of Constellation Energy's facility in Baltimore where the SDT will meet in November. The Chair thanked Rob Antonishen for his excellent hosting of the SDT in Toronto.

The meeting adjourned at 4:40 on Thursday

_____

Cyber Security Order 706 SDT- Project 2008-06
27TH MEETING SUMMARY
October 10-12, 2010
Toronto, Canada

I. AGENDA REVIEW, WORKPLAN SCHEDULE AND UPDATES

A. Agenda Review and Adoption of Meeting SDT Summaries

John Lim, Chair of the CSO 706 SDT welcomed members and other participants to Toronto and thanked Rob Antonishen at Ontario Power Generation for hosting the meeting. Rob covered logistics. Howard Gugel, NERC, conducted a roll call *(See Appendix #2)* and reviewed the antitrust and public meeting guidelines *(See Appendix #3)* with the meeting participants at the outset on each day. On Wednesday morning, the SDT unanimously adopted the September 8-11, 2010 Winnipeg meeting summary and the September 15, 2010 SDT Conference Call Summary. John Lim reviewed the proposed meeting objectives, the facilitator Bob Jones reviewed and the SDT agreed to the proposed timed agenda. On Wednesday at noon, the Chair, on behalf of the SDT, bid Jackie Collett a fond farewell and thanked her for her leadership and contributions. She will be taking a new position with Manitoba Hydro and will step down from the SDT in December, 2010.

B. Update on the CIP 002-4 and the 010 and 011 Development Schedule

Bob Jones briefly reviewed the schedule for CIP 010 & CIP-011, which was adopted by the SDT during the Chicago meeting and sent to the Standards Committee in September and calls for a draft standard for formal comment to the industry by July, 2011, meaning there are about 6 months starting in December for the SDT to complete this task. In December, the SDT will be reviewing the recommendations from the Framework Sub-Team and determining the course for the further development of the CIP standards in 2011.

He also reviewed the CIP 002-4 schedule. During the November meeting in Baltimore, the SDT will be reviewing and responding to industry comments and determining what changes to make to CIP 002-4 before posting for the 2nd ballot.

C. Updates on other related cyber security initiatives- *NERC Staff and SDT Members*

1. Update on Urgent Action CIP 005-4 process- *Scott Mix*

Scott Mix noted the comments were substantial on CIP 005-4 (over 200 pages). He summarized common themes. The SDT has had several conference calls to resolve issues (such as local definitions of remote access and other issues) and they are treating the posting as an informal comment process. He also noted that the new NERC version of standards development was recently approved by FERC

which removed urgent action and replaced it with an "expedited" process. The SDT plans to have revisions to the proposed standard by next week and a guidance document was posted in the meantime during the ballot period. The intent is to have this out for ballot along with CIP 002-4.

2. **Update on CAN 5-** ***Scott Mix***

Scott noted that Jim Brenton was not able to participate in the Toronto meeting. Scott offered a brief report on the efforts to date include a possible "misstatement" about operator laptop control.

3. **Update on CAN 7-** ***Scott Mix***

Scott noted that this CAN in technically completed.

4. **Update on NESCSO at NETL-** ***Dave Norton***

Dave Norton reported on this new organization that has been funded by DOE and formed to address best practices with an academic flavor. Apparently two organizations have received DOE 3- year funding: Energy Sec a small organization that meets once a year and has established a portal and secure chat facility; and EPRI. The conference was attended by a couple other SDT members (Jim Brenton and John Van Boxtel) and featured a presentation by Mike Assante on his work on professional certification.

5. **October NERC annual standards meeting in St. Louis-** ***Howard Gugel***

Howard Gugel reported on the NERC annual standards meeting in St. Louis and his presentation on the CIP work of the SDT. He noted there were questions about protecting assets (E.g. 69 KV in swamp) and small entities expressed concerns about the thresholds. He underscored the need to look at this from both an engineering and IT perspective and consider the threat of attack vectors and simultaneous attacks. He suggested that the SDT consider including information on why were are making transition to protecting all cyber assets on this up front in their next posting.

The SDT discussed what approach we are taking (bright lines or tailored protection), CIP 002-4 addressing the highest level of protection; the use of mutual distrust and small systems; and until the functional model changes, the SDT should write standards for what is in NERC's purview.

6. **Technical Feasibility Exceptions-** *Scott Mix*

Scott Mix reported that FERC has issued an order accepting the TFEs with some clean up and additional obligations and NERC will file another compliance filing in the next 90 days (Docket # RR 10-1-001). The SDT discussion covered: when will it take effect? A: after FERC approval; NERC has to file compliance filing to add those and other clean up. Until that 006 and 007 not subject; another

Appendix 4D filing will be done; how will the TFE process address applying a patch? A: Not sure yet lawyers are reviewing.

7. CIP 002-1 Declaration of Critical Assets, Balloting for Interpretation.

Howard Gugel reported on this ballot noting it has closed but results not yet available.

II. REVIEW OF CIP 002-4 WEBINAR QUESTIONS AND RESPONSES

The SDT reviewed the questions posed regarding CIP 002-4 on the September 29 Webinar and reviewed and refined responses for each question as a way to prepare for the challenge in responding to industry comments on the first ballot of CIP 002-4 in November. *See Appendix XX for the SDT discussion comments and final response statements.*

At the conclusion of the webinar, NERC offered to post the questions raised and responses offered as a resource for the industry to review in reflecting on CIP 002-4 when balloted. The SDT agreed to offer additional comments, where needed, to clarify any responses that team members offered during the course of the webinar.

Howard Gugel, NERC staff, reviewed with the SDT a few changes agreed to by the SDT in that were inadvertently left off of the formal 45 day comment filing including: deleting "senior officer"; deleting the exception for nuclear facilities in CIP 008; and 1.1 – "greater than 1500 MW" vs."1500 or more." which both should have been deleted. He proposed, and the SDT agreed, to post a new CIP 002-4 version with errata corrected for balloting. Members discussed the fact that the Guidance Document clarified that manually initiated was not automatic load shed and this should be consistent in CIP 002-4.

III. FRAMEWORK TEAM REPORT AND SDT DISCUSSION OF CRITICAL ISSUES

Dave Norton provided a review of the Framework Team's efforts, including several conference call meetings since it was created at the August SDT Chicago meeting. Their charge was to develop a framework strawman for the CIP framework going forward in 2011. Team members included: Dave Norton, Jim Brenton, Jay Cribb, Joe Doetzl, Phil Huff, Doug Johnson, Dave Revill, Jon Stanford, and John Van Boxtel. Mike Keane at FERC and Scott Mix at NERC also participated. He noted that the attendance has been spotty but the Team has begun to develop some documents including: a draft communications plan (Dave Revill), a rationale paper (Phil Huff), a spread sheet with current requirements (Jay Cribb and Phil Huff) and a set of critical issues (Dave Norton).

A. Review of Critical Issues and Premises

Dave Norton presented a power point with some framing premises designed to stimulate SDT discussion on a framework going forward. Howard Gugel noted that the Team had asked Keith Stouffer do a presentation on the NIST framework but he was unable to at this meeting. Keith agreed to do so at the December meeting or in a webinar format prior to that meeting. Jay Cribb suggested the question for the SDT was what "shade of gray are we going to choose?" Dave Norton noted his concern regarding the industry's ability to absorb these changes. The facilitator suggested that the goal of the review of these premises is not driving towards consensus but rather an opportunity for the SDT to flush out and discuss the issues.

Draft Premise #1`: Known vectors that threats can exploit are vulnerabilities. Risk is calculated impact measured as the product of financial loss X probability of exploitation. Risk is difficult to quantify in the case of widespread loss of critical electric infrastructure, except to conclude that it is unacceptable. Therefore:

1. Is rigorous formal syllogistic assessment of threats and risk a necessary prerequisite to drafting, or

2. Is prescription of generally accepted best practice controls and countermeasures for defending against known vulnerabilities satisfactory for writing CIP standards?

Dave Norton posed the following question: while the SDT won't write standards for unknown vulnerabilities, do we need to document how many bad things can happen? The SDT after an extended discussion concluded that it does not make sense, nor will it be possible for the Team to assess the threats and risks and that it should continue with the model of applying best practices against known vulnerabilities. Some consideration should be given to whether the SDT could add rigor to vulnerability threats by utilizing the knowledge of its members and going out to entities to take some informal sampling in order to reasonably conclude that the proposed controls are addressing known vulnerabilities.

Member and participant comments covered the following issues and questions:

- **What Threats are We Defending Against?** We need to clarify these.
- We have looked at threat vectors in building the CIP standards;
- Should we stay where we are with the application of standards protecting against vulnerability;
- The best practices approach makes sense since the top 10 threats have not changed that much from year to year.
- Should we protect for 90% and detect the rest?
- Some threats are not reliant on network connectivity.

- Current standards have threat and risk infused into them because if you have a requirement framework you must do this; in the NIST framework controls are set of tools not requirements, that provide guidance;
- We can't start with a threat assessment since we don't have ability to see every entity and determine which ones apply.
- Most of threats comes from inside which can be addressed by configuration management, awareness and training, Perimeter defenses are generally well designed but its the inner connectivity that gets us into trouble.
- For "advanced persistent threats", firewall defenses are not effective. There is lots of social engineering that goes into this.
- We have an opportunity since we still don't have a way of assessing risk. If we did, wouldn't be problems with these standards. Why not discuss a risk assessment methodology?
- Look at risk assessment for a sector- problem is models are wrong. DHS heavily terrorism focused.
- We are haunted by the risk of writing a cookbook for the bad guys if everything in the overall system is the same.
- We can identify the basis we are coming from and document our assumptions. The problem in over the past year, we have made decisions without a basis to go back to. The SDT needs to restate its assumptions when making applicability decisions.
- **Reliability Standards.** EPA 215 2005- one line: "reliability standard means a requirement". By law we have to focus on requirements and a NIST tailoring effort ultimately won't fit.
- Current CIP standards are not where they need to be and could be stronger. The SDT should make the changes in confines of the law.
- **Audit-ability** against the requirements needs to be addressed and how to address whether the current audit regime needs to be changed;
- Do auditable and measureable standards result in rigorously protecting from the threats;
- **The Framework.** The purpose of the framework is to develop risk assessment on behalf of the industry.
- NERC's framework didn't get the right things and left communication systems out.
- We should avoid an "all risks/all perils" as we can't protect everything. We should clarify what is the dividing bright line. Is it routable protocols?
- We need a narrative cover sheet laying out the elements of what we are doing. These controls map back to that exposure to risk.
- Not an organizational dynamic risk assessment. The narrative- should address this. Narrative to communicate this.
- We may have an opportunity to add rigor to our assessment of vulnerability threats by checking in with entities to informally test whether the proposed controls are addressing known vulnerabilities.
- If dealing with known vulnerabilities, we know that there will always be additional ones. Maybe focus on what to exclude and defend against everything else.
- **Controls and Considering the NIST.** We should talk about generally accepted core controls that apply to the risk and not apply the NIST catalogue. In the NIST catalogue there are too

many controls in the high category and many that shouldn't be in there. Take the NIST controls that have value and work well.

- **Requirements and Controls.** The value will come in providing requirements to apply in your environment that will address the risks without embarking on a NIST risk management approach.
- Need to continue with effort to allow and guide the industry to select controls that fit the environment. How do you determine this without assessing the risk? e.g. CIP 66. 1.1 Secure cabling within a center.
- The SDT needs a narrative (not scientific) map to allow tailoring of controls to the risks we are protecting against.
- We should firm up the under-penning of best practices and be more specific on technical areas where we need to.
- We have to use our collective experience look at the real risks to the BES. Not all threats are equal and too many controls is not a good thing. Currently we don't give enough guidance on how to tailor the controls in light of the weighing of risks.
- **Risk Assessment.** Is a formal assessment of risks a prerequisite? We may have this already ("coordinated means connectivity" from NERC's Report, Critical Infrastructure Strategic Roadmap)

Draft Premise #2: The first CIP SDT considered -003 thru -009 minimum requirements, and expected subsequent augmentative drafting efforts to improve them based on experience.

Should our fundamental approach be:

1. Minimalist: Treat existing standards language as "the" baseline and augment them per specific directives in Order 706, using SP800-53 for enhancement language? Or…

2. Transformative: Literally embrace the NIST paradigm and create new sets of controls for each technical subject area, likely organized differently from the current version?

How much change can the industry absorb? How fast?

Member and participant comments covered the following issues and questions:

- In discussing this premise, the SDT concluded that this is not "either/or" but rather "both/and."

Draft Premise #3: FERC directed the SDT to 'consider' use of the NIST Security Risk Management Framework, which permits use of alternative "compensating measures," and judges adequacy of controls and countermeasures in terms of overall "programmatic effectiveness."

1. Is it in the best interest of all concerned to transition to the NIST "risk management" approach to compliance? Or…
2. Is it better to continue with literal and binary requirement compliance language measurement? Can we infuse needed flexibility through careful crafting of VRF/VSL?

Member and participant comments covered the following issues and questions:

In discussing this premise, the SDT concluded that this, like premise #2, may not be "either/or" but rather "both/and." "Consideration" of NIST is not the same as adoption of NIST and the industry and the SDT should consider what aspects of the NIST approach fit the requirements model. Adopting a programmatic approach to drafting standards will help to address the consideration of NIST. Currently there are few rewards and clear punishment for self-reporting standards violations. This "fear of fines" should be addressed by both FERC and NERC to help develop a "lessons learned" culture within the industry. The standards should give the appropriate flexibility for companies to implement compensating measures like those in the NRC as well as the TFE process. - allows compensating measure and this is similar to TFE process. In drafting standards the SDT should focus on "overall programmatic effectiveness" which can create both technical (physical, electronic and technical) and procedural defense in depth.

Member and participant comments covered the following issues and questions:

- **Requirements language.** If we avoid making it a violation and find the right words for the requirements, we don't have to worry about assigning a VRF/VSL.
- The requirements language has to be binary. The requirements are the only thing the SDT has responsibility for. Industry does not vote for VRFs/VSLs.
- There probably isn't a framework for question #1.
- **TFE.** Industry can shed light on direction the SDT might consider going in terms of TFE. Which requirements should the TFE apply to. Compensating measures were asked for. This will require discussion with audit team.
- Note the "Safe harbor" provision in TFE- advanced knowledge and ability to predict what is happening in a compliance action.
- **Programmatic Approach.** A programmatic approach will make this easier and go a ways towards meeting the directive of "considering" the NIST.
- Does programmatic effectiveness = compensating measures?
- A program is not an approach. Documentation for compliance purposes to prove you are doing the steps and if you find a problem you have a feedback loop to catch, address and fix the problem.
- **Compensating measures** will be judged in an audit. Prove "as good as or comparable to."

- Feedback loop and requirements should be an iterative process. People are not supported and valued for doing it.
- **Lessons Learned Culture.** Write good clear standards and provide guidance to help. The system should support with a "lessons learned" culture and a change in the audit approach.
- The FERC 706 Order directs the Team to "consider NIST framework."
- In our first draft, lows had 30% of the requirements, which was not viewed well.
- Are we focusing on risk management vs. the NERC binary compliance model?
- Can we infuse any flexibility into VRF/VSL? To drive constant improvement?
- What is a program approach? If you miss something but other controls caught that and corrected. That is a program approach to defense in depth. More complicated and you are layering standards to compensating and mitigating.
- Agree with this but it is hard to write this in as a requirement. When requirements went from voluntary to mandatory and enforceable – lawyers and executives have been telling what these words meant.
- Model is based on fear in CIP 002 R1 and R2- $1 million a day fines. NERC and FERC have to help and get truth out to the regions.
- FERC has to help. Commission has to say we understand- tone this down. If everyone wasn't scared for penalties. That's why minimized everything out of CIP 002.
- We (NERC and FERC) need to help each other. 80/20%. Thinking outside the box moving the platform forward. How to move best practices forward. Provides more of a conversation. We will get more polarized if we go that route. Doesn't see the 215 language is quite as restrictive.
- The law shouldn't prohibit this expertise. For Versions 1-3 the requirement was for a risk-based methodology.
- The second option is on enforcement not audit side.
- Technical people at FERC are very grounded and balanced. We need a little more outreach to address the fact that the guy writing the "self report" gets fired.
- The Federal definition of IT is very expansive.
- Version 1 CIP- risk assessment- what is the risk to BES of the asset. Use judgment to decide what controls to add.
- The standards should give the appropriate flexibility for companies to implement compensating measures. E.g. NRC- allows compensating measure and this is similar to TFE process.
- Standards- "overall programmatic effectiveness" – this creates both technical and procedural defense in depth. Can be physical, electronic, technical, procedural
- 40,000 every 7 years. Built in compensation for extra level of risk and institute program for catching errors (feedback loop).
- Enforcement- $$ amounts. NERC website. Fines that have gone through the process. The magnitude should persuade this is not the problem it is made out to be. They are rational and reasonable.
- We need to look at how many ways can we look at the "consider"- different pieces of the NIST approach we might use without using all.

- FIPS 199 and 200. Starting with systems- from control to payroll and communications. Evaluate sensitivity of this system to your mission (confidentiality, integrity availability). Very different in the federal context.
- Electric is the hub of many other systems and we are charged to keep it going. This is up high in terms of criticality.
- Bonneville's only high is a control center.
- Mission is to keep the lights on for BES. Control security vs. information security
- CIP 10- take model of FIPS 199 and its impact to mission. Assumptions about mission and impact levels. It would be Electric power system customization of the FIPS 199 process. (not a CIA but an AIC mapping)

Premise #4 Categorization: Destabilization of the BES through cyber/hybrid means requires simultaneous, successfully debilitating attacks on CCA at multiple CA locales.

Critical Questions/Options

1. If so, is size-based CA categorization the key differentiator in cyber security engineering? And, if so, what are the 'bright line' size demarcations between High/Medium, and Medium/Low; or High/All Else?

2. If not, what is the key differentiator(s) in cyber security engineering for protection of the BES, and is categorization of this differentiator appropriate or necessary? How?

The SDT agreed that both electrical impact and cyber security views should inform the standards and trying to distinguish between high, medium and low may not be the best approach to providing cyber protection of the BES. The difference between transmission, generation and control centers may be more important than distinguishing H/M/L. Navigability to the control host may be the key and boundary protections and zone of control remain very important as a fundamental concept.

Member and participant comments covered the following issues and questions:

- We need to focus on how bad guys navigate in networks.
- **H/M/L.** When H/M/L came up before we discovered it was hard to put medium definitions in. Liked it as a concept but in talking with security people, they think it will be very difficult to implement.
- The problem the SDT has faced after high, is where is the medium and low.
- H/M/L may be too complex. Move to two tiered. Real difficult to say what is a medium.
- H/M/L – moderate/medium won't work well. Lows are getting controls inherited.
- High and other? Other will take care of your base programmatic controls. Works out better to standardize with one base and train to that.
- We have been focused on high to date. Now if we say in two tiered. Look again at controls
- "Scope of impact: "- 500 kv with lots of things. 100 69 kv connected IP. Combines both-engineering view of electrical impact and cyber security view of how much stuff could I do

because of connectivity, age of equipment. Might bring more under the tent. Will be a complicated method of arriving at where you need to do what.

- **Big iron** is used to assess impact. Limits you cyber security scope. In NIST is impact to your agency. Risks can be inherited. Interconnectivity.
- Look at defining violation levels. High= interconnectivity?
- Maybe a baseline with enhancement for high impact. Facilities by themselves with an impact vs. those in combination with others.
- How much change can people take each time? Every year? 3-5 year. Precedent of changing the structure. Have the high coming in and supplement. CIP 002-4 sets high mark. Come in next time to set baseline.
- **Complexity.** The SDT released its concept paper in mid-2009 which was 2 dimensional- BES and cyber impacts and the industry said too complex.
- In favor of keeping 10 in terms of impact.
- Same criteria as attachment 1? Baseline requirement- change management, password protection. What will be layered on that? This will increase in assets coming under scrutiny.
- Need to make sure there are some could have something that is not high. E.g. 69 kv. owned by one company. No impact on BES.
- There is something in low that is not apparent. Some apply to the RE and not to the asset. Lot of inefficiency of current standards. We could make apply uniformly to RE even if you have small assets. Programs for the future.
- What do you have for physical security, personnel security etc.
- Pin to a company or to their function in the functional model? NERC does not control certain aspects in industry. It should at least be tied to NERC functional model.
- We are looking to have a common set of controls that apply to all. If you are in set of entities that CIP standards apply to then you will implement common controls.
- BES cyber systems is the universe within which we need to develop standards.
- The difference between transmission, generation and control centers may be more important than H/M/L.
- Transmission communicates with a control center and locally and unmanned (except for maintenance)
- Generation- manned more often (generally). Different criteria with security already embedded. They talk with control centers or with other generation sites.
- Control centers talk the most with other entities and need layers of protection. Highest around controls around control center, less around field assets.
- Vulnerability back to control center- whether in swamp or big generator.
- This may be more effective than to think about high/medium/low.
- Navigability to the control host is the key.
- What about mini-data center in the substations- bunch of control centers. Scope of impact less. Creating new set of sub-stations.
- What should the entity consider in making decisions on selection of controls?
- Framework should provide the parameters for the drafters in putting together controls.

- Considered going through each of requirements and listing the parameters. Look at organizational security requirements that should provide across the board/ BES.
- Look then at operational and technical controls and consider some of the characteristics based on environment (generation, transmission, control centers) and make distinctions on how to apply.
- Does the size of the asset connected to control center determine whether and how to protect the center?
- Connectivity- it is an attack vector that the spot needs to address.
- We should focus on the sake of BES security and not for protecting computer systems.
- Boundary protections and zone of control remain very important. This is fundamental concept.
- Thinking about to my control hosts and syncro-phasers.

Premise #5- Characterization Asset Classes: The first CIP SDT considered -003 thru -009 to be foremost applicable specifically to control system hosts and operator consoles at work in data/control centers. They did not expect CIP V1 to be applied to field assets without adaptation.

Critical Questions/Options

1. Should we adopt a two tier paradigm; in essence writing <u>two sets</u> of standards as appropriate for:
   a. Bastion sites: generating plants and data/control centers, and,
   b. Distributed Field sites: Substations, dams, etc.?

2. Or, a <u>three set</u> paradigm, specific to each: 1) Generation 2) Transmission 3) Control Centers?

The SDT agreed that the three set paradigm should be the one to build on for the CIP.

Member and participant comments covered the following issues and questions:

- Generation, transmission and control centers set the paradigm. Define the baseline and break out three sets.
- This turns on physical security- use this a compensating measure. Does it give us an out?
- **Physical security** is most difficult issue we have to deal with. Many utilities use distribution personnel as first responders. Toughest nut to crack is to use as compensating measure to ensure you have access control, etc. Direction industry needs to go. Difficult going forward. Unintended reliability contact.
- How can we use this physical security as a tool
- Physical security- bastion/distributed field sites- makes sense.
- This should be a tool to mitigate risk. Some modicum of physical security should exist. E.g. security reviews on annual basis.
- CIP only addresses critical cyber asset. This level of security at the lows- puts at whole different level.
- We can bleed these together as a both/and: Bastion/distributed field and generation/transmission/control centers.
- This would make it more complicated as it is hybrid of the two- physical and electronic.

- Devil is in the details. Useful tool to include- G/T/CCs- with 3 different standards?
- Could bastion equate to high? Big substations as bastions/ high. Variations on 3 - G/T/CCs.
- Provide requirements in areas of physical security that describe what your are trying to protect against. Provide security controls. Have utility determine what compensating are equivalent.
- Remove high from geography. Don't care where it is sitting. Scope of impact. The most critical sub-stations. May not be a high- function.
- Cyber system focus-what is the cyber system and what it can do.
- What is the amount of protection required? Not impacted as much as this needs high level of protection. What level of protection do you want to apply physical/electronic?
- Some teams were writing in the G/T/CCs in this approach.
- Direction- we are in agreement with the direction heading in the first place.
- Do we need some granularity in terms of devices out there?
- In practice look at all requirements on CIP 10 and 11. Little differentiation in using these concepts. There is a difference in environments which should be taken into account.
- Is it really environmental or is it at the component level.
- Framework team to put some structure around this. Define a little better and structure it so it is more formal and consistent. Express those and formalize somewhat in a document to hand off to the sub-teams in order to get some uniformity.
- Reason this didn't get separated into G/T/CCs is it is missing the general narrative regarding what we are protecting against. Are we protecting against everything everywhere? This will lend it self to creating differences and nuances to different environments.
- Does the programmatic model lend itself to a more general approach
- Some programmatic areas depend on the organization and it won't matter in terms of context/environment and where it connects to the assets. Use enhancements only where needed.
- This isn't a fair characterization of Version 1 SDT.
- Expected the auditors to take care of this. Lawyers insisted it to be verified.

Premise #6 Different Genre/Age of Control Equipment: CIP V1 did not take into account differences in the genre and age of controls equipment; resulting in "one size fits all" requirements that are inadequate for protecting some subsets of CCA and overkill for others, and the apparent cause of the need for many TFE.

Critical Questions/Options

1. Do we need to write different standards requirements for different genre and ages of control system/IED?
2. If so, how shall we parse the different genre and ages of control system/IED? What are the 'bright lines'?

Member and participant comments covered the following issues and questions:

- The Sub-team has struggled this. CCA gets a package of stuff dumped. (or next to CCA).
- BES cyber system ("target of a "plop")

- What are the device classes we can make applicability judgments that make sense.
- It is the technology: routable, serial, type of communication vs. class of device?
- We should take care in "communications" Is it an issue of the type of system? What differentiation of a device that will determine the type of controls.
- Do we go to granular level on vulnerability issue regarding those devices?
- Do we have the sub-team do the more granular vulnerability assessment piece? Yes.
- We will need to address this at the controls level by each sub team.
- How do we determine the classes of device to apply the controls?
- We need a classification model from the Drafting Team.
- Fragility caused by complexity and connectivity.
- Better approach- consider the characteristics of each device applicable to each individual requirement. 'general purpose operating system.' (e.g. networking requirements- how device communicates, etc)
- Everything has such a system. Knowledge there just not readily available.
- We missed an opportunity to impose on vendors- they should participate in this. Entities trying to educate- kick. Need government to step in.
- Protect against pieces of equipment used for purposes other than they were designed to. What other things can be done with the piece of equipment.
- National SCADA test bed program. Procurement document. That won't help us here now on this one.
- Premises regarding V1- SDT- were addressed but implementation and crafting of final requirements.
- E.g. TFE came in as different ages of equipment. Wouldn't have been introduced.
- Didn't believe this was going to the field.
- Attempted to address and failed miserably. We got to fix next time around.

B. Final SDT Guidance Statements for the Framework Team

On Thursday the Team developed a set of framework guidance statements based on the discussion. Phil Huff offered an initial draft of statements which the Team reviewed, refined and agreed to. Below are the final statements.

Ultimately, we need more structure in the requirement drafting process. The Framework Sub-Team's deliverable in December should be very concrete and clear in the proposed direction moving forward.

1. The Framework Sub-Team will develop a framework (e.g. style guide) for writing program- based requirements, where appropriate. This framework should include:
   - Minimizing zero-defects in compliance requirements
   - Guidance for rationale statements for individual requirements that speak to the vulnerabilities they address.

2. The Framework Sub-Team will develop a high-level narrative to answer the foundational question of "What are we trying to protect against?"
3. The Framework Sub-Team will develop a model which applies a baseline set of requirements for all BES Cyber Systems which allows for enhanced requirements for:
    a. High impact
    b. Specifications for generation, transmission, and control centers
    c. Specifications for legacy vs. state-of-the-art equipment
    d. Connectivity considerations
4. The Framework Sub-Team will consider developing a framework for incorporating vulnerability assessments into the current standards for the purpose of allowing flexibility in applying security controls.

Following the discussion of the premises and prior to refining and finalizing the guidance statements, the SDT discussed the development of the framework. Some of those comments are noted below:

- **Manage security like reliability.** We need to manage our security posture the same way we continuously monitor the reliability of the grid.
- **Change the Zero-defect approach.** We have to change the "zero defect" approach to the enforcement of standards.
- Power to fix some of these in our hands, way to craft words. Requirements often written with zero defect approach. Maybe the real requirements- review every X month, fix. Can get us down the road fixing that.
- **Change the Industry approach to Self Reports.** We need to find ways to promote the feedback loop and self-correcting mechanism by giving rewards to detecting and fixing cyber security issues in a timely manner. We need to explore how we change current the self reporting syndrome. We could suggest adjusting the penalty range- automatically set at the floor if you have taken measures and self reported thereby starting at a lesser penalty.
- Look to other industries- e.g. FAA/pilots with anonymous database that can be reported and doesn't affect licensing.
- Jerry Cauley, President, NERC, has promoted a "lessons learned" process at NERC. NERC staff will look at all of the reports- incident, self, etc. and cull out lessons learned for the CIP.
- What kind of behavior do we want to incent? In the human resources area we "look monitor, find, fix and repeat."
- How do you cause good cyber security to occur?
- Self reports are not made public until they go to end of the enforcement process. CEII provisions protect details and names. Specific instances where self reports made public on CIP issues. NERC rules of procedures- protect details and identity.
- Remember everything that is public info- audit schedule is public information. Tenaska up for audit and include CIP.

- Model based on fear and politics. Entities deal with incoming from wall street, congress etc.
- Other problem with shielding self reports- industry gets no lessons learned for the industry. Information is shielded. Prevents this.
- **Uniformity of Audits.** We need to separate myths from facts and talk with the NERC audit people and test our assumptions.
- Address the issue of non-uniformity of audits across the region. When self reporting you could declare how you are fixing the issue to the region without it getting publicly reported, and go through a process of mitigation. Early cycle of correction in that method. Is something like that possible?
- This is a complex problem in that auditors are not uniformly sticking to the words in standards. Can the lack of consistency in application be fixed by CANs? May not be fixed by re-writing standards.
- **More granularity in standard writing-** access review list. Conduct a review, provide evidence you conducted a review. What are expectations? Won't go all the way in fixing a problem.
- Write programmatic requirements. Make a difference in how much effort. E.g. Requirement for training vs. awareness. Tracking training.
- Do we have a different set of requirements based on environment /equipment?
- Do we have multiple levels of requirements based on risk/impact (including communications)?

C. Organizing the CIP Format- Rember Round-Robin Perspectives on CIP Format

The Framework Team has been asked to provide a draft answer the question of the organization of the CIP going forward and has been developing a clearer documentation of the rationale for the changes reflected in the draft CIP 10 and 11. Following a question regarding guidance on the format by Dave Norton, the Chair asked each SDT member, through a round robin review, to describe their current thinking on the format for the CIP. He noted that at its Sacramento meeting the SDT was nearly evenly split on the format question. Several members noted they had changed their earlier position supporting the use the existing CIP 003-009 format and many now said that form should follow function and that either format approach, or even another format approach would be acceptable. The following summarizes the results of the round-robin review. Several members noted they were personally and not necessarily for their company:

- Those members open to creating a new standards format and not tweaking CIP 003-009 which could be a single CIP 11 or a sequence of separate standards (11,12,13, etc.) included: Rob Antonishen, Jackie Collett, Jon Stanford, Doug Johnson, Jay Cribb, Bill Winters, Bill Gross and Scott Rosenberger.

- Those members suggesting that form should follow function and were neutral on the format or could live with it either way consistent with the function, included: Tom Stevenson, Joe Doetzl, Kevin Sherlin, Dave Revill, Dave Norton Gerry Freese, John Lim, Phil Huff, Jeff Hoffman.

- Those favoring tweaking the existing 3-9 but may be willing to accept another formatting approach included: John Varnell.

- FERC representatives suggested the SDT focus on getting the requirements right and less on the format.

- Participants also offered perspectives on the changes and the format.

Stu Langton summarized the results of the exercise suggesting there was in evidence a lot more openness around this issue than in Sacramento and a shared value of getting the requirements right first and then organizing the format. The Framework Team could focus on the goal of eliminating or reducing cross-linking in the standard requirements and TFEs. The Chair suggested there was not a sense from the team for a basic shift in direction and asked the Framework Team to continue its efforts in preparing a strawman for the December, 2010 meeting in Orlando. He also noted that the communication plan for industry outreach and education that the Team is developing will be critical to the success of the SDT.

IV. NEXT STEPS AND ASSIGNMENTS

The Team reviewed the steps and assignments coming into the Baltimore meeting. The SDT agreed to engage in a series of conference call meetings (Monday-Friday, 11:00 a.m.-3:00 p.m.) the week before the Baltimore meeting to review industry comments and review and refine a set of strawman SDT responses to the comments. Howard Gugel will develop and circulate an initial strawman of responses to the industry comments drawing on the webinar responses reviewed in Toronto.

Tom Stevenson provided an overview of Constellation Energy's facility in Baltimore where the SDT will meet in November.

The Chair thanked Rob Antonishen for his excellent hosting of the SDT in Toronto.

The meeting adjourned at 4:40 on Thursday

Appendix # 1— Meeting Agenda
Project 2008-06 Cyber Security Order 706 EDT
Draft 27th Meeting Agenda
October 12, 2010, Tuesday- 8:00 AM to 6:00 PM EDT
October 13, 2010 Wednesday- 8:00 AM to 6:00 PM EDT
October 14, 2010 Thursday- 8:00 AM to 6:00 PM EDT
Toronto, Canada

NOTE: 1. Agenda Times May be Adjusted as Needed during the Meeting
NOTE: 2. Drafting Sub-team Meetings May Not Have Access to Telephones and Ready Talk

Proposed Meeting Objectives/Outcomes:

- To review September 29 webinar questions and begin the development of a response document for industry posting
- To review and discuss and test acceptability of proposals for addressing key issues presented by the CIP Framework Team
- To review the Sub-team summaries of the CIP 010 & 011 and Workshop industry comments and discuss possible responses in light of the framework review
- To agree on next steps and assignments

Tuesday, October 12, 2010 8:00 a.m. - 6:00 p.m. EDT
- Introduction, welcome -*(Morning)*
- Receive updates on other related cyber security initiatives- *NERC Staff and SDT Members (Morning)*
- Review meeting and milestone schedule for CIP 002-4 and CIP 010 and 011 *(Morning)*
- Review changes to CIP Version 4 prior to ballot (CIP-002-4 R3 and CIP-008-4 applicability)
- Review results of September 29 CIP 002-4 Webinar *(Morning)*
- Participate in ERC Event Process Analysis Webinar and discuss implications for CIP development
- Draft responses and consider any changes to CIP-002-4 based on September 29 webinar questions *(Afternoon)*

Wednesday, October 13, 2010 8:00 a.m. - 6:00 p.m. EDT
- Receive a report from the team assigned to work on the framework *(Morning)*
- Discussion of Framework Team key issues *(Morning)*
- Review and provide feedback on the acceptability of the presented approach *(Afternoon)*

Thursday, October 14, 2010, 8:00 a.m. - 6:00 p.m. EDT
- Continue discussion of prospective framework *(Morning)*
- Review Sub-teams summaries of industry and Dallas workshop comments on CIP 010 & 011
- Discuss potential responses in light of the framework
- Review Preparation for CIP 002-4 Team Organization for Responding to Industry Comments before and in Baltimore *(Afternoon)*
- Review SDT November, 2010 Baltimore Meeting Agenda (*Afternoon)*

Appendix # 2 Attendees List
October 12-14, 2010 Winnipeg

Attending in Person — SDT Members and Staff

1. Rob Antonishen	Ontario Power Generation
2. Jackie Collett	Manitoba Hydro
3. Jay S. Cribb	Southern Company Services
4.Gerald S. Freese	America Electric Pwr.
5. Jeff Hoffman	U.S. Bureau of Reclamation, Denver
6. Doug Johnson	Exelon Corporation – Commonwealth Edison
7. John Lim, Chair	Consolidated Edison Co. NY
8. David Norton	Entergy
9. David S. Revill	Georgia Transmission Corporation
10. Jonathan Stanford	Bonneville Power Administration
11. Tom Stevenson	Constellation
12. John D. Varnell	Technology Director, Tenaska Power Services Co. (W/Th)
13 William Winters	Arizona Public Service, Inc.

SDT Members Attending via ReadyTalk and Phone

14. Joe Doetzl	Kansas City Pwr. & Light Co
15.Sharon Edwards	Duke Energy
16. William Gross	Nuclear Energy Institute
17. Phillip Huff, Vice Chair	Arkansas Electric Coop Corporation (W/Th)
Rich Kinas	Orlando Utilities Commission (Tu/W)
18. Scott Rosenberger	Luminant Energy
19. Kevin Sherlin	Sacramento Municipal Utility District (Tu/W)
Scott Mix	*NERC*
Howard Gugel	*NERC*
Roger Lampila	*NERC*
Robert Jones	*FSU/FCRC Consensus Center*
Stuart Langton	*FSU/FCRC Consensus Center*

SDT Members Not Participating

Jim Brenton	ERCOT
Patricio Leon	Southern California Edison
Keith Stouffer	National Institute of Standards & Technology
John Van Boxtel	WECC

Others Attending in Person

Jan Bargen	FERC
Robert Preston Lloyd	Southern California Edison
Tom Alrich	Matrikon
Jim Fletcher	American Electric Power
Brian Newell	American Electric Power
Mark Simon	Encari
Jason Marshall	Midwest ISO
Roger Fradenburgh	NetSecTech

Others Attending via Readytalk and Phone
October 12, 2010, Tuesday

Wang, Anna	amwang@burnsmcd.com
le, vincent	vincent.le@ferc.gov
Hammad, Amir	amir.hammad@constellation.com
Wilson, Bryn	wilsonwb@oge.com
Rayo, Ingrid	ingrid.rayo@constellation.com
Kelly, Justin	Justin.Kelly@ferc.gov
Farquharson, Jerome	jfarquharson@burnsmcd.com
Hardiman, Rod	rchardim@southernco.com

October 13, 2010, Wednesday

Hardiman, Rod	rchardim@southernco.com
le, vincent	vincent.le@ferc.gov
Farquharson, Jerome	jfarquharson@burnsmcd.com
Wilson, Bryn	wilsonwb@oge.com
Kelly, Justin	Justin.Kelly@ferc.gov

October 14, 2010, Thursday

Name	Email
Rayo, Ingrid	ingrid.rayo@constellation.com
Wilson, Bryn	wilsonwb@oge.com
le, vincent	vincent.le@ferc.gov
Hardiman, Rod	rchardim@southernco.com
lopez, andres	andres.lopez@usace.army.mil
Hammad, Amir	amir.hammad@constellation.com

Appendix #3 NERC Antitrust Compliance Guidelines

See Antitrust Compliance Guidelines read at the beginning of each day's session at:

The NERC reminder below was read at the beginning of each day's session.

NERC REMINDER FOR USE AT BEGINNING OF MEETINGS AND CONFERENCE CALLS THAT HAVE BEEN PUBLICLY NOTICED AND ARE OPEN TO THE PUBLIC

For face-to-face meeting, with dial-in capability:

Participants are reminded that this meeting is public. Notice of the meeting was posted on the NERC website and widely distributed. The notice included the number for dial-in participation. Participants should keep in mind that the audience may include members of the press and representatives of various governmental authorities, in addition to the expected participation by industry stakeholders.

Appendix #4
Review and Discussion of Results of September 29,2010 CIP 002-4 Webinar

The SDT reviewed, discussed and reached agreement on the over 100 questions and the actual responses provided during the webinar. Webinar questions were offered verbally and by a chat function. Howard Gugel noted that the final question and response document will be posted for industry review on the NERC website as soon as the SDT reviewed and agreed with the responses. The SDT agreed to craft, where needed, additional clarification comments to the member responses offered during the Webinar.

1. **What are reasonable costs? Slide 10**

   Comments on Response
   - Alan Mosher presentation of context and response. Slide speaks to "reasonable" costs.
   - Generally speaking we should de personalize SDT responses but not this one since Alan is not speaking for the SDT but for the Standards Committee.

   Final Response: (Allen Mosher) The idea here is that we all are subject to our budget constraints. We want to use our resources effectively. The question is, can we craft controls that present reasonable costs to the industry to secure BES assets from cyber attacks, and what's the best use of the resources? We could spend a lot of money getting perfection in one area, but since we're trying to accomplish defense in depth, we need to have controls that are balanced across all the requirements so that in total we get an effective Cyber Security program. So there's a balance in both the cost of requirements and, in my mind, across this whole reliability budget that each utility and the industry faces.

2. **Was the fact that the Second Ballot overlaps the Thanksgiving Holiday discussed? This only gives 5 business days for the industry to respond.**

   Response Comments, Tuesday
   - OK with response. A participant pointed out this could mean the SDT may get less industry response and review.

   Final Response: Yes. Unfortunately, that's just the way the timing fell, and in order for us to prepare this as a filing to FERC by the end of the year, that's just an unfortunate part of the schedule.

3. **Slide 14: Is the plan in addressing the remaining 50 FERC directives still to keep the CIP-003 through CIP-009 nomenclature or will it be to combine into CIP-011?**

Response Comments, Tuesday

- Edit the redundant response. OK

Final Response: We received a lot of feedback on whether to keep CIP-10 and -11 and CIP-3 through -9 from the informal comment period. We're still dealing with that as a Drafting Team and trying to determine the best approach to present those requirements. What we come forward with in July of next year will reflect where we're going as a team.

4. **Slide 17: Will the data request results be provided external to the SDT (e.g. industry, FERC, others)?**

Response Comments, Tuesday

- Make this a NERC response to the data request. Howard made edits.

*Final Response: "*Yes, they will be posted by NERC at some point. NERC is in the process of scrubbing the responses and determining how to post a summary But certainly, the results of that would have to be provided to FERC and to the participants. Individual responses will not be posted publicly, so that any individual entity cannot be identified."

5. **What is the process to update the criteria in the future? will it go through industry voting? Is there something in the NERC ROP to accommodate this?**

Response Comments, Tuesday

- Delete 2nd line of draft response.

*Final Response: "*Attachment 1 is part of CIP standard 002-4. Any changes to the criteria will have to go through the Standard Development Process*."*

6. **Does the definition on slide 19 apply to the StruxNet LNK Recommendation? Do you expect entities to report on DCS or SCADA that are not critical to BES?**

Response Comments, Tuesday

- Critical Cyber Asset Identification Slide 19
- Answer to first quest is No.
- This is an alert to industry and has nothing to do with the CIP standards.
- This is a NERC Rules of Procedures alert process.

Final Response: (Scott Mix) The Stuxnet alert advisory came out independent of any Standards or compliance or auditing actions, and so anything that happens in the Standards world is not directly applicable to the alerts that come out. Stuxnet was a mandatory recommendation with a required response. And as such, it actually falls

under the NERC Rules of Procedure, not the compliance program or in response to a Standards action.
***Additional clarification from SDT*:** The answer to the first question is No. The answer to the second question is Yes.

7. **Slide 16 - If the intent is to replace the non-uniform risk based methodologies with the bright-line criteria in new attachment 1, why does the new R3 still require Sr Manager approval of the risk based methodology as shown in Draft 1 dated 9/20/2010? It seems that Sr. Manager approval of the CA and CCA lists would be sufficient.**

   Response Comments, Tuesday
   - Howard Gugel will make the changes regarding the errata
   - Is there a fiduciary level manager sign off?

   Final Response: (Howard Gugel) "This was an oversight, and at the time when the Standards will be balloted, we will be issuing an errata change to R3 to remove the reference to the approval of the risk based methodology. There is one other area that was missed in the editing process (CIP-008-4). These changes will be made before the balloting is performed and the ballot body will be notified of the changes."

8. **Second question - How can compliance be measured for "anything else the RE wants to include"? This kind if ambiguity is not appropriate in a Standard.**

   Response Comments- Tuesday
   - "Any asset as a critical"

   Final Response: "This particular criterion is not intended to be measurable; it is an option that allows a responsible entity to identify any asset as a Critical Asset, it can be anything the entity wants to include. So from the point of view of enforcement, there's really not much in terms of how you measure that. However, any Critical Asset that you include in that list would also have to be evaluated to determine if it has identified Critical Cyber Assets associated with it."

9. **What is "bright-lines"**

   Response Comments- Tuesday
   - 1500 does not apply to blackstart?
   - Reference to 1.1.?
   - There are other criteria that apply.

   Final Response: Generally, bright lines are those types of criteria that have a very well defined threshold that allows you to decide whether a BES Asset is qualified as a Critical Asset or not. There are usually very definite numeric values which are not subject to any kind of evaluation or subject to engineering studies and such.
   For example, Criterion 1.1 refers to aggregate generation at a single location of 1,500 megawatts. This is a bright line. So aggregate generation below 1,500 megawatts does

not have to be identified as a Critical Asset based on Criterion 1.1, and aggregate generation that is equal to or above 1500 megawatts has to be identified as a Critical Asset based on Criterion 1.1.

10. Slide 22- How was the 1500 MW criteria determined and or what was it based on?

Response Comments- Tuesday

- 1/3 generation would be captured. Average of a sampling
- Average of the sampling of the reserve sharing. Missing WECC.
- Argument for average is weak.
- Chose number because 1/3 of generation fell into that. Took an average of those numbers.
- "Desk survey"- informal-
- "Determined" – vs. supported
- Additional clarification statement agreed to. U.S. Energy Administration source of the data-base.

*Final Response: "*In prior versions we had wording about reserve sharing, and that was the threshold to be compared for critical threshold for generation. We got a lot of feedback that that wording was confusing, that the amount referred to in the reserve sharing was not a specific amount, and that the amounts changed daily.
So we did an informal survey of the regions, and we identified what the megawatt value of the reserve sharing would be for various groups, and then we took an average of those numerical values. And that 1,500 megawatts represents that numerical average of the values of the reserve sharing amounts."
Additional clarification from SDT: The 1500 MW level was supported by looking at the DOE Energy Information Administration database, and it was determined that approximately a third of the generation in the US would be classified as Critical Assets.

11. Slide 22: Will nuclear units under the 1500 MW units be classified as critical?

Response Comments- Tuesday

- "Units"- Wording in standard- reference aggregate generation at a single plant location.

Final Response: "The standard as it stands today does not specifically call out anything special about nuclear units. You apply the same criteria that are in Attachment 1 that apply to generation and determine whether these are Critical Assets or not.
Additional clarification from SDT: The wording of Criterion 1.1 refers to aggregate generation at a single plant location, not unit specific.

12. Slide 22 - I assume critical assets "designated" by Transmission Planners will be independently verified?

Final Response: "According to our understanding of the audit process, pre work that would be done by the audit team in preparation for doing an audit against the revised CIP 002-4 would be to contact the appropriate transmission planners and planning authorities to determine if there were any assets that had been designated and verify that those assets were included in the Critical Asset list. That is consistent with the way other Standards that have linkages between them are audited."

13. **Slide 21: If existing Critical Assets do not meet the bright line criteria and are not identified under the catch all, what would the effective date of retiring them as Critical Assets? Would the implementation plan address this or would they drop off the list when CIP-002-4 becomes effective?**

Response Comments- Tuesday

- 3-6 years. Is this longer than the standard requires.
- "May" be retired? Keeps open the CIP 010-11.
- Scott checked with Roger and approved the language with edits.

Response Comments- Wednesday

- Joe Doetzl offered draft language. "The post version 4 version 4 standards…..
- OK with new language.

Final Response. "The implementation plan for the Version 4 CIP Standards does not specifically address this scenario, but since the methodology that identified them as Critical Assets is only required under Version 3 of the Standards, they would be retired as Critical Assets upon the effective date of the Version 4 Standards, which is when you're required to be in compliance with the new version of CIP 002-4.
The post version 4 standards are still in development and may impact your decision to remove assets from the list. So even though it may be retired as a Critical Asset, it still may be included as either a medium impact or a low impact in the future.
From a compliance standpoint, the compliance scope is either three or six years, so you would need to maintain any evidence of compliance for that asset during the time that it was on the Critical Asset list."

14. **Are we to understand that reliability purpose in 1.3 is for long term only (RMR)?**

Response Comments- Tuesday

- We didn't answer during the webinar? Spoke about RMR. (on row 45 -answer provided is right. Reference: See line 45).

*Final Response: "*See answer to question 44. (line 45)"

15. **Does this include black start even if it is the 3rd or 4th path**

Response Comments- Tuesday

- Question is confusing. Talking about a unit in blackstart.

- Are we talking about path?
- Path is dealing with cranking path not black start unit.
- Does blackstart definition include units and paths? This is adequately answered.

Final Response: What we've done in the attachment is use the term "Blackstart Resource," which is a term that is defined in the NERC glossary. As the Standard is currently written, if it's identified as a Blackstart Resource, it would be included as a Critical Asset, regardless of whether it's the third or fourth path. If it's in the Transmission Operator's restoration plan, then it is a Critical Asset.

16. **Slide 22 Can we discuss the definition of Plants with group of units? (16)**

Response Comments- Tuesday

- OK

Final Response: "This is in reference to Criterion 1.1, which says, "Each group of generating units, including nuclear generation, at a single plant location." This is generally understood to be a single plant, whether it's a single unit or all the units in that plant. One thing to note is that "plant" is not a NERC-defined term, so we can't really refer to "plant" as a defined term within the Standards."

17. **Slide #24 In the Rational document, page 15, the following statement is made: "While it is clear that the primary and all backup control centers operated by RCs, BAs, and TOPs must be designated as Critical Assets". This statement not based on any Commission approved Standard and goes could be interpreted as an unjust interpretation. Recommend a qualification of a MW level be added to 1.14, as written in CIP-010. If not all BAs, TOP's and RC's regardless of size will automatically be designated as a Critical Asset.**

Response Comments- Tuesday

- OK

Final Response: "As discussed in the Reference Document, this requirement is sourced from EOP-008. Control centers performing these functional obligations are considered important enough to require mandatory backup requirements and warrant designation as Critical Assets."

18. **Assume that a power plant has four 400 MW units and is > 1500 MW power plant and therefore meets the definition of a Critical Asset in accordance with attachment 1. Let's assume also that there are no systems (other than the EMS) that impact more than one of the four units. How would one go about determining if any DCS's or digital relays at the plant are critical cyber assets or not since in this example no cyber asset (besides EMS) can impact more than 400 MW? There seems to be a lack of bright lines specific to cyber assets within a power plant or substation.**

Response Comments- Tuesday

- Didn't respond to this in webinar.
- Proposed language: "only"? "excluding blackstart resources"
- "Only shared"?
- Is this "communications"? Adds a whole new layer.
- Need to evaluate before agreeing to the assumption about DSC or digital relays not impacting more than 400 MW?
- Lack of bright lines for cyber assets.
- Bright lines focus was for critical assets not critical cyber assets.

Final Response: Requirement R2 states "For each group of generating units (including nuclear generation) at a single plant location identified in Attachment 1, criterion 1.1, the only Cyber Assets that must be considered are those shared Cyber Assets that could adversely impact the reliable operation of any combination of units that in aggregate exceed Attachment 1, criterion 1.1 within 15 minutes." The focus of Version 4 was to provide bright lines for Critical Asset identification, not Critical Cyber Asset identification.

19. Please elaborate on the term functional obligations in 1.14

Response Comments- Tuesday

- Rewrote the response referencing functional obligations from the NERC functional model.

Final Response: "Functional obligations are determined from the NERC functional model. That term used here refers to the tasks those functional entities (e.g. RCs, BAs, and TOPs) perform, which is referred to in EOP-008."

20. Attachment 1, 1.15 A Black Start Unit should not by itself trigger a GOP Control Center as a Critical Asset - The Black Start Unit is under the TOP Control Center during Black Start conditions - not the GOP Control Center

Response Comments- Tuesday

- "Blackstart under" TOP?
- Verbal control from a GOP? Does the control center become a critical asset.
- Vulnerability in non black out condition.
- Disable it?
- Answers the question what has been posted.
- Is what has been posted what the SDT wants?
- Separate determination for a critical cyber asset?
- Is what the standard says what we intended?
- Are we reinforcing this?

Final Response: "As currently proposed, Criterion 1.15 states that each generation control center and backup control center used to control generation identified as Critical Assets, or used to control generation for an aggregate of 1,500 megawatts within a single Interconnection is a Critical Asset. So if a Black Start unit is designated as a Critical Asset and you have a control center that is used to control generation for that Critical Asset, then that generation control center is a Critical Asset."

21. Which guideline is being referred to?

Response Comments- Tuesday

- Several "guidance" references-all posted. Assume it is the "Guideline for identification for critical assets, etc"

Final Response: "The SDT notes that this is probably in reference to the difference between control centers and control rooms. This guidance can be found in *Security Guideline for the Electricity Sector: Identifying Critical Assets*, which can be found at http://www.nerc.com/fileUploads/File/Standards/Critcal_Asset_Identification_2009Nov19.pdf . Additional guidance documents can be found on the NERC Reliability Standards page under Critical Infrastructure Protection (CIP)."

22. Can you clarify what is meant by "automatic load shedding"? Would this include load management systems that have the ability to reduce loads by greater than 300 MWs?

Response Comments- Tuesday

- This was the answer of the member at the time.
- What we have in the response is not entirely clear.
- "language"- offered- for clarification.

Final Response: "We had a somewhat extended discussion in the Drafting Team about the term "automatic", and in the paper that we put out, we discussed what we mean by "automatic." It includes those assets, those systems that are in the transmission system that would automatically trigger load shed under certain conditions. So those are certainly in scope here. As far as computer systems, the criteria says, "common control systems capable of performing automatic load shedding of 300 megawatts or more." So if you have a single control system that is capable of performing automatic load shedding of 300 megawatts or more, that is in scope.
Additional clarification by the SDT: If you feel that additional clarification on the definition is needed, please provide that in your comments along with a proposed solution.

23. Could you please expand on what is meant by Control Generation in 1.15 Criteria.

Response Comments- Tuesday

- Expand on what we mean by control?
- "by which generation can be controlled?
- Can ISO send a zero set point?
- Use "supervisory control?" What does this mean?
- If GOP supervises a plant-
- Further discussion needed
- Need to do this now.
- Review "control center" definition.
- "display of data" is not critical. Had trouble with several things in the definition. This is on another team.
- Functional obligations of the GOP? Instead of singling out control center. Control centers performing functional obligations of the GOP…..?
- Part of comment period.
- Putting this out for comment.
- What does control generation mean?
- Provide us alternative language as part of their comments. E.g. given.
- Little time to respond to comments and no comments. If we do a better job of answering.
- Primary objectives- get the responses finalized. Use this time to come up with solutions.
- Taking the time.
- Go through get out in front. Get what we can resolved now. Get through the response document
- We haven't answered what was asked for. What do we mean when we say control generation. Guideline re control center- 1st aspect of control center.
- Howard Gugel will work on language.
- Struggling without common terms. Answer the question with the SDT's intent. We may need others to define. Other cyber contexts- years of discussion allow for.
- The webinar response was not correct reading of the standard language.
- As a team what do we want to say. Reset the common intent and common definitions.
- Some others not responded.
- Can we say in this standard what the term means- e.g. for the purpose of this requirement or standards… Each one has to have those words.

Response Comments- Wednesday

- "Monitoring and control?"
- Question focuses on control generation. 1.15.
- Version 1 FAQ- monitoring and operating control functions- covers the water front.
- Control = Seeing their display- picking up phone and telling them to do something.

- Operator is part of completing the control loop.
- Operator is a "filter"-
- Monitoring data that would affect the operation- considered in scope of control of the critical asset.
- Why not include monitoring? Monitor for maintenance, for trade,
- What was meant was monitoring for control" Control of generation includes Monitoring control.
- "Display of data" as a term is problematic.
- 1.15 Refers only to "control centers"
- Only looking for those with supervisory or automated control. Only consider for 1.15.
- Not one bullet vs. 5 but a non-binding definition.
- It means what it meant in Version 3.
- "supervisory control" used in SCADA. Is this different?
- In terms of the guidance document- meant in terms of SCADA
- Functional model- "as directed by BA and TOP" GOP receives that direction and makes changes.
- Identify critical asset, later further define. RE would further investigate to see if they have critical cyber assets. Possibly brings in your cyber equipment. If doing it by voice.
- Puts you on a critical asset list.
- Purpose not to include monitoring was to not to include qualification.
- New language- on functional model.
- Delete the 2nd paragraph. OK.

Final Response: There are a number of generation control centers that really just monitor, and if you need to actually do generation control, they don't actually have the capability of doing that, and they would have to call up the actual local control room to be able to effect those controls. For these, the discussion was that these types of control centers are not really in scope unless they have the ability of actually controlling generation.

Additional clarification by the SDT: Based on the language in the functional model, a Generator Operator is responsible to adjust "real and reactive power as directed by the Balancing Authority and Transmission Operator." A control center that provides this functionality *would be considered a Critical Asset if it meets the rest of Criterion 1.15.)*

24. CIP-002-4 attachment 1, 1.15 includes control centers that control critical assets, in addition to the 1500MW criteria. You didn't mention that - has that changed?

Response Comments- Tuesday

- Linked to the ones above.

Final Response: No, these are required to be designated as Critical Assets as well

25. Question about Comment stated during Slide 24: "Generation Control Centers are those locations which perform control of more than one location, while Generation Control Rooms perform control for one location." I would like confirmation that a Control Room controlling multiple Units, at the same location and fenced perimeter, is still considered a Generation Control Room, and not a Control Center.

Response Comments- Tuesday

- Good as is.

*Final Response: "*That is correct. We are targeting those that are controlling multiple generation locations. There is some discussion of that in the guideline for identification of Critical Assets for CIP Version 1 and 2. There is a discussion of control room and control center there, and this is what we mean by a control center in this criterion."

26. You need to provide guidance on control centers. There are some TOPs that operate only low voltage transmission. 46 kV, 69 kV and 115 kV are examples. None of these facilities qualify as Critical Assets from a transmission perspective. These facilities are often operated and monitored from a dispatch center using SCADA. Would the current CIP-002-004 language define these dispatch offices as "Control Centers?" Is there some NERC document that defines these dispatch offices as something other than a control center?

Response Comments- Tuesday

- Ok
- If you have a control center 115 KV but has load shedding capability, put that entire control center under scope.
- Criteria speaks to control systems.

Final Response: The NERC Guideline on Critical Asset Identification has a good discussion of Control Centers. For the purpose of the this standard, control centers that perform the functional obligations of Reliability Coordinators, Balancing Authorities or Transmission Operator are designated as Critical Assets. For generation, part 1.15 of Attachment 1 designates generation control centers that control generation for Critical Assets or that control generation for 1500 MW or more in a single Interconnection as Critical Assets.

27. How would the implementation plan address where we have a currently identified CA, but based on recently issued guidance, have now identified new CCA's in the CA?? Do we have 18 months to get the new identified CCA's into compliance?

Response Comments- Tuesday

- Ok

Final Response: "The assumption is that the question is referring to the guideline for identifying Critical Cyber Assets that was approved by the NERC Critical Infrastructure Protection Committee back in June. Specifically, we have not introduced additional language in the implementation plan to address this situation. Because we did not actually modify the way that Critical Cyber Assets were identified in Version 4, this situation is handled for Version 4 the way it would be handled in Version 3 in that an entity would need to refer to the Implementation Plan For Newly Identified Critical Cyber Assets and Newly registered Entities to determine the appropriate milestone that that plan identifies."

28. Slide 22: EOP-005-2 is not yet mandatory. Does the associated Blackstart definition only impact version 4 of the CIP standards (i.e. CIP-002-4)?

Response Comments- Tuesday
- OK

Final Response: The definition of Blackstart Resource was approved by the NERC Board of Trustees effective August 5, 2010.

29. On slide 38, it was noted that the key words were "support and maintenance". If those words are so key, how come they don't appear in the language of the requirements within the UASAR?

Response Comments- Tuesday
- Ok
- Doesn't occur in the SAR. In the revision history. Support and maintenance not mentioned. Its in the standard and in the SAR.

Final Response: has been communicated to the UASAR drafting team for consideration.

30. For Jim Brenton - slide 39 - is this the draft document that is posted on the project page? If so, how does the document move from the "draft" version to the "final" version?

Response Comments- Tuesday
- Will work with Jim.

Final Response: This document is posted on the Project 2010-15 web page. This document will be considered final upon approval of CIP-005-4. Until then, the document will continue to be modified based on comments received by the Project 2010-15 Drafting Team.

31. Will you be providing links to the documents mentioned in numerous slides i.e. slide 39 CIP-005 guidance document

Response Comments- Tuesday
- Ok

Final Response: They are posted at: http://www.nerc.com/filez/standards/SAR-Urgent_Action_Revisions%20to%20CIP-005-3.htm

32. When will the redline versions of the changes to CIP003-CIP009 be made availale to the industry?

Response Comments- Tuesday
- Ok

Final Response: They have been posted in the Project 2008-06 Phase II project page. http://www.nerc.com/filez/standards/Project_2008-06_Cyber_Security_PhaseII_Standards.html

33. Slide 22 - How is "initial plant for restoration" defined?

Response Comments- Tuesday
- Answer does say how it is defined. Did this come from EOP 005-2. “Initial plan for restoration.” Not defined as glossary term.
- Not defined. Is in an old standard.
- Misquoted on a slide- standard doesn’t use.
- Howard Gugel will draft new language

Final Response. The criterion calls for the term "Blackstart Resource," and as long as the facility is identified in the Transmission Operator's restoration plan as a Blackstart Resource, then it should be designated as a Critical Asset.
Additional Clarification from the SDT - initial plant for restoration is not a defined term. The slide was an attempt to frame a discussion around Blackstart Resources, specifically concerning initial switching requirements.

34. Please clarify when CCA is replaced by H/M/L?

Response Comments- Tuesday
- Ok

Final Response: The post version 4 standards are still in development.

35. There is no more CIP-10 AND CIP-11?

Response Comments- Tuesday
- Ok

Final Response: The post version 4 standards are still in development.

36. Has the drafting committee abandoned the H,M,L categorization method?

Response Comments- Tuesday
- Ok

Final Response: The post version 4 standards are still in development.

37. Regarding CIP 002 Attachment 1, 1.1. can you define the word capability

Response Comments- Tuesday
- Ok
- Howard Gugel has language: "the drafting team referred to MOD-024-1 when developing 1.1. Please refer to this standard when determining net Real Power capability.

Final Response: The drafting team referred to MOD-024-1 when developing Criterion 1.1. Please refer to this standard when determining net Real Power capability.

38. CIP 002-4 R3 includes verbiage for annual review of risk-based methodology

Response Comments- Tuesday
- The answer is yes.
- Already answered in question 6.

Final Response: Refer to answer for question 7 (line 8)

39. What version of the CIP standards are going to be audited against, version 1, 2, or 3?

Response Comments- Tuesday
- Audit for time frame based on which version enforced.
- Version 3- does not begin until January 15 2011.

Final Response: The answer is yes. It depends on the specific timeframe that the audit is addressing. Remember that the audits look back three years or six years, depending on the type of entity that you are, and you are expected to demonstrate compliance with the Standard that was in force at the time of the audit. So right now, if an entity is being audited today, as we speak, they would be expected to demonstrate compliance with Version 2 of the Standards going back to April 1, and Version 1 of the Standards going before April 1. After this week, next week, they would be required to demonstrate compliance with Version 3 for anything going back to October 1, Version 2 going back to April 1, and Version 1 moving back beyond that.

Assuming that the implementation timeframe for Version 4 comes in within the general timelines that were discussed in the presentation, it is possible that the three-year look-back period will have requirements that will have the expectation that you would have to demonstrate compliance for all four versions of the Standards, depending on which particular timeframe the auditors are looking at. And any further information on that, you would have to discuss with your particular audit team to determine exactly how they're going to request that kind of evidence and what they're going to be looking for.

40. How "robust" are the 1500 MWe and 15 minute limits in R1 Attachment for Generators, i.e. voting position may depend on these limits.

Response Comments- Tuesday
- The limit is what it is.
- Proposed limits. You are encouraged to submit comments.
- It is a politically motivated number addressing concern. Can't rationalize any number.
- Refer to question 10 (line 11)

Final Response: Please refer to the answer to question 10 (line 11).

41. Is it still acceptable to have critical assets with no CCA'a

Response Comments- Tuesday
- Use Howard Gugel's language-.

Final Response: "It is not necessary for a Critical Asset to have Critical Cyber Assets."

42. Question - It appears that NERC has addressed a common way to determine Critical Assets, but NERC did not define "essential to reliable operation of a Critical Asset" thus, the new CIP-002-4 standard does not seem to actual compell the Industry to protect any more devices.

Response Comments- Tuesday
- Issues of identifying critical assets"
- The point of standard to identify critical cyber assets.

Final Response: 'The scope of the changes to CIP-002−4 is directed at resolving a certain number of issues of identifying Critical Assets.'

43. Question regarding control centers at the distribution side with automatic load shed capability of 100MW or more. Will these be expected to be evaluated under CIP 002-4?

Response Comments- Tuesday
- Flag to come back to.

Final Response: Currently the criteria says that you have to designate as Critical Assets those systems that are capable of load shedding automatically--automatically load shed--300 megawatts or more within 15 minutes.

***Additional clarification from the SDT*:** Please refer to the answer to question 22.

44. You mention required to run for reliability is not the same as RMR. Is the guidance to then simply request a determination from the Trans Planner?

Response Comments- Tuesday
- Tie to automatic load shed.
- OK. With edits.

*Final Response: "*The responsible entity has to check with his Planning Coordinator or Transmission Planner on whether his unit is designated, or what other units are designated as "must run for reliability reasons." In certain regions, the term "RMR" is used for different reasons."

45. Could you post or advise on the specific URL where CIP info is included?

Response Comments- Tuesday
- OK.

Final Response: They have been posted in the Project 2008-06 Phase II project page. http://www.nerc.com/filez/standards/Project_2008-06_Cyber_Security_PhaseII_Standards.html.

46. Will there be a formal comments period and ballot available for the changes being introduced for CIP003-CIP009?

Response Comments- Tuesday
- OK.

Final Response: The conforming changes to CIP-003-CIP-009 have been posted. The comment period and ballot are coincident with the CIP-002-4 standard.

47. Why wasn't "essential to reliable operation" addressed?

Response Comments- Tuesday
- OK.

Final Response: This is part of the definition for Critical Cyber Asset. The definition was not changed. Version 4 is narrowly scoped to address issues with Critical Assets.

48. Has FERC reviewed the proposed implementation schedules and are they in agreement?

Response Comments- Tuesday
- OK.

*Final Response: "*FERC approved the Version 3 Implementation Plans. The Implementation Plan for Version 4 will be submitted for FERC approval with Version 4 of the CIP standards."

49. If the revised CIP-005 refers to "guidelines" what is the risk that a utility interprets "guidelines" as optional and an auditor doesn't?

Response Comments- Tuesday
- CIP 005 doesn't refer to guidelines. No standard refers to guidelines.
- The auditor works to the requirements not the guidelines.

*Final Response: "*There is not a reference to a "guideline" in CIP-005-4. The auditor audits to the standards/requirements, not any guidelines."

50. In relation to R2.1, is there any intention to remove the serial exemption in the future? Previous draft version 4's have removed the serial exemption. Is this intended to be reintroduced into future revisions of the standard?

Response Comments- Tuesday
- OK.

*Final Response: "*The connectivity qualifications for Critical Cyber Assets still apply in CIP-002-4. Post Version 4 development is in progress, and connectivity is a consideration in the application of security controls."

51. Please provide additional clarification regarding the black start and cranking path brightliness associated with CIP-002 V4.

Response Comments- Tuesday
- Initial switching requirements and multiple path options are used in criteria?
- Lack of clarity comes from the sourced standards..
- Referring to the Transmission Operators restoration plan?
- What does multiple path mean?
- Is it the first load that you sync to?
- This was debated right before we posted.
- Is there a standard way of testing black start capability? Following the EOP? Testing the unit.
- Reference those are out of the EEI. Wording added. Consider including examples in guidance document.
- Jackie Collett and Doug Johnson will look at wording at what in standard. Address that language which isn't clear.

Response Comments-Wednesday
- Wish there was something about EOP.
- The SDT moved away from using the term "cranking path" because it wasn't defined.
- The proposed response language is consistent with what we have in the draft standard.

- EOP 005-2 requires testing everything in your plan for 3 years. Whatever you tested is critical, not what you have in the plan.
- "The choice of the next load" is key?
- First part of change reference cyber assets. Take the first reference out.

*Final Response: "*The intent of Criterion of 1.5 is to identify enough Cranking Path Facilities required during initial restoration as Critical Assets, up to the point where the entity has a choice of the next Facility or Facilities to use as part of the Cranking Path. The result is to provide protection for the constrained portions of the Cranking Paths, and to allow an entity some flexibility in defining their restoration sequence during an actual event."

52. Where can I find a document that summarizes only the differences between Rev 3 and the proposed 4?

Response Comments- Tuesday

- OK.

Final Response: The redline versions provide changes from Version 3 to Version 4. The mapping document also provides a review of changes.

53. Slide 16 - please explain the term "significantly mitigate" as it relates to oversight

Response Comments- Tuesday

- OK.

Final Response: The FERC directive really applies with respect to the previous Versions 1, 2, and 3 Standards where entities were using their self-defined risk-based assessment methodology to define Critical Assets. Paragraph 439 of Order 706 basically talked about the requirement for some oversight over that list of Critical Assets to ensure that it is adequate or not.
The opinion of the Drafting Team with respect to this particular directive from FERC is that by the use of bright line criteria in Attachment 1, there is no longer a need to verify the list, because it is a list derived from bright lines. A BES asset is either in or out, or the criteria are bright enough so that you can determine whether the Critical Asset qualifies or not, so there is no longer a need for oversight. "Significantly mitigated," means that, if not eliminated, there is significant mitigation of that requirement or of the issue by the use of bright line criteria.

54. For entities that have not claimed any CC's, 24 months could pose an extreme hardship both staffing and financially. Many entities have budgets that have been set for 2011 for both staffing levels and for finances. Could this implementation plan be expanded out to allow entities to plan financially and staffing wise?

Response Comments- Tuesday

- OK.

Final Response; The 24 month period to comply for entities who had not previously identified Critical Cyber Assets is the timeframe that's in the existing IPFNICCAANRE, or Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities. This is the currently approved implementation plan.

55. Item 1.6 on Attachment 1 of CIP-002-4 uses the term "Transmission Facilities". As defined in the NERC glossary this is a very broad definition covering lines, generators, shunt compensators, transformers, ETC. Facilities inside a substation enclosure can be protected but not miles of lines. Can you please clarify?

Response Comments- Tuesday

- Language okay substantively. Jackie will work with Howard for some editorial suggestions.

*Final Response; "*The standard does not require the protection of Critical Assets. It requires the protection of Critical Cyber Assets. So whether your cyber asset is in a centralized location within a substation, or a little away from the substation, that cyber asset would be subject to the requirements of the CIP Standards if it is essential to the operation of the Critical Asset."

56. Are isolated SCADA systems required to comply with these NERC reporting requirements

Response Comments- Tuesday

- Meet criteria for CAs and qualifications for CCAs?
- OK with Howard Gugel.

Final Response: Yes, if their associated BES asset meets the criteria for Critical Assets and the SCADA meets the qualifications for Critical Cyber Assets.

57. There are entities that have performed varies technical analysis to show that the requirements of attachment 1 do not affect the BES. Will these studies be considered to have an asset NOT defined a critical asset.

Response Comments- Tuesday

- Small coops- fall under this with possible expenses.
- Should we revisit this?
- Based on what we have out as CIP 002-4. They are critical asset if they meet.
- What is definition of a proper "authoritative study" to determine these and codify in the standard? Probably couldn't do.

- If we open any criteria up to evaluation to allow an exception it will produce a new "can of worms" and TFEs. Will this puts back on the table someone to review and approve a criteria?
- The ability to have custom user defined studies introduces the need for oversight which is what bright lines are trying to eliminate.

Final Response; No, if a BES Asset meets any of the criteria in Attachment 1, it must be designated as a Critical Asset. The ability to have user-defined technical analysis to exclude an asset that would meet the criteria of a Critical Asset would introduce the need for oversight, which defeats the purpose for bright line criteria.

58. What is meant by "single plant location" in criterion 1.1 of attachment 1? What about adjacent plants?

Response Comments- Tuesday

- We mean area encompasses a plant.
- We don't have the answer that what is a plant.
- Can a plant have multiple shipyards.
- Gerry Freese will draft a strawman response.

Final Response: Single plant location refers to a group of generating units occupying a defined physical footprint and designated as an individual "plant" using commonly accepted generating facility terminology. Adjacent plants would be defined using the same criteria. The units do not necessarily have to be connected to the BES at the same substation or interconnection point in order to be considered a single plant.

59. Was CAN-005 sent out via the NERC Alert system only?

Response Comments- Tuesday

- OK.

Final Response: No, CAN-005 was issued by compliance through a notice to NERC stakeholders.

60. Shouldn't the current CIP-005-3 have the same modifications as CIP-003 thru CIP-009 to prevent complications for Nuclear facilities?

Response Comments- Tuesday

- OK.
- Removed nuclear exclusion to be consistent with 706 B. Applied only to US jurisdictions not to Canadian facilities. Handled by CNSC.
- Not a conforming change, but an actual substantive change? No it is conforming.

Final Response: Conforming changes will be made upon filing.

61. Item 1.7 on Attachment 1 of CIP-002-4 was changed from "4 or more" to "3 or more". This has a tremendous impact on affected transmission facilities. Can you please explain the reasoning behind this change?

Response Comments- Tuesday
- Drafting team felt it was appropriate to refer to connected transmission substations to address parallel lines
- Not doing generating sub-stations.

Final Response: "In order to be more accurate in terms of the impact, the Drafting Team thought that it was more appropriate to refer to the number of connected transmission substations instead of lines connected to any particular transmission sub-station. The intent was to get away from the double-circuit conditions and to include facilities that are actually more a part of the network than simple substations with double circuits between them."

62. Will the regional entities push back if assets are removed from the CA lists because of the new criteria?

Response Comments- Tuesday
- SDT can't comment on this.

Final Response: The drafting team cannot comment on the possibility of push back.

63. Is the remote access Reference\Guidance document available yet?

Response Comments- Tuesday
- OK.

*Final Response: "*This document has been posted to the draft CIP-005-3 Modifications Urgent Action Standard page."

64. If the RE designates an entity as a CA, should the RE be responsible to communicate the determination or will the responsibility be on the entity to prove they were not designated as such for audit purposes?

Response Comments- Tuesday
- OK.

*Final Response: "*With the bright-line criteria, the responsible entity should be able to determine its own Critical Assets. Input from the RE or other registered entities may be required for that determination, in which case, the responsible entity is responsible for soliciting that information."

65. Will the Security Guideline for the Electricity Sector: Identifying Critical Cyber Assets be updated and included with the approved Version 4 CIP Standards posting?

Response Comments- Tuesday
- Guideline doesn't need to be updated since haven't changed critical cyber asset.

*Final Response: "*The SDT will discuss necessary changes with CIPC, since they own this document."

66. A SCADA system is capable of opening breakers that would shed 300+ MWs of load but is not presently programmed to perform automatic load shed. The SCADA owner is not a BA, RC or TOP. Is the SCADA system a critical asset under 1.13 of CIP-002-4 attachment 1?

Final Response: Please refer to the answer to question 22.

67. Will it take a SAR to change the 1500 when needed

Comments
- OK.

Final Response: The criteria in attachment 1 are part of the CIP-002-4 standard and must follow standard revision procedures.

68. So since there is no technical justification for generation; what is the justification for the transmission thresholds?

Comments
- OK

Final Response: The reference document outlines the rationale for the criteria.

69. Would David Revill repeat his comment regarding Effective Date as determined by NERC- vs. FERC-approval?

Comments
- In Canada vs. U.S.? In the presentation.

Final Response: (from Speaker Notes) All entities should be compliant with CIP-002-4 on the Effective Date of the Standard. The Effective Date is defined in the Standard to be the first day of the third calendar quarter after applicable regulatory approvals. For those that do not have an applicable regulatory approval, the Effective Date is the first day of the third calendar quarter after the NERC Board of Trustees adoption. For those in the U.S., this is at least 6 months following FERC approval.

70. Does Attachment 1 criteria 1.4 apply to all blackstart resources in the restoration plan or is it limited to those associated with primary restoration paths. For example, if a restoration plan lists several alternate paths in addition to the primary restoration path, would the resources associated with the alternate paths be considered critical assets.

Comments
- "primary restoration path?"
- OK with response.

Final Response: The criterion calls for the term "Blackstart Resource," and as long as the facility is identified in the Transmission Operator's restoration plan as a Blackstart Resource, then it should be designated as a Critical Asset.

71. Slide 24 / CIP2 R4 Attachment 1 paragraph 1.14. All TOP Control Centers and Backup Control Centers are being classified as High risk CA's. This is independent of the criteria for determining the criticality of the substations that they control (paragraph 1.6 & 1.7). Why are ALL of these control centers being included as high risk CA's via the bright line criteria?

Comments
- OK

Final Response: EOP-008 specifically requires control centers that perform the obligations of the RC, BA or TOP to have backups. As such, these control centers and backup control centers must be designated as Critical Assets, irrespective of size.

72. What is the new timeline associated with the development of CIP-010 and CIP-011?

Comments
- OK

Final Response: Posting for formal comment and first ballot in July 2011 and filing to FERC by the end of 2011.

73. Bright Line criteria question. In the case of generation controlled/dispatched by a "Control Center" for wholesale power marketing purposes, how do you determine the 1500MW value? Would that be an aggregate of the regulation/dispatch limits (since the entire output cannot be controlled) or the aggregate output of all generation under control?

Comments
- EOP 5? Doesn't deal with control centers but with units?
- 1.15- rated net real power capability?

- FLAG- DJ.
- Goes with 24-

Response Comments Wed.

- We expect to use the aggregate higher rate real power
- The aggregate output of
- Use the aggregate of the same criteria as 1.1.
- The answer to the question is th
- If you deviate from 1.1 criteria, the value changes on the fly.
- Nothing for reliability for control? Plant controlled for economics part of reliability of the BES.
- If this control system tied to anyone else?
- 2 sentences.?
- Encourage more people to vote no with comments.
- "Part of the reason for this is that data flowing through the control center to others is the full output of the center."
- Does having the ability to take them off line do that.
- Multiple scenarios out- do we allow generation control centers to use the smaller number, and potentially lose some of those that are a data source. Or more fancy words to try to lock those in.
- Use the larger of the values. Use the same as 1.1. Our standard doesn't distinguish between marketing and reliability.
- Nameplate minimum and maximum loads are known.
- Switched off of nameplate because of the variability.
- Respond to what the standard is today.
- Say we are doing this on a generation basis. Wholesale market is not part of reliability. "
- The control center is identified because it is performing generation control irrespective of market purpose.
- We need to come back to this when we get comments on the standard.

Final Response: We would expect to use the same criteria as in Criterion 1.1. This is the aggregate output of all generation under dispatch/control. The control center is considered a Critical Asset due to the fact that it is performing generation control, irrespective of whether it is performing wholesale power marketing functions.

74. For determination of critical assets, how was the 1000 MVAR threshold for reactive resources arrived at?

Response Comments

- OK

Final Response: This value was determined to be reasonable by the CIP-002 subteam, based on generation criteria.

75. Why is there a preoccupation with moving to CIP 10 and 11? CIP-002 - CIP-009 have some natural breaks in them that can make them easier to administer among departments and the industry is comfortable with them. Why can't the team just continue to add new versions of the existing standard numbers?

Response Comments
- OK

Final Response: The drafting team continues to consider structuring options based on comments and requirements.

76. Attachment 1, 1.3 - can specific criteria be added to 1.3 for more specificity?

Response Comments
- OK

Final Response: Please propose alternative language that would clarify the criterion without introducing terms that already have implied use in certain regions.

77. **What about TFE's? RFC is requesting vendor letters, such as CISCO, that states that their product does not meet xxsx standard. This seems rather archaic. Can NERC make some sense of this issue?**

Response Comments
- OK

Final Response: The issue of Technical Feasibility Exceptions is high on the SDT's consideration in drafting the next version of the standards.

78. In the future, does the SDT still plan to revise CIP-002 to have all BES Assets identified as High , Medium, or Low?

Response Comments
- OK

Final Response: The SDT is still developing the next version. This is a consideration in this development.

79. As part of CIP-002-4 initiative, will there be a "bright line" categorization for Critical Cyber Assets?

Response Comments
- OK

Final Response: There is no substantive change in Version 4 for categorizing/ qualifying Critical Cyber Assets.

80. GO/GOP in some cases, such as wind generation, utilize remote operations centers operated by third party operators for tasks such as restarts and generation curtailments. What should be considered in determining if this is a Control Center as opposed to a control room?

Response Comments

- Point back to critical asset guideline for distinction between control centers and control rooms- perimeter around 1 or multiple locations. Point to same criteria. Point to Line 24
- This is pointing to a specific example.
- "Security Guidance for Electricity Sector: Guideline provides a discussion on the difference…..

Final Response: These are considered generation control centers subject to the criteria for generation control centers. The document "Security Guideline for the Electricity Sector: Identifying Critical Assets" provides a discussion on the difference between control centers and control rooms.

81. What if those group of units at one plant location do not all have common, interconnected cyber systems?

Response Comments

- Point to criteria in Attachment-
- Row 19 language.

Final Response: The plant location should be considered for qualification as a Critical Asset per Criterion 1.1. The cyber assets to be considered for qualification as Critical Cyber Assets have a specific qualification in R2 of CIP002-4, which is "For each group of generating units (including nuclear generation) at a single plant location identified in Attachment 1, criterion 1.1, the only Cyber Assets that must be considered are those shared Cyber Assets that could adversely impact the reliable operation of any combination of units that in aggregate exceed Attachment 1, criterion 1.1 within 15 minutes."

82. For Section 1.3 of CIP-002-4, shouldn't the SDT add that the PC or TP needs to notify the GO/GOP that his generation is designated as critical?

Response Comments

- OK

Final Response: The responsible entity has to check with his Planning Coordinator or Transmission Planner on whether his unit is designated, or what other units are designated as "must run for reliability reasons." Again, not all RMR are--in certain regions, the term "RMR" is also used for units designated as "must run" for market stabilization reasons.

83. When will the standards development and implementation plan be available on the NERC website?

Response Comments
- Current schedules were slides in the webinar.

Final Response: The slides for the webinar (including a high level view of the schedule) are available on the NERC site at http://www.nerc.com/files/CIP002-004-092910.pdf. The Implementation Plan for Version 4 is posted in the CIP Version 4 standards area.

84. If the effective date is the first day of the 3rd quarter after approval, couldn't the effective date be July 1 if FERC approves during the 1st quarter?

Response Comments
- Answer -No. assuming approval anytime during the first quarter,….

Final Response: No. Approval at any time during the first quarter would make April 1 the first day of the first quarter after approval, July 1 the first day of the second quarter after approval, and October 1st the first day of the third quarter after approval.

85. For example if an analysis has been performed at a local control center that opens all BES breakers and the BES remains stable would this study prevent the LCC from being a critical asset?

Response Comments
- Delete "for example"
- Line 58./ Question 57

Final Response: No, if the control center satisfies the criterion for control centers. Bright-lines do not consider the responsible entity's analysis or studies. Please refer to the answer to question 57 for additional clarification.

86. If the cranking path from Black Start resource to the next start resource is within the same substation, do you have to include the additional substations to the interconnecting/synchronizing point as critical assets?

Response Comments- Tuesday
- Is the answer yes or no?
- Blackstart unit in same substation?
- JC can look at this language differently. "Choice" is left open.
- More discussion on intent
- Look outside the sub-station?
- EOP 005, R15- have to have a plan and if all is covered..
- Flag this for further discussion.

- Glossary definition of "cranking path"? Could be within the same plant? The cranking path becomes a bus.
- 1.4 and 5 cover cranking path.

Response Comments- Wednesday

- If this substation has more than 1 path, then you could stop there.
- If meeting the EOP 005 standard, they will have additional paths.
- Draws picture. Straight bus with three transmission generators.
- Is this more than what the definition requires?
- Determines what is the unit to be started.
- If you are going to meet the other standards- says to the next generator?
- Good points. Issues with the GOP standards? NERC's definition of cranking paths?
- Wanted to use "primary cranking paths"- but it isn't defined. Was intended to be a compromise to scope this down. Did we go too far?
- Depends on what your restoration plan says.
- Hold this thought for revision of the standard.
- Interconnect is already in and this may already be covered.
- 1.10 covers this- Add 1.4 to 1.10.
- Concerns are valid but not in the CIP standards.
- 1.4 is needed to be added. The sub is part of the cranking path- where the generator connects to get it somewhere.
- Choices for path are units in the station. Take out first sentence?
- The GSU and a piece of the bus would be the cranking path in her example.
- Does it have to get of interconnecting to the system-
- Leave the one sentence

Final Response: It depends on how the Cranking Path is defined in the Transmission Operator's restoration plan.

87. Attachment 1, 1.8 - Facilities whose loss can create IROL's varies in time depending on what other transmission facilities are in service? Under what conditions is this determination to be made - in the planning horizon or the operating horizon. Also, is 1.8 meant to assume the loss of an entire substation?

Response Comments- Tuesday

- This has fundamental issues with it. Loss of facility doesn't generally create an IROL. Will be getting comments on this.
- In the planning horizon or the operating horizon
- Impacts that happen are what we are focusing on. Plan for varying operating conditions that occur.
- Don't generally violate an IROL.
- Do you calculate IROL for loss of a substation?
- Document the contingency but not doing anything about.

- Class D is the floor? Does this relate to IROLs? Not necessarily. Impact of the contingency not what kind it is.

Final Response: The criterion applies to the planning horizon. Part 1.8 assumes the loss of any combination of facilities including the loss of the whole substation.

88. Attachment 1 now creates a uniform criteria for Critical Assets. Why was the original requirement for determining Critical Cyber Assets left as "essential to reliable operation" which will just create the same problems with uniformity and auditing we had previously with Critical Assets?

Response Comments

- This was John Van Boxtel's question.

Final Response: The scope of the changes to CIP-002–4 is really directed at resolving a certain number of issues on Critical Assets.

89. 1. What devices are considered FACTS? 2. Is series cap considered a reactive resource? 3. Any IROL in Western Interconnection?

Response Comments

- SVCs, series caps,
- HVDC? Not
- #2? Yes. But may not always be a FACTS device.
- Where is definition of FACTS? Direct them there.
- WECC doesn't use the "IROL" philosophy.
- Language in Pittsburgh
- #3; FAC 014-2 requires all Reliability Coordinators to establish IROLs. Planning coordinator does the same thing.
- Refer to IEEE definition?
- Talk with planning coordinator and RC to determine if there are any in the region.
- SOL methodology.

Final Response: 1. IEEE has established a definition for FACTS. 2. Yes, but it may not always be a FACTS device. 3. FAC-014-2 requires all Reliability Coordinators and Planning Authorities to establish IROLs consistent with its SOL methodology. Please refer to your Planning Coordinator or Reliability Coordinator.

90. Are AMI systems considered to be ALS if they are 300mw or larger?

Response Comments

- Automated/Advanced Metering Infrastructure.
- Need to discuss the 300MW in the future.
- 300 MW- DOE requirement. Triggered a reporting.
- Doesn't stand up to the 1500 for generation.

- AMI distribution level? In scope? Either distribution provider. Load shed done at distribution level.
- Some could be inside commercial facility.
- Most load shed- done automatically.
- 300 MW is what it is now and get comments to change the number.

Response Comments- Wednesday

- Refer to question 22/response?
- Does the AMI act on its own?
- AMI issue before- "within 15 minutes" clarification.
- "Furthermore, the response time must be within 15 minutes in order to qualify.
- Functional model. DP implements under the direction of the TO.
- Should be the DP not the LSE in the CIP standard.
- Haven't decided yet included in DP moving forward.

Final Response: Please see the answer to question 22. Furthermore, the response time must be within 15 minutes in order to qualify.

91. Is there a specific implementation plan for CIP-005-4? Upon FERC approval, when would a Registered Entity be required to comply with the changes in CIP-005-4?

Response Comments

- 12-18 months- There will be an implementation plan developed and posted in next round of balloting.

Final Response: There will be an Implementation Plan for CIP-005-4, which will be developed and posted by Project 2010-15.

92. What is the meaning of "location" in 1.1 of Attachment 1 to CIP-002-4? For example: If a new 20 MW CT is located at an existing 1500+ MW plant and the CT connects to a different substation than the existing plant, is the 20 MW CT a critical asset?

Response Comments-Wednesday

- Refer to question.
- Plant is a critical asset by hypothesis. Unit is part of critical asset.
- Since the plant already meets bright line criteria, additional units installed at that plant….?
- If had a common control system.

Final Response: The plant would be considered a Critical Asset because it exceeds the 1500 MW threshold at a single plant location. For additional clarification in location, please refer to question 58.

93. Just as a comment, the redline and clean version of CIP-008-4 does not have the Nuclear plant exception removed. Will this be re-posted?

Response Comments
- OK. Have to go back to make sure proper language in for Canadian.
- Refer to question #7 and question on (nuclear)

Final Response: Yes, as part of an errata prior to balloting. Please refer to the answer to question 7 and question 60.

94. Where in the NERC Website that I can locate the presentation slides for today webinar?

Response Comments
- OK

Final Response: They are available at: http://www.nerc.com/files/CIP002-004-092910.pdf

95. Also, CIP-005-4 does not have the Nuclear plant exception removed either. Will this be removed with the next ballot of CIP-005-4?

Response Comments
- OK same as 93

Final Response: Yes, as part of an errata prior to balloting. Please refer to the answer to question 7 and question 60.

96. I don't believe the WECC has IROLs - how does this impact 1.8, 1.9, 1.12 in attachment 1

Response Comments
- If you have no IROLs in your area, in essence NO to 1.8,1.9 and 1.12. Copied from earlier response.

Final Response: FAC-014-2 requires all Reliability Coordinators and Planning Authorities to establish IROLs consistent with its SOL methodology. Please refer to your Planning Coordinator or Reliability Coordinator. If no IROLs have been designated, then an entity would have no assets determined to be Critical Assets based on Criteria 1.8, 1.9, and 1.12.

97. Is the 300MW load shed applicable if loads are connected less than 100kV?

Response Comments- Wed.
- **Refer to question 22.**

Final Response: No. This issue has been forwarded to Project 2010-15.

98. As it applies to the new NERC requirement in CIP005, will the term "remote access" be added to the glossary of terms?

Final Response: The definition is approved by the NERC BOT, and is provided in the current NERC Glossary of Terms.

~~**99. Are these slides currently posted on the NERC site and if so where are they located?**~~
- Asked and answered.

~~**100. CIP-002-4, R3 - includes verbiage for annual review of risk-based methodology - to be removed in errata?**~~

Response Comments
- OK

101. Since the EOP-005-2 standard and the Blackstart Resource definition are not yet FERC approved, how will this be coordinated with the FERC approval of CIP-002-4 which utilizes the Blackstart Resource definition.

Response Comments
- OK

Final Response: This issue has been referred to Project 2010-15.

102. For the purpose of interpretation of CIP-005-3, R6, does NERC consider this case as a remote access? "A person is using a CCA within an ESP to access another CCA in another ESP for the maintenance purpose."

Response Comments
- This issue has been forwarded to Project 2010-15.

Final Response: This issue has been referred to Project 2010-15.

103. Regarding the Control Room versus Control Center issue. Would a location that communicates with 2 substations, but controls a singular transmission asset be a Control Room or Center, whether the transmission asset is CA or not?

Response Comments

- OK

Final Response: It would be considered a control center if it is at a remote location.

104. Since it has been said that CIP-010 and 011 will eventually be implemented and CIP-010 (as currently drafted) CCA level impacts are High, Med and Low. If under CIP-002-4 bright line criteria in Attachment 1, you are not a CA, yet under CIP-010 you are implied to be a low impact CCA -- shouldn't there be a "no impact" category under CIP-010?

Response Comments

- Use the stock answer about future work part of CIP 010 and 11.

Final Response: The post version 4 standards are still in development.

Appendix #5 SDT Sub-Teams

Sub-Team	
CIP 010 BES System Categorization	John Lim (Lead), Rich Kinas, Jim Brenton, Dave Norton *(Observer Participants: Rod Hardiman, Jim Fletcher) (FERC: Mike Keane, Peter Kuebeck)*
Personnel and Physical Security	Doug Johnson (Lead), Rob Antonishen, Patrick Leon, Kevin Sherlin *(FERC: Drew Kittey)*
System Security and Boundary Protection	Jay Cribb (Lead), Jackie Collett, John Varnell, John Van Boxtel, Philip Huff *(Observer Participant: Brian Newell) (FERC: Justin Kelly)*
Incident Response and Recovery	Scott Rosenberger (Lead), Joe Doetzl, Tom Stevenson (*Observer Participant: Jason Marshall) (FERC: Dan Bogle)*
Access Control	Sharon Edwards (Lead), Jeff Hoffman, Jerry Freese, Bill Winters *(Observer Participants: Roger Fradenburgh, Robert Preston Lloyd) (FERC: Mike Keane)*
Change Management, System Lifecycle, Information Protection, Maintenance, and Governance	Dave Revill (Lead), Jon Stanford, Keith Stouffer, Bill Winters *(Observer Participant: Brian Newell) (FERC: Jan Bargen, Matthew Dale)*
CIP 002-4 Drafting Team	John Lim (Lead), Jim Brenton, Jackie Collett, Jay Cribb, Sharon Edwards, Doug Johnson, Rich Kinas, Dave Norton, Dave Revill, and Bill Winters *(Observer Participants: Rod Hardiman; Jim Fletcher; Bryn Wilson) (FERC: Mike Keane, Peter Kuebeck; NERC: Scott Mix)*
Implementation Plan CIP 002-4	Dave Revill (Lead), Sharon Edwards, Kevin Sherlin, Scott Rosenberg, Dave Norton and Phil Huff *(FERC: Mike Keane; NERC: Scott Mix)*
Framework CIP 010 &011	Dave Norton (Lead), Jim Brenton, Jay Cribb, Joe Doetzl, Phil Huff, Doug Johnson, Dave Revill, Jon Stanford, and John Van Boxtel. *(FERC: Mike Keane; NERC: Scott Mix)*

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Agenda
Cyber Security Order 706 SDT - Project 2008-06

October 12, 2010 | 8:00 AM to 6:00 PM EDT
October 13, 2010 | 8:00 AM to 6:00 PM EDT
October 14, 2010 | 8:00 AM to 6:00 PM EDT
Toronto, Canada

Proposed Meeting Objectives/Outcomes:

- To review September 29 webinar questions and begin the development of a response document for industry posting
- To review and discuss and test acceptability of proposals for addressing key issues presented by the CIP Framework Team
- To review the Sub-team summaries of the CIP 010 & 011 and Workshop industry comments and discuss possible responses in light of the framework review
- To agree on next steps and assignments

Tuesday, October 12, 2010 8:00 a.m. - 6:00 p.m. EDT

- Introduction, welcome -*(Morning)*
- Receive updates on other related cyber security initiatives- *NERC Staff and SDT Members (Morning)*
- Review meeting and milestone schedule for CIP 002-4 and CIP 010 and 011 *(Morning)*
- Review changes to CIP Version 4 prior to ballot (CIP-002-4 R3 and CIP-008-4 applicability)
- Review results of September 29 CIP 002-4 Webinar *(Morning)*
- Participate in ERC Event Process Analysis Webinar and discuss implications for CIP development
- Draft responses and consider any changes to CIP-002-4 based on September 29 webinar questions *(Afternoon)*

Wednesday, October 13, 2010 8:00 a.m. - 6:00 p.m. EDT

- Receive a report from the team assigned to work on the framework *(Morning)*
- Discussion of Framework Team key issues *(Morning)*
- Review and provide feedback on the acceptability of the presented approach *(Afternoon)*

116-390 Village Blvd.
Princeton, NJ 08540
609.452.8060 | www.nerc.com

Thursday, October 14, 2010, 8:00 a.m. - 6:00 p.m. EDT

- Continue discussion of prospective framework *(Morning)*
- Review Sub-teams summaries of industry and Dallas workshop comments on CIP 010 & 011
- Discuss potential responses in light of the framework
- Review Preparation for CIP 002-4 Team Organization for Responding to Industry Comments before and in Baltimore *(Afternoon)*
- Review SDT November, 2010 Baltimore Meeting Agenda (*Afternoon)*

NERC

NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

28th Meeting Summary
Cyber Security Order 706 SDT — Project 2008-06

Adopted Unanimously by the SDT December 15, 2010

Baltimore, Maryland

November 16, 2010, Tuesday - 8 AM to 6 PM EDT
November 17, 2010, Wednesday - 8 AM to 6 PM EDT
November 18, 2010, Thursday - 8 AM to 6 PM EDT

Robert Jones, Stuart Langton, and Hal Beardall
Facilitation and Meeting Design
FCRC Consensus Center, Florida State University

http://www.nerc.com/filez/standards/Project_2008-06_Cyber_Security.html

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

CSO706 SDT November 16-18, 2010 Meeting Summary Contents

Cyber Security Order 706 SDT- Project 2008-06
28TH MEETING
November 16-18, 2010
Baltimore, Maryland

EXECUTIVE SUMMARY

John Lim, Chair of the CSO 706 SDT welcomed members and other participants to Baltimore and thanked Tom Stevenson and Maggie Powell at Constellation Energy for hosting the meeting. Howard Gugel, NERC, conducted a roll call and reviewed the antitrust and public meeting guidelines at the beginning of each day. On Thursday morning, the SDT unanimously adopted the October 12-14, 2010 Ontario meeting summary.

The chair outlined the objectives the SDT sought to accomplish by the end of the meeting and Bob Jones reviewed the timed agenda for each day The Chair and Vice Chair thanked the members who joined in the daily Readytalk conference calls during the prior week to bring strawman responses to industry comments for the SDT review at this meeting.

Phil Huff reviewed the milestone schedule noting that the SDT had agreed to prepare and submit the CIP XX Version 5 to industry by July, 2011. Mr. Huff noted that the proposed schedule may be adjusted slightly in the Spring based on SDT progress but will lead to a balloting of the Version 5 proposed CIP standards by mid-year. He also pointed out that currently the Team has agreed not to put preliminary drafts out for informal industry comment in 2011.

The Chair welcomed several industry groups and invited them to make comments on the CIP 002-4. Barry Lawson on behalf of NRECA noted that he supports the efforts of the SDT and hopes they can get to a consensus on some changes based on the industry comments. He noted he abstained from voting but he and NRECA members want to be able to vote in the affirmative on the next ballot. He summarized the association's concerns around control centers for balancing authorities and transmission operators and the bright line MW criteria as well as the Blackstart portions of the criteria. The NRECA hopes that SDT will address the question of whether this draft will "incentivize people to withdraw assets from blackstart plans." Nathan Mitchell, representing APPA noted that while they voted against the standard, they are not against what the SDT is doing overall. They hope the SDT will take a new look at and address a few areas of concern regarding control centers and blackstart units. He believed it was possible to pull in public power members with some modifications in these areas. David Batz, representing EEI, echoed the other trade association comments, noting that EEI appreciated the efforts of the SDT and the complexity of the job. He reinforced EEI members' interest in a successful balloting of CIP 002-4 and suggested there was an opportunity for the SDT to improve the product noting that it won't be perfect.

Mark Weatherford, VP/Chief Security Officer, NERC, introduced himself to the Team noting that he was relatively new at NERC and at the drafting process but wanted to see how the Team is functioning.

He assured the Team that he is a supporter of the process and appreciates that the SDT is working very hard to perform a needed service for the industry.

Scott Mix reported on the CIP 005-4 Urgent Action. The CIP 005 drafting team received numerous significant comments on the posted standard. The previous standard and its associated SAR were withdrawn and replaced by updated versions. The language for CIP 005-4 Requirement R6 has been significantly modified based on industry comment, and was approved for an abbreviated posting and ballot period by the Standards Committee. NERC has posted a summary of comments received, and summary of issues raised during the previous posting period. An updated guidance document was also posted. The goal of the team is to still file the revisions for concurrent consideration of a single "Version 4" package by regulators.

Many of the SDT members and other meeting participants participated in a tour of a Constellation Energy sub-station on site on Wednesday mid-day.

Howard Gugel reported that there was a 43% approval rating from the industry. He suggested that the way the ballot process is set up leads to a high negative first vote as industry entities want to be able to make comments for the SDT to consider in any redrafting for the next ballot. He offered that the industry ballot results and comments do not represent an insurmountable task for the SDT to respond to these comments, make appropriate changes in the standard and succeed in a new ballot. He suggested the largest concerns and strongest feelings surrounded the following three areas in the standards and Attachment 1: Control Centers; Blackstart Resources; and 1.3- Transmission planner reliability "must run" units. He noted that it was very helpful to have worked through and reached agreement of the SDT on responses to the September 29 webinar questions and comments at the Toronto SDT meeting many of which were presented as comments to the ballot. Mr Gugel offered his appreciation for the participation of many of the SDT members who set time aside for each day of the preceding week to help prepare strawman responses for consideration at the Baltimore meeting.

The SDT reviewed the industry comments and a strawman response document and conducted straw polls for a number of proposed changes to the standard. In general, if the proposal received greater than 2/3 support from the Team it was incorporated into the text of the standard. The SDT initially focused on Attachment 1 and the implementation plan documents and then returned to the standards document to make any changes consistent with the agreed upon changes in Attachment 1 and the implementation plans. The SDT reviewed strawman responses to each industry comment. At the conclusion of the meeting the SDT reviewed and amended the Guidance Document consistent with the changes in the standards documents and adopted a response document for posting.

The SDT reviewed the industry comments on the Implementation Plan and the Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities and concluded that the effective date should be a 24-month period for all entities without exceptions to address the industry confusion on the first ballot proposal.

Below are displayed the results of the straw polls that formed the basis for the SDT refining and adopting a revised CIP 002-4 and related documents.

CYBER SECURITY — CRITICAL CYBER ASSET IDENTIFICATION CIP-002-4 SDT STRAW POLLS

A. INTRODUCTION-PROPOSED WORDING STRAW POLLS	Yes	No	Abstain	% Support
Applicability 4. 2				
Add: 4.2.1 Facilities regulated by the Canadian Nuclear Safety Commission.	**17**	**0**	**-**	**100%**
Add: 4.2.3 Cyber assets associated with Cyber Security Plans submitted to U.S. Nuclear Regulatory Commission pursuant to 10CFR73.54.	**17**	**0**	**-**	**100%**
Effective Date 5. "The first day of the eighth ~~third~~ calendar quarter after applicable regulatory approvals have been received (or the Reliability Standard otherwise becom effective the first day of the ninth ~~third~~ calendar quarter after BOT adoption in those jurisdictions where regulatory approval is not required)"	**17**	**0**	**-**	**100%**
B. REQUIREMENTS-PROPOSED WORDING STRAW POLLS	**Yes**	**No**	**Abstain**	**% Support**
R.1 Critical Asset Identification — The Responsible Entity shall develop a list of its identified Critical Assets determined through an annual application of the criteria contained in *CIP-002-4 Attachment 1 – Critical Asset Criteria*. The Responsible Entity shall update ~~review~~ this list ~~at least annually, and update it~~ as necessary, and review it at least annually.	**17**	**0**	**-**	**100%**
R2. Critical Cyber Asset Identification — Using the list of Critical Assets developed pursuant to Requirement R1, the Responsible Entity shall develop a list of associated Critical Cyber Assets essential to the operation of the Critical Asset. The Responsible Entity shall update this list as necessary, and review it at least annually. For each group of generating units (including nuclear generation) at a single plant location identified in Attachment 1, criterion 1.1, the only Cyber Assets that must be considered are those shared Cyber Assets that could, within 15 minutes, adversely impact the reliable operation of any combination of units that in aggregate equal or exceed Attachment 1, criterion 1.1 ~~within 15 minutes The Responsible Entity shall review this list at least annually, and update it as necessary~~ For the purpose of Standard CIP-002-4, Critical Cyber Assets are further qualified to be those having at least one of the following characteristics: R2.1 The Cyber Asset uses a routable protocol to communicate outside the Electronic Security Perimeter; or, R2.2 The Cyber Asset uses a routable protocol within a control center; or, R2.3 The Cyber Asset is dial-up accessible.	**17**	**0**	**-**	**100%**
R3. Annual Approval — The senior manager or delegate(s) shall approve annually the list of Critical Assets and the list of Critical Cyber Assets. Based on Requirements R1 and R2 the Responsible Entity may determine that it has no Critical Assets or Critical Cyber Assets. The Responsible Entity shall keep a signed and dated record of the senior manager or delegate(s)'s approval of the ~~risk-based assessment methodology~~ list of Critical Assets and the list of Critical Cyber Assets (even if such lists are null.)	**17**	**0**	**-**	**100%**

ATTACHMENT #1-PROPOSED WORDING STRAW POLLS	Yes	No	Abstain	% Support
1.3 *Proposed Wording* Each generation Facility that the Planning Coordinator, Transmission Planner or Reliability Coordinator designates as required to avoid BES	**13**	**4**	**-**	**76%**
Adverse Reliability Impacts in the planning horizon.				
1.4 *Support for Strawman language:* "Each Blackstart Resource identified in the Transmission Operator's restoration plan."	**16**	**0**	**1**	**94%**
1.5 The Facilities comprising the Cranking Paths and meeting the initial switching requirements from the Blackstart Resource to the first interconnection point of the generation unit(s) to be started, or up to the point on the Cranking Path where ~~multiple~~ two or more path options exist, as identified in the Transmission Operator's restoration plan.	**15**	**1**	**-**	**94%**
1.7 *Support for Strawman Language plus addition*: "Transmission Facilities operated at 300 kV or higher at stations or substations interconnected at 300 kV or higher with three or more other transmission stations or substations.	**16**	**0**	**-**	**100%**
1.8 *Proposed Changes:* Transmission Facilities at a single station or substation location that ~~if destroyed, degraded, misused or otherwise rendered unavailable, violate one or more~~ are identified by the Reliability Coordinator, Planning Authority or Transmission Planner as critical to the derivation of Interconnection Reliability Operating Limits (IROLs) and their associated contingencies.	**17**	**0**	**-**	**100%**
1.9 *Proposed Changes:* Flexible AC Transmission Systems (FACTS) at a single station or substation location, that, ~~if destroyed, degraded, misused or otherwise rendered unavailable, violate one or more~~ are identified by the Reliability Coordinator, Planning Authority or Transmission Planner as critical to the derivation of Interconnection Reliability Operating Limits (IROLs) and their associated contingencies.	**16**	**0**	**-**	**100%**
1.10 *Proposed Changes:* Transmission Facilities providing the generation interconnection required to ~~directly~~ interconnect generator output to the transmission system that, if destroyed, degraded, misused, or otherwise rendered unavailable, would result in the loss of the assets identified by the ~~any Responsible Entity~~/Generator Owner as a result of its application of Attachment 1, criterion 1.1 or 1.3.	**15**	**1**	**-**	**94%**
1.12 *Proposed Language:* "Each Special Protection System (SPS), Remedial Action Scheme (RAS) or automated switching system that operates BES Elements that ~~if destroyed, degraded, misused or otherwise rendered unavailable, violate one or more Interconnection Reliability Operating Limits (IROLs)~~ is identified by the Reliability Coordinator, Planning Authority or Transmission Planner as critical to the derivation of Interconnection Reliability Operating Limits (IROLs) and their associated contingencies."	**14**	**0**	**2**	**87%**
1.13 ~~Common control system(s) capable of performing~~ Each system or facility that perform automatic load shedding, without human operator ~~intervention~~ initiation, of 300 MW or more ~~within 15 minutes~~ implementing undervoltage load shedding (UVLS) or underfrequency load shedding (UFLS) as required by the regional load shedding program	**12**	**0**	**5**	**71%**

1.14 *Final Language:* Each control center, ~~control system,~~ or backup control center~~, or backup control system~~ used to perform the functional obligations of the Reliability Coordinator, ~~Balancing Authority, or Transmission Operator.~~	**15**	**2**	**-**	**88%**
1.15 *Final language* "Each control center or backup control center used to control generation at multiple plant locations for any generation Facility or group of generation Facilities identified in 1.1,1.3, and 1.4. Each control center or backup control center used to control generation equal to or exceeding 1500 MWs in a single Interconnection."	**14**	**0**	**-**	**100%**
1.16 *Final draft:* Each control center or backup control center used to perform the functional obligations of the Transmission Operator that includes control of at least one asset identified in criteria 1.2, 1.5, 1.6, 1.7, 1.8, 1.9, 1.10, 1.11 or 1.12.	**17**	**0**	**-**	**100%**
Original 1.16 *Original strawman wording:* ~~Any additional assets that the Responsible Entity deems appropriate to include.~~	**0**	**17**	**-**	
1.17 *Final Draft*: Each control center or backup control center used to perform the functional obligations of the Balancing Authority that includes at least one asset identified in criteria 1.1, 1.3, 1.4, or 1.13. Each control center or backup control center used to perform the functional obligations of the Balancing Authority for generation equal to or greater than an aggregate of 1500 MWs in a single Interconnection.	**17**	**0**	**-**	**100%**
IMPLEMENTATION PLANS- PROPOSED WORDING STRAW POLL	**Yes**	**No**	**Abstain**	**% Support**
Create a 24 month implementation deadline for all CA and CCA assets and reflect this in the standard's effective date (A.5) and in the implementation plan language.	**15**	**2**	**-**	**88%**
OVERALL ADOPTION OF CIP 002-4 RESPONSE DOCUMENT	**Yes**	**No**	**Abstain**	**% Support**
Motion to approve adoption of the CIP 002-4 SDT response document as refined with direction to Howard Gugel to provide any needed Editorial Changes Consistent with the SDT's agreement on the responses.	**17**	**0**	**-**	**100%**
OVERALL ADOPTION OF CIP 002-4 AND RELATED DOCUMENTS AS REFINED	**Yes**	**No**	**Abstain**	**% Support**
Motion to approve overall adoption of CIP 002-4 and related Documents (Implementation Plans & Guidance Document) consistent with the SDT straw polling results.	**15**	**3**	**-**	**83%**

The Team reviewed the steps and assignments leading up to the Orlando meeting which member Rich Kinas will host once again at the OUC facilities. The Framework Sub-Group will be meeting several times in the interim to prepare documents for the SDT to review at the December meeting. The 2nd Ballot is expected to close on Friday, December 10 COB. NERC staff will prepare the ballot results and comments with strawman draft responses and send out as soon as possible following the close of the ballot in advance of the Orlando meeting the following Tuesday. The Orlando meeting agenda will include review and response to the 2nd ballot results and comments, an orientation and training session on the results-based standards process and a review, discussion and consensus testing of a framework for CIP Version 5. The Chair thanked Tom Stevenson and Margaret Powell for the excellent hosting of the SDT in Baltimore.

The meeting adjourned at 4:40 on Thursday

Cyber Security Order 706 SDT- Project 2008-06
28TH MEETING SUMMARY
November 16-18, 2010
Baltimore, Maryland

I. AGENDA REVIEW, WORKPLAN SCHEDULE, INTRODUCTORY REMARKS AND UPDATES

A. Agenda and Milestone Schedule Review

John Lim, Chair of the CSO 706 SDT welcomed members and other participants to Baltimore and thanked Tom Stevenson and Maggie Powell at Constellation Energy for hosting the meeting. Howard Gugel, NERC, conducted a roll call and reviewed the antitrust and public meeting guidelines at the beginning of each day. On Thursday morning, the SDT unanimously adopted the October 12-14, 2010 Ontario meeting summary.

The chair outlined the objectives the SDT sought to accomplish by the end of the meeting and Bob Jones reviewed the timed agenda for each day including starting with any proposed changes to the requirements and Attachment 1 criteria and then proceeding through each of the industry comments and draft responses. The Chair and Vice Chair thanked the members who joined in the daily Readytalk conference calls during the past week to bring strawman responses to industry comments for the SDT review at this meeting.

Phil Huff reviewed the milestone schedule noting that the SDT had agreed to prepare and submit the CIP XX-XX Version 5 to industry by July, 2011. Phil noted that the proposed schedule may be adjusted slightly in the Spring based on SDT progress but will lead to a balloting of the Version 5 proposed CIP standards by mid-year. He also pointed out that currently the Team is not planning to put preliminary drafts out for informal industry comment.

B. Introductory Remarks- Trade Associations

Barry Lawson on behalf of NRECA noted that he supports the efforts of the SDT and hopes they can get to a consensus on some changes based on the industry comments. He noted he abstained from voting but he and NRECA members want to be able to vote in the affirmative on the next ballot. He summarized the association's concerns around control centers for balancing authorities and transmission operators and the bright line MW criteria as well as the Blackstart portions of the criteria. The NRECA hopes that SDT will address the question of whether this draft will "incentivize people to withdraw assets from blackstart plans."

Nathan Mitchell, representing APPA noted that while they voted against the standard, they are not against what the SDT is doing overall. They hope the SDT will take a new look at and address a few

areas of concern regarding control centers and blackstart units. He believed it was possible to pull in public power members with some modifications in these areas.

David Batz, representing EEI, echoed the other trade association comments, noting that EEI appreciated the efforts of the SDT and the complexity of the job. He reinforced EEI members' interest in a successful balloting of CIP 002-4 and suggested there was an opportunity for the SDT to improve the product noting that it won't be perfect.

C. Introductory Remarks by Mark Weatherford, VP/Chief Security Officer, NERC

Mark introduced himself to the Team noting that he was relatively new at NERC and at the drafting process but wanted to see how the Team is functioning. He noted that he understood that CIP security efforts have been evolving rapidly and that Scott Mix has kept him in the loop. He assured the Team that he is a supporter of the process and appreciates that the SDT is working very hard to perform a needed service for the industry.

D. Related Cyber Security Initiative Update- CIP 005-4 Urgent Action

Scott Mix reported on the CIP 005-4 Urgent Action. The CIP 005 drafting team received numerous significant comments on the posted standard. That previous standard and its associated SAR were withdrawn and replaced by updated versions. The language for CIP 005-4 Requirement R6 has been significantly modified based on industry comment, and was approved for an abbreviated posting and ballot period by the Standards Committee. The comment and ballot period closes on 12/1/2010. Also posted was the summary of comments received, and summary of issues raised during the previous posting period. An updated guidance document was also posted. The goal of the team is to still file the revisions for concurrent consideration of a single "Version 4" package by regulators.

SDT Member Comments

- This is not the normal procedure in terms of comment and ballot.
- The Team and NERC are hoping to be able to request FERC to take action on the two filings together. The industry wants only one Version 4.
- Scott Mix has done an excellent job in facing and addressing the many challenges for this urgent action effort.

E. Field Trip to a Constellation Energy Sub-Station

Many of the SDT members and other meeting participants participated in a tour of a Constellation Energy sub-station on site on Wednesday mid-day.

II. REVIEW OF CIP 002-4 PROPOSED CHANGES

A. Overview of the Ballot Results

Howard Gugel reported that there was a 43% approval rating from the industry. He suggested that the way the ballot process is set up leads to a high negative first vote as industry entities want to be able to make comments for the SDT to consider in any redrafting for the next ballot. He offered that the industry ballot results and comments do not represent an insurmountable task for the SDT to respond to

these comments and make appropriate changes in the standard and succeed in a new ballot. He suggested the largest concerns and strongest feelings surrounded the following three areas in the standards and Attachment 1:

- Control Centers;
- Blackstart Resources; and
- 1.3- Transmission planner reliability "must run" units.

He noted that it was very helpful to have worked through and reached agreement of the SDT on responses to the September 29 webinar questions and comments at the Toronto SDT meeting many of which were presented as comments to the ballot. Finally Howard offered his appreciation for the participation of many of the SDT members who set time aside for each day of the preceding week to help prepare strawman responses for consideration at the Baltimore meeting.

B. Review and Consensus Building on Proposed Changes to CIP 002-4 and Related Documents

The SDT reviewed the industry comments and a strawman response document and conducted straw polls for a number of proposed changes to the standard. In general, if the proposal received greater than 2/3 support from the Team it was incorporated into the text of the standard. In calculating the percentage of members in support of a proposal, the abstentions were not included.

The SDT initially focused on Attachment 1 and the implementation plan documents and then returned to the standards document to make any changes consistent with the agreed upon changes in Attachment 1 and the implementation plans. The SDT reviewed strawman responses to each industry comment. At the conclusion of the meeting the SDT reviewed and amended the Guidance Document consistent with the changes in the standards documents.

CYBER SECURITY — CRITICAL CYBER ASSET IDENTIFICATION CIP-002-4 SDT STRAW POLLS

A. INTRODUCTION-PROPOSED WORDING STRAW POLLS	Yes	No	Abstain	% Support
Applicability 4. 2				
Add: 4.2.1 Facilities regulated by the Canadian Nuclear Safety Commission.	**17**	**0**	**-**	**100%**
Add: 4.2.3 Cyber assets associated with Cyber Security Plans submitted to U.S. Nuclear Regulatory Commission pursuant to 10CFR73.54.	**17**	**0**	**-**	**100%**
Effective Date 5. "The first day of the eighth ~~third~~ calendar quarter after applicable regulatory approvals have been received (or the Reliability Standard otherwise become effective the first day of the ninth ~~third~~ calendar quarter after BOT adoption in those jurisdictions where regulatory approval is not required)"	**17**	**0**	**-**	**100%**

B. REQUIREMENTS-PROPOSED WORDING STRAW POLLS	Yes	No	Abstain	% Support
R.1 Critical Asset Identification — The Responsible Entity shall develop a list of its identified Critical Assets determined through an annual application of the criteria contained in *CIP-002-4 Attachment 1 – Critical Asset Criteria*. The Responsible Entity shall update ~~review~~ this list ~~at least annually, and update it~~ as necessary, and review it at least annually.	**17**	**0**	**-**	**100%**
R2. Critical Cyber Asset Identification — Using the list of Critical Assets developed pursuant to Requirement R1, the Responsible Entity shall develop a list of associated Critical Cyber Assets essential to the operation of the Critical Asset. The Responsible Entity shall update this list as necessary, and review it at least annually. For each group of generating units (including nuclear generation) at a single plant location identified in Attachment 1, criterion 1.1, the only Cyber Assets that must be considered are those shared Cyber Assets that could, within 15 minutes, adversely impact the reliable operation of any combination of units that in aggregate equal or exceed Attachment 1, criterion 1.1 ~~within 15 minutes~~ ~~The Responsible Entity shall review this list at least annually, and update it as necessary~~ For the purpose of Standard CIP-002-4, Critical Cyber Assets are further qualified to be those having at least one of the following characteristics: R2.1 The Cyber Asset uses a routable protocol to communicate outside the Electronic Security Perimeter; or, R2.2 The Cyber Asset uses a routable protocol within a control center; or, R2.3 The Cyber Asset is dial-up accessible.	**17**	**0**	**-**	**100%**
R3. Annual Approval — The senior manager or delegate(s) shall approve annually the list of Critical Assets and the list of Critical Cyber Assets. Based on Requirements R1 and R2 the Responsible Entity may determine that it has no Critical Assets or Critical Cyber Assets. The Responsible Entity shall keep a signed and dated record of the senior manager or delegate(s)'s approval of the ~~risk-based assessment methodology~~ list of Critical Assets and the list of Critical Cyber Assets (even if such lists are null.)	**17**	**0**	**-**	**100%**

ATTACHMENT #1- PROPOSED WORDING STRAW POLLS	Yes	No	Abstain	% Support
1.3 *Proposed Wording* Each generation Facility that the Planning Coordinator, Transmission Planner or Reliability Coordinator designates as required to avoi Adverse Reliability Impacts in the planning horizon.	**13**	**4**	**-**	**76%**

1.3 *Add* "Reliability Coordinator designate"	0	17	-	
1.3 *Add* "Reliability Coordinator communicated as necessary"	0	17	-	
1.4 *Support for Strawman language:* "Each Blackstart Resource identified in the Transmission Operator's restoration plan."	**16**	**0**	**1**	**94%**
1.4 *Add* "Each generator identified as a Blackstart Unit in the Transmission Operator's restoration plan."	12	6	-	
1.4 *Add,* "Each generator identified as Blackstart resource"-	7	11	-	
1.4 *Add,* "If more than a single generator is identified, only the first three fall under this."	0	16	-	
1.5 The Facilities comprising the Cranking Paths and meeting the initial switching requirements from the Blackstart Resource to the first interconnection point of the generation unit(s) to be started, or up to the point on the Cranking Path where ~~multiple~~ two or more path options exist, as identified in the Transmission Operator's restoration plan.	**15**	**1**	**-**	**94%**
1.5 *Add,* "meeting the"	15	1	-	
1.5 *Add* "first interconnection point of the generation"	12	6	-	
1.5 *Delete* "~~multiple~~", *Add* "two or more"	15	1	-	
1.5 *Delete*- "~~to the point on the Cranking Path where multiple two or more path options exist .~~"	1	15	-	
1.7 *Support for Strawman Language plus addition*: "Transmission Facilities operated at 300 kV or higher at stations or substations interconnected at 300 kV or higher with three or more other transmission stations or substations.	**16**	**0**	**-**	**100%**
1.8 *Proposed Changes:* Transmission Facilities at a single station or substation location that ~~if destroyed, degraded, misused or otherwise rendered unavailable, violate one or more~~ are identified by the Reliability Coordinator, Planning Authority or Transmission Planner as critical to the derivation of Interconnection Reliability Operating Limits (IROLs) and their associated contingencies.	**17**	**0**	**-**	**100%**
1.9 *Proposed Changes:* Flexible AC Transmission Systems (FACTS) at a single station or substation location, that, ~~if destroyed, degraded, misused or otherwise rendered unavailable, violate one or more~~ are identified by the Reliability Coordinator, Planning Authority or Transmission Planner as critical to the derivation of Interconnection Reliability Operating Limits (IROLs) and their associated contingencies.	**16**	**0**	**-**	**100%**
1.10 *Proposed Changes:* Transmission Facilities providing the generation interconnection required to ~~directly~~ interconnect generator output to the transmission system that, if destroyed, degraded, misused, or otherwise rendered unavailable, would result in the loss of the assets identified by the ~~any Responsible Entity~~/Generator Owner as a result of its application of Attachment 1, criterion 1.1 or 1.3.	**15**	**1**	**-**	**94%**
1.12 *Strawman Language:* Each Special Protection System (SPS), Remedial Action Scheme (RAS) or automated switching system that operates BES Elements that, if destroyed, degraded, misused or otherwise rendered unavailable, violate one or more Interconnection Reliability Operating Limits (IROLs).	0	16		

1.12 *Proposed Language:* "Each Special Protection System (SPS), Remedial Action Scheme (RAS) or automated switching system that operates BES Elements that ~~if destroyed, degraded, misused or otherwise rendered unavailable, violate one or more Interconnection Reliability Operating Limits (IROLs)~~ is identified by the Reliability Coordinator, Planning Authority or Transmission Planner as critical to the derivation of Interconnection Reliability Operating Limits (IROLs) and their associated contingencies."	**14**	**0**	**2**	**87%**
1.13 Common control system(s) capable of performing automatic load shedding, without human operator intervention, of 300 MW or more within 15 minutes.	12	3	0	
1.13 ~~Common control system(s) capable of performing~~ Each system or facility that perform automatic load shedding, without human operator ~~intervention~~ initiation, of 300 MW or more ~~within 15 minutes~~ implementing undervoltage load shedding (UVLS) or underfrequency load shedding (UFLS) as required by the regional load shedding program	**12**	**0**	**5**	**71%**
1.13 Support for 300 MW	6	-	-	
1.13 Support for 1500 MW	10	-	-	
1.13 Support for more than 1500 MW	2	-	-	
1.14 *Final Language:* Each control center, ~~control system,~~ or backup control center~~, or backup control system~~ used to perform the functional obligations of the Reliability Coordinator, ~~Balancing Authority, or Transmission Operator.~~	**15**	**2**	**-**	**88%**
1.15 Final "Each control center or backup control center used to control generation at multiple plant locations for any generation Facility or group of generation Facilities identified in 1.1,1.3, and 1.4. Each control center or backup control center used to control generation equal to or exceeding 1500 MWs in a single Interconnection."	**14**	**0**	**-**	**100%**
1st Proposed Edit of Strawman: Each control center or backup control center used to ~~control~~ change generation output at multiple plant locations for any generation Facility or group of Facilities identified as a Critical Asset, or ~~used to control generation greater than an~~ aggregate generation ~~of~~ greater than 1500 MWs in a single Interconnection.	**12**	**2**	**-**	
2nd Proposed Edit of Strawman: "Each control center or backup control center used to control generation output at multiple plant, locations for any generation Facility or group of Facilities identified in 1.1.1.3. and 1.4 Each control center or backup control center used to control aggregate generation ~~greater than an aggregate~~ equal to or exceeding 1500 MWs in a single Interconnection."	**13**	**1**	**-**	
1.16 *Final draft:* Each control center or backup control center used to perform the functional obligations of the Transmission Operator that includes control of at least one asset identified in criteria 1.2, 1.5, 1.6, 1.7, 1.8, 1.9, 1.10, 1.11 or 1.12.	**17**	**0**	**-**	**100%**
Original 1.16 *Original strawman wording:* ~~Any additional assets that the Responsible Entity deems appropriate to include.~~	**0**	**17**	**-**	
Original 1.16 *Alternative wording:* ~~Any additional assets owned by the Responsible Entity that the Responsible Entity deems appropriate to include.~~	**0**	**17**	**-**	

1.17 *Final Draft*: Each control center or backup control center used to perform the functional obligations of the Balancing Authority that includes at least one asset identified in criteria 1.1, 1.3, 1.4, or 1.13. Each control center or backup control center used to perform the functional obligations of the Balancing Authority for generation equal to or greater than an aggregate of 1500 MWs in a single Interconnection.	**17**	**0**	**-**	**100%**
1.17 *Alternative wording***.** Each control center or backup control used to perform the functional obligations of the Balancing Authority that includes at least one asset identified in criteria 1.1, 1.2, 1.3, 1.4, 1.14, for a generation greater than aggregate of 1500 MW in a single interconnection~~/in a single region/remove~~.	**11**	**4**	**-**	
(114 b "in a single interconnection")	**11**	**4**	**-**	
(114 b "in a single region")	**10**	**1**	**4**	

The SDT spent nearly two days reviewing the industry comments related to Attachment 1, a strawman Attachment 1 document for changes to the standards, and draft responses to the industry. They tested the level of support for existing, proposed and alternative wording. *(See, Appendix #5 for a summary of the Attachment 1 issues reviewed)*

IMPLEMENTATION PLANS- PROPOSED WORDING STRAW POLL	**Yes**	**No**	**Abstain**	**% Support**
Create a 24 month implementation deadline for all CA and CCA assets and reflect this in the standard's effective date (A.5) and in the implementation plan language.	**15**	**2**	**-**	**88%**

Implementation Plan Discussion Issues

The SDT reviewed the industry comments on the Implementation Plan and the Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities. The SDT and participant discussion covered the following issues: apparent confusion over the complications for the proposed exceptions in the timing for implementation of IPFNICCANRE vs. a 24-month period for all entities without exceptions; affording time for budgeting for CIP 002-4 implementation; minimizing the need to take TFEs along with mitigation plans; balance the exceptions process with a simple, less confusing approach that has the optic of not getting the lists for 2 years; is it best to get an early report card regarding fewer or greater number of assets; and take CIP 002-4 into account when developing Version 5 (CIP 010….).

OVERALL ADOPTION OF CIP 002-4 RESPONSE DOCUMENT	**Yes**	**No**	**Abstain**	**% Support**
Motion to approve adoption of the CIP 002-4 SDT response document as refined with direction to Howard Gugel to provide any needed Editorial Changes Consistent with the SDT's agreement on the responses.	**17**	**0**	**-**	**100%**

OVERALL ADOPTION OF CIP 002-4 AND RELATED DOCUMENTS AS REFINED	Yes	No	Abstain	% Support
Motion to approve overall adoption of CIP 002-4 and related Documents (Implementation Plans & Guidance Document) consistent with the SDT straw polling results.	**15**	**3**	**-**	**83%**

The 3 SDT members voting no (*Jim Brenton, Dave Norton and Rich Kinas*) agreed on the following rationale statement explaining their votes:

- The 15 min criteria for real time is vague and should not apply to cyber assets:
- Attachment 1.1 The 1500 MW criteria for Generation is too high. ISO/RTOs recommended 300 MW for Generators. This criteria will miss too many generators and a lot of NUKES
- Attachment 1.5 We must include all blackstart restoration paths, not just primary path to the first sub with two transmission paths
- Attachment 1.13 Remove "without human intervention." This item originally addressed Load Serving Entities, not automatic load shedding. The revisions since last posting significantly change intent of this control.
- Attachment 1.15-1.17. All RC/BA/TOP/GOPs should be Critical Assets
- ISO/RTO position- We are not sure that many of the ISOs/RTOs will support this version as we have regressed in the level of cyber security included in CIP Version 4 when compared to that of CIP Version 3.
- NERC will be hard pressed to show these standards will improve security for the BES."

III. NEXT STEPS AND ASSIGNMENTS

The Team reviewed the steps and assignments leading up to the Orlando meeting which member Rich Kinas will host once again at the OUC facilities. The Framework Sub-Group will be meeting several times in the interim to prepare documents for the SDT to review at the December meeting. The 2nd Ballot is expected to close on Friday, December 10 COB. NERC staff will prepare the ballot results and comments with strawman draft responses and send out as soon as possible following the close of the ballot in advance of the Orlando meeting the following Tuesday.

The Chair thanked Tom Stevenson and Margaret Powell for the excellent hosting of the SDT in Baltimore.

The meeting adjourned at 4:40 on Thursday

Appendix # 1— Meeting Agenda
Project 2008-06 Cyber Security Order 706 SDT
Draft 28th Meeting Agenda
November 16, 2010, Tuesday- 8:00 AM to 6:00 PM CDT
November 17, 2010 Wednesday- 8:00 AM to 6:00 PM CDT
November 18, 2010 Thursday- 8:00 AM to 6:00 PM CDT
Baltimore, Maryland

NOTE: 1. Agenda Times May be Adjusted as Needed during the Meeting
NOTE: 2. Drafting Sub-team Meetings May Not Have Access to Telephones and Ready Talk

Proposed Meeting Objectives/Outcomes:

- To review and test consensus on responses to industry comments on CIP 002-4 and on any changes for inclusion in the 2nd ballot.
- To review progress of the CIP Framework Team
- To agree on next steps and assignments

Tuesday, November 16, 2010 8:00 a.m. - 6:00 p.m.

- Introductions, welcome -*(Morning)*
- Introductory Remarks by Mark Weatherford, VP/Chief Security Officer, NERC
- Introductory Remarks by Trade Organizations – Allen Mosher, APPA, Barry Lawson, NRECA, and David Batz, EEI
- Receive updates on other related cyber security initiatives- *NERC Staff and SDT Members (Morning)*
- Review meeting and milestone schedule for CIP 002-4 and CIP 010 and 011 *(Morning)*
- Review and Test Consensus on the Draft CIP 002-4 Response Document *(Morning and Afternoon)*

Wednesday, November 17, 2010 8:00 a.m. - 6:00 p.m.

- Continue Review and Consensus Testing on the Draft CIP 002-4 Response Document *(Morning)*
- *Local Sub-Station Tour (Mid-day)*
- Review and Test Consensus on possible CIP 002-4 Changes *(Afternoon)*

Thursday, November 18, 2010, 8:00 a.m. - 6:00 p.m.

- Review and Test Consensus on possible CIP 002-4 Changes *(Morning)*
- Adopt CIP-002-4 for 2nd Ballot and SDT Industry Response Document (*Afternoon)*
- Review progress on Framework Team (*Afternoon)*
- Review SDT December, 2010 Orlando Meeting Agenda (*Afternoon)*

Appendix # 2 Attendees List
November 16-18, 2010 Baltimore

Attending in Person — SDT Members and Staff

1. Rob Antonishen	Ontario Power Generation
2. Jim Brenton	ERCOT
3. Jay S. Cribb	Southern Company Services
4. Joe Doetzl	Kansas City Pwr. & Light Co
5.Sharon Edwards	Duke Energy
6.Gerald S. Freese	America Electric Pwr.
7. Jeff Hoffman	U.S. Bureau of Reclamation, Denver
8. Phillip Huff, Vice Chair	Arkansas Electric Coop Corporation (W/Th)
9. Doug Johnson	Exelon Corporation – Commonwealth Edison
10.Rich Kinas	Orlando Utilities Commission (Tu/W)
11. John Lim, Chair	Consolidated Edison Co. NY
12. David S. Revill	Georgia Transmission Corporation
13. Kevin Sherlin	Sacramento Municipal Utility District (Tu/W)
14. Tom Stevenson	Constellation
15. Keith Stouffer	National Institute of Standards & Technology
16. John D. Varnell	Technology Director, Tenaska Power Services Co. (W/Th)
17. William Winters	Arizona Public Service, Inc.

SDT Members Attending via ReadyTalk and Phone

18. Jackie Collett	Manitoba Hydro
19. David Norton	Entergy
20. Scott Rosenberger	Luminant Energy
21. John Van Boxtel	WECC (Tu)
Scott Mix	*NERC*
Howard Gugel	*NERC*
Roger Lampila	*NERC*
Mallory Higgins	*NERC (W)*
Brian Harrell	*NERC (Tu)*
Laura Hussey	*NERC (W)*
Mark Weatherford	*NERC (Tu)*
Robert Jones	*FSU/FCRC Consensus Center*
Stuart Langton	*FSU/FCRC Consensus Center*

SDT Members Not Participating

William Gross	Nuclear Energy Institute
Patricio Leon	Southern California Edison
Jonathan Stanford	Bonneville Power Administration
Bradley Yeates	South Nuclear Operating Company

Others Attending in Person

Jan Bargen	FERC
John Bussman	AECI
Robert Preston Lloyd	Southern California Edison
Carey W. Flemming	Constellation Energy Nuclear Group (W)
Jim Fletcher	American Electric Power
CJ Ingersoll	Constellation Energy (Tu/W)
Barry Lawson	NRECA (Tu)
Andres Lopez	USACE
Nathan Mitchell	APPA (Tu)
Brian Newell	American Electric Power
Margaret Powell	Constellation Energy
Stan Rae	Constellation Energy (Tu)
Ingrid Rayo	Constellation Energy
Mike Rossman	Constellation Energy
Kevin Ryan	FERC (Tu/W)
Mark Simon	Encari

Others Attending via Readytalk and Phone

November 16, 2010, Tuesday

Chris	Ewing	chris_ewing@selinc.com
David	Batz	dbatz@eei.org
Drew	Kittey	Drew.Kittey@ferc.gov
Larry	Camm	larry_camm@selgs.com
Bryn	Wilson	wilsonwb@oge.com
Rod	Hardiman	rchardim@southernco.com
David	Gordon	dgordon@mmwec.org

November 17, 2010, Wednesday

Chris	Ewing	chris_ewing@selinc.com
Rod	Hardiman	rchardim@southernco.com
Barry	Lawson	barry.lawson@nreca.coop
Bryn	Wilson	wilsonwb@oge.com
Drew	Kittey	Drew.Kittey@ferc.gov
Anna	Wang	amwang@burnsmcd.com

November 18, 2010, Thursday

Drew	Kittey	Drew.Kittey@ferc.gov
Chris	Ewing	chris_ewing@selinc.com
Bryn	Wilson	wilsonwb@oge.com
Todd	Williams	trwilliams@midamerican.com
Barry	Lawson	barry.lawson@nreca.coop
Rod	Hardiman	rchardim@southernco.com

Appendix #3 NERC Antitrust Compliance Guidelines

See Antitrust Compliance Guidelines read at the beginning of each day's session at:

The NERC reminder below was read at the beginning of each day's session.

NERC REMINDER FOR USE AT BEGINNING OF MEETINGS AND CONFERENCE CALLS THAT HAVE BEEN PUBLICLY NOTICED AND ARE OPEN TO THE PUBLIC

For face-to-face meeting, with dial-in capability:

Participants are reminded that this meeting is public. Notice of the meeting was posted on the NERC website and widely distributed. The notice included the number for dial-in participation. Participants should keep in mind that the audience may include members of the press and representatives of various governmental authorities, in addition to the expected participation by industry stakeholders.

Appendix #4

Final SDT CIP 002-4 Documents for Posting

http://www.nerc.com/filez/standards/Project_2008-06_Cyber_Security_PhaseII_Standards.html

Appendix #5
Attachment 1 Summary of Issues Discussed by the SDT

During the course of the three-day meeting there were extended discussions and proposals for revision of Attachment 1 criteria to address industry comments that covered the following issues:

- 1.3 The SDT discussion and review of industry comments covered the following issues: clarifying the meaning of "adverse reliability impacts" and "planning horizon", forced retirement issues, explain long term planning in guidance document and including or excluding reliability coordinator.
- 1.4 Blackstart Resource**.** The SDT discussion and review of industry comments covered the following issues:: considering whether to include "each generation facility", the reference to EOP 5 restoration plans and distinguishing them from cyber issues, providing incentives to keep Blackstart resources in the transmission plan, considering a bright line limitor, and clarifying this criteria in the guidance document.
- 1.5 The SDT discussion and review of industry comments covered the following issues: delineating between generator and transmission responsibilities and clarify what "up to the unit being started" includes.
- 1.7 The SDT discussion and review of industry comments covered the following issues: criticality vs. reliability in protecting against distributed attacks, 500 KVand above as backbone of the BES,
- 1.8 The SDT discussion and review of industry comments covered the following issues: reference to FAC 014-2, the relationship between 1.7 and 1.8., and planning vs. operational IROLs.
- 1.9 The SDT discussion and review of industry comments covered the following issues: make clear that FACTs devices are included in standard.
- 1.10 The SDT discussion and review of industry comments covered the following issues: "directly" was intended to scope down this criteria but may add confusion, consider whether the generator interface may change in the near future, and focus on generator owners vs. responsible entity.
- 1.12 The SDT discussion and review of industry comments covered the following issues: is "operates" or "identified" the right action here, is it a failure to operate as designed, clarify who is testing and maintaining the SPS and the RAS, generator run back schemes focused internally on the generation system not externally on the BES. Blanket statements about these might not be appropriate.
- 1.13 The SDT discussion and review of industry comments covered the following issues: automatic load shed has been an ongoing SDT discussion; target was auto load shedding system for version 1; "capable of" vs. "configured to" vs. "limiting to underfrequency/underload"; "initiation" vs. "intervention;" reference to regional load shedding programs; consider the smart grid issues coming down the road; considering advanced persistent threats that can get into control systems and load malicious software

1500 MW would be too high; in some shops distribution SKADA system in different system than transmission system; should regional diversity be addressed; consider PRC 6.1 for planning coordinators, and PRC 007-0 & PRC 20-1; reference "under-frequency load shedding and under voltage load shedding systems; consider retaining 300 MW with caveat that this will be revisited in Version 5. *On Wednesday SDT 2nd review of redraft:* reference to human operator may confuse manual and automatic load shed; concern is with this function not being available when needed.

- 1.14 The SDT discussion and review of industry comments covered the following issues: definition and differences between control system lead to removing control system; what should the bright line be, 1500, 2000 or other; with cyber vulnerability threats to smaller entities (i.e. jumping point or gateway to other areas, size may not be the key factor; address all control centers in Version 5; CSO 706- paragraph 280 addresses control centers; bright line for BA and TOP needed now.
- *1.14- 1.17 New Wording*
- 1.14 New: *On Wednesday SDT 2nd review of redraft:* Break out the different actors and their responsibilities; reference asset(s) identified in previous applicable criteria for each actor (TO, BA, RC); cover reliability coordinator in this criteria.
- 1.15 New. The SDT 2nd review on Wednesday of this criteria and discussion of industry comments covered the following issues: this is consistent with CSO 706 paragraph 280; single region vs. single interconnection; interconnection deals with reliability and regions may change overtime; consider this as interim change before Version 5 addresses the appropriate level of controls needed; in an open standards process, if we can't validate information we can't use it;
- 1.6 the unknown level of threat is what we are protecting against and TOPs have a broader breadth of control compared to other systems;; is verbal communication the same as electronic control; careful not to bring in market groups.
- 1.16 New The SDT 2nd review on Wednesday of this criteria and discussion of industry comments covered the following issues:
- Original 1.16 The SDT discussion and review of industry comments covered the following issues: ("Any additional assets owned by the Responsible Entity that the Responsible Entity deems appropriate to include.") Delete this criteria as there is no SDT support for retaining this criteria due to compliance and enforcement and other issues.

Appendix #5 SDT Sub-Teams

Sub-Team	
CIP 010 BES System Categorization	John Lim (Lead), Rich Kinas, Jim Brenton, Dave Norton *(Observer Participants: Rod Hardiman, Jim Fletcher) (FERC: Mike Keane, Peter Kuebeck)*
Personnel and Physical Security	Doug Johnson (Lead), Rob Antonishen, Patrick Leon, Kevin Sherlin *(FERC: Drew Kittey)*
System Security and Boundary Protection	Jay Cribb (Lead), Jackie Collett, John Varnell, John Van Boxtel, Philip Huff *(Observer Participant: Brian Newell) (FERC: Justin Kelly)*
Incident Response and Recovery	Scott Rosenberger (Lead), Joe Doetzl, Tom Stevenson (*Observer Participant: Jason Marshall) (FERC: Dan Bogle)*
Access Control	Sharon Edwards (Lead), Jeff Hoffman, Jerry Freese, Bill Winters *(Observer Participants: Roger Fradenburgh, Robert Preston Lloyd) (FERC: Mike Keane)*
Change Management, System Lifecycle, Information Protection, Maintenance, and Governance	Dave Revill (Lead), Jon Stanford, Keith Stouffer, Bill Winters *(Observer Participant: Brian Newell) (FERC: Jan Bargen, Matthew Dale)*
CIP 002-4 Drafting Team	John Lim (Lead), Jim Brenton, Jackie Collett, Jay Cribb, Sharon Edwards, Doug Johnson, Rich Kinas, Dave Norton, Dave Revill, and Bill Winters *(Observer Participants: Rod Hardiman; Jim Fletcher; Bryn Wilson) (FERC: Mike Keane, Peter Kuebeck; NERC: Scott Mix)*
Implementation Plan CIP 002-4	Dave Revill (Lead), Sharon Edwards, Kevin Sherlin, Scott Rosenberg, Dave Norton and Phil Huff *(FERC: Mike Keane; NERC: Scott Mix)*
Framework CIP 010 &011	Dave Norton (Lead), Jim Brenton, Jay Cribb, Joe Doetzl, Phil Huff, Doug Johnson, Dave Revill, Jon Stanford, and John Van Boxtel. *(FERC: Mike Keane; NERC: Scott Mix)*

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Agenda
Cyber Security Order 706 SDT - Project 2008-06

November 16, 2010 | 8:00 AM to 6:00 PM CDT
November 17, 2010 | 8:00 AM to 6:00 PM CDT
November 18, 2010 | 8:00 AM to 6:00 PM CDT

Baltimore, Maryland

Proposed Meeting Objectives/Outcomes:

- To review and test consensus on responses to industry comments on CIP 002-4 and on any changes for inclusion in the 2nd ballot.
- To review progress of the CIP Framework Team
- To agree on next steps and assignments

Tuesday, November 16, 2010 8:00 a.m. - 6:00 p.m.

- Introductions, welcome -*(Morning)*
- Introductory Remarks by Mark Weatherford, VP/Chief Security Officer, NERC
- Introductory Remarks by Trade Organizations – Allen Mosher, APPA, Barry Lawson, NRECA, and David Batz, EEI
- Receive updates on other related cyber security initiatives- *NERC Staff and SDT Members (Morning)*
- Review meeting and milestone schedule for CIP 002-4 and CIP 010 and 011 *(Morning)*
- Review and Test Consensus on the Draft CIP 002-4 Response Document *(Morning and Afternoon)*

Wednesday, November 17, 2010 8:00 a.m. - 6:00 p.m.

- Continue Review and Consensus Testing on the Draft CIP 002-4 Response Document *(Morning)*
- *Local Sub-Station Tour (Mid-day)*
- Review and Test Consensus on possible CIP 002-4 Changes *(Afternoon)*

Thursday, November 18, 2010, 8:00 a.m. - 6:00 p.m.

- Review and Test Consensus on possible CIP 002-4 Changes *(Morning)*
- Adopt CIP-002-4 for 2nd Ballot and SDT Industry Response Document (*Afternoon)*
- Review progress on Framework Team (*Afternoon)*
- Review SDT December, 2010 Orlando Meeting Agenda (*Afternoon)*

116-390 Village Blvd.
Princeton, NJ 08540
609.452.8060 | www.nerc.com

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Agenda
Cyber Security Order 706 SDT - Project 2008-06

December 14, 2010 | 8:00 AM to 6:00 PM EST
December 15, 2010 | 8:00 AM to 6:00 PM EST
December 16, 2010 | 8:00 AM to 6:00 PM EST

Orlando Utilities Commission Offices
6113 Pershing Avenue
Orlando FL

Proposed Meeting Objectives/Outcomes:

- To review the results of the 2nd Ballot and test consensus on responses to industry comments on CIP 002-4 and, if needed, on any changes for inclusion in a CIP 002-4 3rd ballot.
- To review, refine and test support for recommendations of the CIP Version 5 Framework Team.
- To participate in a Results Based Standards Development Training
- To agree on next steps and assignments

Tuesday, December 14, 2010 8:00 a.m. - 6:00 p.m. EST

- Introduction, welcome -*(Morning)*
- Review meeting and milestone schedule for CIP 002-4 and CIP 010 and 011 *(Morning)*
- Review results of 2nd Ballot CIP-002-4*(Morning)*
- Draft responses to industry and consider any changes to CIP-002-4 *(Morning & Afternoon)*

Wednesday, December 15, 2010 8:00 a.m. - 6:00 p.m. EST

- Seek Motion to Adopt SDT Responses to Industry, and if needed, any changes for inclusion in the 3rd Ballot. *(Morning)*
- Overview of Results Based Standards Development and CIP Version 5- Howard Gugel NERC *(Morning)*
- Receive a Version 5 Framework report *(Morning)*
- Review Draft Strawman Documents and discuss key issues *(Afternoon)*
- Review and initial testing of the acceptability of the approach as refined *(Afternoon)*

Thursday, December 16, 2010, 8:00 a.m. - 6:00 p.m. EST

- Results Based Standards Training- Keith Heidrich, FRCC & Howard Gugel, NERC *(Morning & Afternoon)*
- Review Version 5 Framework in light of Results Based Approach

- Test SDT Support for the Version 5 Framework *(Afternoon)*
- Review Work plan for the Version 5 Framework *(Afternoon)*
- Review SDT January, 2011 Columbus Meeting Agenda (*Late Afternoon)*

Draft Timed Agenda

Tuesday	**December 14, 2010**	**8:00 a.m. - 6:00 p.m. EST**

8:00 a.m.	**Introduction, Welcome Opening and Host remarks**- *John Lim, Chair & Phil Huff, Vice Chair, Rich Kinas, Orlando Utilities Commission Host* Roll Call; NERC Antitrust Compliance Guidelines- *Howard Gugel*
8:15	**Review of meeting objectives, agenda and meeting guidelines**- *John Lim & Bob Jones*
8:20	**Review of CSO 706 SDT CIP milestone schedule for CIP 002-4 and CIP 010 & 011**: *Phil Huff & Stu Langton*
8:30	**NERC Presentation on CIP**- *Gerry Cauley*
9:00	**Overview of CIP 002-4 Industry Response & 2nd Ballot Results**- *Howard Gugel, NERC*
9:45	*Break*
10:00	**Review and Test Consensus on the Draft CIP 002-4 Response Document**
12:00	*Lunch*
1:00	***Continue,* Review and Test Consensus on the Draft CIP 002-4 Response Document**
3:00	*Break*
3:15	**Review any Drafting Team Work and Test Consensus on possible CIP 002-4 Changes**
5:50	**Review any drafting assignments and Wednesday's agenda**
6:00	*Recess*

Wednesday	**December 15, 2010**	**8:00 a.m. - 6:00 p.m. EST**

8:00	**Welcome and Agenda Review, Roll Call and Antitrust Guidelines**- *John Lim, Phil Huff, Howard Gugel* Facilitator review and SDT acceptance of November, 2010 Baltimore SDT meeting summary.
8:15	**Seek Motion to Adopt SDT Changes to CIP 002-4 and Responses to Industry, and if needed**, any changes for inclusion in the 3rd Ballot.
10:00	*Break*
10:15	Overview of Results Based Standards Development and CIP Version 5- Howard Gugel NERC *(Morning)*
12:00	Lunch
1:00	**Version 5 Framework Team report** Review Draft Strawman Documents and discuss key issues
3:30	*Break*
3:45	Review and initial testing of the acceptability of the approach as refined
5:50	**Review any drafting assignments and Thursday's agenda**
6:00	*Recess*

Thursday	**December 16, 2010**	**8:00 a.m. - 6:00 p.m. EST**
8:00	**Welcome and Agenda Review, Roll Call and Antitrust Guidelines**- *John Lim, Phil Huff, Howard Gugel*	
8:15	**Results Based Standards Training-** Keith Heidrich, FRCC & Howard Gugel, NERC	
10:15	*Break*	
10: 30	**Results Based Standards Training** *(Cont'd)*	
12;00	*Lunch*	
1:00	**Results Based Standards Training** *(Cont'd)*	
2:30	*Break*	
2:45	**Review Version 5 Framework in light of Results Based Approach**	
3:15	**Test SDT Support for the Version 5 Framework**	
4:45	**Review Work plan for the Version 5 Framework**	
5:45	**Review SDT January, 2011 Columbus Meeting Agenda**	
6:00	*Adjourn*	

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Cyber Security Order 706 Standard Drafting Team (Project 2008-06)

1. **Chairman**	John Lim, CISSP Department Manager, IT Infrastructure Planning	Consolidated Edison Co. of New York 4 Irving Place Rm 349-S New York, New York 10003	(212) 460-2712 (212) 387-2100 Fx limj@coned.com
2. **Vice Chairman**	Philip Huff Manager, IT Security and Compliance	Arkansas Electric Cooperative Corporation 1 Cooperative Way Little Rock, Arkansas 72119	(501) 570-2444 phuff@aecc.com
3. **Members**	Robert Antonishen Protection and Control Manager, Hydro Engineering Division	Ontario Power Generation Inc. 14000 Niagara Parkway Niagara-on the-Lake, Ontario L0S 1J0	(905) 262-2674 (905) 262-2686 Fx rob.antonishen@opg.com
4.	Jim Brenton, CISSP-ISSAP Director, CIP Standards Development	Electric Reliability Council of Texas, Inc. 2705 West Lake Drive Taylor, Texas 76574	(512) 248-3043 (512) 248-3993 Fx jbrenton@ercot.com
5.	Jackie Collett Cyber Security Operations Engineer	Manitoba Hydro 1565 Willson Place P.O. Box 815 Winnipeg, Manitoba R3C 2P4	(204) 477-7709 jcollett@hydro.mb.ca
6.	Jay S. Cribb Information Security Analyst, Principal	Southern Company Services, Inc. 241 Ralph McGill Boulevard N.E. Bin 10034 Atlanta, Georgia 30308	(404) 506-3854 jscribb@southernco.com
7.	Joe Doetzl Manager, Information Security	Kansas City Power & Light Co. 1201 Walnut Kansas City, Missouri 64106	(816) 556-2280 joe.doetzl@kcpl.com
8.	Sharon Edwards Project Manager	Duke Energy 139 E. 4th Streets 4th & Main Cincinnati, Ohio 45202	(513) 508-1285 -cell (513) 287-1564 sharon.edwards@duke-energy.com
9.	Gerald S. Freese Director, Enterprise Information Security	American Electric Power 1 Riverside Plaza Columbus, Ohio 43215	(614) 716-2351 (614) 716-1144 Fx gsfreese@aep.com
10.	William Gross	Nuclear Energy Institute	(202) 739-8123 wrg@nei.org
11.	Jeffrey Hoffman Chief Architect IT Policy & Security Division	U.S. Bureau of Reclamation Denver Federal Center Bldg. 67, Rm. 380 PO Box 25007 (84-21200) Denver, CO 80225	(303) 445-3341 (303) 445-6307 Fx JHoffman@usbr.gov

12.	Doug Johnson Operations Support Group Transmission Operations & Planning	Exelon - Commonwealth Edison 1N301 Swift Road Lombard, IL 60148	(630) 691-4593 douglas.johnson@ comed.com
13.	Patricio Leon-Alvarado Engineer, E&TS Compliance and Quality	Southern California Edison One Innovation Way Pomona, CA 91768	(909) 274-1697 (909) 274-1692 Fx Patricio.leon-alvarado@sce.com
14.	Richard Kinas Manager of Standards Compliance	Orlando Utilities Commission 6113 Pershing Avenue Orlando, Florida 32822	(407) 384-4063 rkinas@ouc.com
15.	David L. Norton Policy Consultant - CIP	Entergy Corporation 639 Loyola Avenue MS: L-MOB-17A New Orleans, Louisiana 70113	(504) 576-5469 (504) 576-5123 Fx dnorto1@ entergy.com
16.	David S Revill Group Lead, Electronic Maintenance	Georgia Transmission Corporation 2100 East Exchange Place Tucker, Georgia 30084	(770) 270-7815 david.revill@ gatrans.com
17.	Scott Rosenberger Director, Security and Compliance	Luminant 1601 Bryan Street 46th Floor Dallas, TX 75201	(214) 812-2412 scott.rosenberger@ energyfutureholdings.com
18.	Kevin Sherlin Manager, Business Technology Operations	Sacramento Municipal Utility District 6201 S Street Sacramento, California 95817	(916) 732-6452 csherli@smud.org
19.	Jon Stanford Chief Information Security Officer	Bonneville Power Administration 905 NE 11th Avenue, JB-B1 Portland, Oregon 97232	(503) 230-4222 jkstanford@bpa.gov
20.	Thomas Stevenson Gen Supv Engineering Projects Generation Services Dept	Constellation Energy 1005 Brandon Shores Rd Baltimore, MD 21226	(410) 787-5260 (410) 227-3728 - cell Thomas.W.Stevenson@constellation.com
21.	Keith Stouffer Program Manager, Industrial Control System Security	National Institute of Standards & Technology 100 Bureau Drive Mail Stop 8230 Gaithersburg, Maryland 20899-8230	(301) 975-3877 (301) 990-9688 Fx keith.stouffer@ nist.gov
22.	John Van Boxtel CIP Compliance Engineer	Western Electricity Coordinating Council Suite #201 7600 NE 41st Street Vancouver, WA 98662	(360) 713-9090 jvanboxtel@wecc.biz
23.	John D. Varnell Director, Asset Operations Analysis	Tenaska Power Services Co. 1701 East Lamar Blvd. Arlington, Texas 76006	(817) 462-1037 (817) 462-1035 Fx jvarnell@tnsk.com

24.	William Winters IS Senior Systems Consultant	Arizona Public Service Co. 502 S. 2nd Avenue Mail Station 2387 Phoenix, Arizona 85003	(602) 250-1117 William.Winters@ aps.com
25.	Bradley (Brad) Yeates IT Security Analyst, Principal	Southern Nuclear Operating Company 241 Ralph McGill Blvd. Bin 10030 Atlanta, Ga. 30308	(404) 314-4096 blyeates@southernco .com
Consultant to NERC	Hal Beardall	Florida State University Morgan Building, Suite 236 2035 East Paul Dirac Drive P.O. Box 3062777 Tallahassee, Florida 32310-4161	(850) 644-4945 (850) 644-4968 Fx hbeardall@fsu.edu
Consultant to NERC	Joseph Bucciero President and Executive Consultant	Bucciero Consulting, LLC 3011 Samantha Way Gilbertsville, Pennsylvania 19525	(267) 981-5445 joe.bucciero@ gmail.com
Consultant to NERC	Robert M. Jones Director Florida Conflict Resolution Consortium	Florida State University Morgan Building, Suite 236 2035 East Paul Dirac Drive Tallahassee, Florida 32310-4161	(850) 644-6320 (850) 644-4968 Fx rmjones@fsu.edu
Consultant to NERC	Stuart Langton, PhD Senior Fellow	Florida State University 2010 Wild Lime Drive Sanibel, Florida 33957	(239) 395-9694 (239) 395-3230 Fx slangton@ mindspring.com
NERC Staff	Herb Schrayshuen Vice President and Director of Standards	North American Electric Reliability Corporation 116-390 Village Boulevard Princeton, New Jersey 08540-5721	(609) 452-8060 (609) 452-9550 Fx Herb.schrayshuen@ nerc.net
NERC Staff	Howard L. Gugel Standards Development Coordinator	North American Electric Reliability Corporation 116-390 Village Boulevard Princeton, New Jersey 08540-5721	(609) 452-8060 (609) 452-9550 Fx howard.gugel@ nerc.net
NERC Staff	Roger Lampila Regional Compliance Auditor	North American Electric Reliability Corporation 116-390 Village Boulevard Princeton, New Jersey 08540-5721	(609) 452-8060 (609) 452-9550 Fx roger.lampila@ nerc.net
NERC Staff	Scott R Mix Manager Infrastructure Security	North American Electric Reliability Corporation 116-390 Village Boulevard Princeton, New Jersey 08540-5721	(215) 853-8204 (609) 452-9550 Fx Scott.Mix@ nerc.net
NERC Staff	David Taylor Director of Standards Development	North American Electric Reliability Corporation 116-390 Village Boulevard Princeton, New Jersey 08540-5721	(609) 452-8060 (609) 452-9550 Fx david.taylor@ nerc.net
NERC Staff	Todd Thompson Compliance Investigator	North American Electric Reliability Corporation 116-390 Village Boulevard Princeton, New Jersey 08540-5721	(609) 452-8060 (609) 452-9550 Fx todd.thompson@ nerc.net

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

CSO706 SDT
Meeting Schedule and Objectives

Meeting Location	Dates	Meeting Objective
Orlando, FL OUC	12/14 to 12/16/2010	CIP-002-4 – Review Ballot Results & Approve for SC CIP-010/CIP-011 – Framework proposal
Interim	12/16 to 01/18/2011	Designated individuals begin drafting assignments on CIP-010 and 011 with direction from SDT
Columbus, OH AEP	01/18 to 01/20/2011	Full review of CIP-011 requirements in response to industry comment (first of several development iterations for posting in late June)
Interim	1/20 to 2/15/2011	Designated individuals complete drafting assignments on CIP-011
Taylor, TX ERCOT	2/15 to 2/17/2011	Begin review of CIP-010, BES Cyber System Identification Full review of CIP-011 (requirements, measures, change rationale, guidance)
Interim	2/17 to 3/15/2011	Designated individuals complete drafting assignments on CIP-010 and CIP-011 Begin developing implementation plan
New York, NY ConEd	3/15 to 3/17/2011	Review of CIP-011 (requirements, measures, change rationale, guidance) Review of CIP-010 Initial review of implementation plan
Interim	3/17 to 4/12/2011	Designated individuals complete drafting assignments on CIP-010, CIP-011 and implementation plan
Pomona, CA SCE	4/12 to 4/14/2011	Review of CIP-010, CIP-011 and implementation plan
Interim	4/14 to 5/17/2011	Designated individuals complete drafting assignments on CIP-010, CIP-011 and implementation plan Sneak peak industry webinar in early May
Little Rock, AR AECC	5/17 to 5/19/2011	Review of industry feedback Review of change rationale and guidance
Interim	5/19 to 6/21/2010	Designated individuals complete drafting assignments on CIP-010, CIP-011 and implementation plan NERC begins QA
Portland, OR BPA	6/21 to 6/23/2011	SDT and NERC QA on document for posting
Interim	6/23 to 7/19/2011	Posting for comment Prepare for technical workshop?
TBD	7/19 to 7/21/2011	Technical Workshop?

Meeting Location	Dates	Meeting Objective
TBD	8/23 to 8/25/2011	Respond to comments
TBD	9/20 to 9/22/2011	Respond to comments and prepare for second posting and ballot
TBD	10/11 to 10/13	
Baltimore, MD Constellation	11/16 to 11/19/2010	CIP-002-4 – Response to Comments Revise for Ballot
Orlando, FL OUC	12/13 to 12/16/2010	CIP-002-4 – Review Ballot Results & Approve for SC CIP-010/CIP-011 – Framework proposal
Columbus, OH AEP	01/18 to 01/20/2011	Full review of CIP-011 requirements
Taylor, TX ERCOT	2/15 to 2/17/2011	Full review of requirements and Guidance
New York, NY ConEd	3/15 to 3/17/2011	Full review of requirements, Guidance, and Implementation plan
Pomona, CA SCE	4/11 to 4/15/2011	Perform full QA on documents to be posted
Little Rock, AR AECC	5/17 to 5/19/2011	
Webinar	*6/14/2011*	
Portland, OR BPA	6/21 to 6/23/2011	Discuss and respond to Webinar comments Approve documents for posting
TBD	7/19 to 7/21/2011	Review industry comments and develop responses
TBD	8/23 to 8/25/2011	Develop documents for second ballot
TBD	9/20 to 9/22/2011	Develop documents for third ballot
TBD	10/11 to 10/13	Prepare documents for BOT

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

CSO 706 SDT DRAFTING SUB-TEAMS (OCTOBER, 2010)

Sub-Team	
CIP 010 BES System Categorization	John Lim (Lead), Rich Kinas, Jim Brenton, Dave Norton *(Observer Participants: Rod Hardiman, Jim Fletcher)* *(FERC: Mike Keane, Peter Kuebeck)*
Personnel and Physical Security	Doug Johnson (Lead), Rob Antonishen, Patrick Leon, Kevin Sherlin *(FERC: Drew Kittey)*
System Security and Boundary Protection	Jay Cribb (Lead), Jackie Collett, John Varnell, John Van Boxtel, Philip Huff *(Observer Participant: Brian Newell)* *(FERC: Justin Kelly)*
Incident Response and Recovery	Scott Rosenberger (Lead), Joe Doetzl, Tom Stevenson (*Observer Participant: Jason Marshall)* *(FERC: Dan Bogle)*
Access Control	Sharon Edwards (Lead), Jeff Hoffman, Jerry Freese *(Observer Participants: Roger Fradenburgh, Sam Merrell)* *(FERC: Mike Keane)*
Change Management, System Lifecycle, Information Protection, Maintenance, and Governance	Dave Revill (Lead), Jon Stanford, Keith Stouffer, Bill Winters *(Observer Participant: Brian Newell)* *(FERC: Jan Bargen, Matthew Dale)*
CIP 002-4 Drafting Team	John Lim (Lead), Jackie Collett, Rich Kinas, Jim Brenton, Dave Norton
Implementation Plan CIP 002-4	Sharon Edwards, Dave Revell, Kevin Sherlin, Scott Rosenberg, Dave Norton and Phil Huff and Scott Mix. *(FERC: Mike Keane)*
Framework CIP 010 &011	Jay Cribb (Lead), Joe Doetzl, Phil Huff, Doug Johnson, Dave Norton, Dave Revill, Jon Stanford and John Van Boxtel. Mike Keane FERC and Scott Mix, NERC

CYBER SECURITY FOR ORDER 706 STANDARD DRAFTING TEAM

CSO 706 SDT Consensus Guidelines*)*

(Adopted, November, 2008, Revised June 2010, Revised July, 2010)

The Cyber Security for Order 706 Standard Drafting Team (Team) will seek consensus on its recommendations for any revisions to the CIP standards.

Consensus Defined. Consensus is a participatory process whereby, on matters of substance, the Team strives for agreements which all of the members can accept, support, live with or agree not to oppose. In instances where, after vigorously exploring possible ways to enhance the members' support for posting CIP standards documents for industry comment or balloting, and the Team finds that 100% acceptance or support of the members present is not achievable, decisions to adopt standards documents for balloting will require at least 2/3rds favorable vote of all members present and voting.

Quorum Defined. The Team will make decisions only when a quorum is present. A quorum shall be constituted by at least 2/3 of the appointed members being present in person or by telephone.

Electronic Mail Voting. Electronic voting will only be used when a decision needs to be made between regular meetings under the following conditions:

- It is not possible to coordinate and schedule a conference call for the purpose of voting, or;
- Scheduling a conference call solely for the purpose of voting would be an unnecessary use of time and resources, and the item is considered a small procedural issue that is likely to pass without debate.

Electronic voting will not be used to decide on issues that would require a super majority vote or have been previously voted on during a regular meeting or for any issues that those with opposing views would feel compelled to want to justify and explain their position to other team members prior to a vote. The Electronic Voting procedure shall include the following four steps:

1. The SDT Chair or Vice-Chair in his absence will announce the vote on the SDT mailing list and include the following written information: a summary of the issue being voted on and the vote options; the reason the electronic voting is being conducted; the deadline for voting (which must be at least 4 hours after the time of the announcement).
2. Electronic votes will be tallied at the time of the deadline and no further votes will be counted. If quorum is not reached by the deadline then the vote on the proposal will not pass and the deadline will not be extended.

3. Electronic voting results will be summarized and announced after the voting deadline back to the SDT+ mailing list.
4. Electronic voting results will be recapped at the beginning of the next regular meeting of the SDT.

Consensus Building Techniques and Robert's Rules of Order. The Team will develop its recommendations using consensus-building techniques with the leadership of the Chair and Vice Chair and the assistance of the facilitators. Techniques such as brainstorming, ranking and prioritizing approaches will be utilized. The Team's consensus process will be conducted as a facilitated consensus-building process. Only Team members may participate in consensus ranking or votes on proposals and recommendations. Observers/members of the public are welcome to speak when recognized by the Chair, Vice Chair or Facilitator. The Team will utilize Robert's Rules of Order *(as per the NERC Reliability Standards Development Procedure)*, as modified by the Team's adopted procedural guidelines, to make and approve motions. However, the 2/3's voting requirement will supersede the normal voting requirements used in Robert's Rules of Order for decision-making on substantive motions and amendments to motions. The Team will develop substantive written materials and options using their adopted facilitated consensus-building procedures, and will use Robert's Rules of Order only for formal motions once the Chair determines that a facilitated discussion is completed.

NERC

NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

29th Draft Meeting Summary
Cyber Security Order 706 SDT — Project 2008-06

Orlando, Florida

December 14, 2010, Tuesday - 8 AM to 6 PM EDT
December 15, 2010, Wednesday - 8 AM to 6 PM EDT
December 16, 2010, Thursday - 8 AM to 6 PM EDT

Robert Jones, Stuart Langton, and Hal Beardall
Facilitation and Meeting Design
FCRC Consensus Center, Florida State University

http://www.nerc.com/filez/standards/Project_2008-06_Cyber_Security.html

CSO706 SDT December 14, 2010 Meeting Summary Contents

Cyber Security Order 706 SDT- Project 2008-06
29TH MEETING
December 14-16, 2010
Orlando, Florida

EXECUTIVE SUMMARY

John Lim, Chair of the CSO 706 SDT welcomed members and other participants to Orlando and thanked member Rich Kinas at Orlando Utility Commission for hosting the meeting. Howard Gugel, NERC, conducted a roll call and reviewed the antitrust and public meeting guidelines at the beginning of each day. On Wednesday morning, the SDT unanimously adopted the November 16-18, 2010 Baltimore meeting summary. The chair outlined the objectives the SDT sought to accomplish by the end of the meeting that included review of and agreement on the response to industry comments as well any changes to CIP 002-4 and its related documents, initial review of strawman documents from the Framework team and training on results based standards development.

The Chair reported to that Team that the successive industry ballot on the CIP 002-4 received a quorum (86%) and received 77% support of the industry which was a significant improvement from the support for the first ballot (43%). Howard Gugel, NERC, reviewed the revised comment process clarifying the distinction between a successive ballot and a recirculation ballot. He suggested the SDT should consider and weigh whether any changes in the standard would help change a "no" vote to a "yes", would help to retain the "yes" votes, and keep from turning abstentions into "no" votes. He explained that the successive and recirculation ballots are part of the ANSI process intended to everyone give chance to reevaluate their votes based on the Team's clarifications and answers.

Gerry Cauley addressed the SDT by telephone at the beginning of its meeting. He started by congratulating the team for its hard work under pressure and in responding to his request to bring CIP 002-4 to the industry for balloting in 2010. He noted it has proved useful in discussions with Congressional staff and has had a positive impact on NERC's reputation and credibility in terms of standards development. He clarified his thinking on the path forward for the Team, consistent with its SAR in addressing the FERC Order 706 directives. He suggested that it might be possible to address those directives in the CIP 10-11 framework the SDT has been developing or within the CIP 003-009 framework. He noted that many CEOs have expressed to him concerns about shifting away from CIP 003-009 and the documentation necessary for compliance, but stated that it is up to the Team under the standards development process to bring the proposal to the industry for comment and balloting.

He reviewed his comments to CIPC the past week which he characterized as exploratory in terms of consideration of a more coordinated and comprehensive approach to the goal of security of the BES among efforts such as the CIP standards, the NIST smart grid initiative etc.. He noted he is considering possible approaches including putting together a team that might, in partnership with NIST, address this broader concept and that might lead to a comprehensive set or suite of voluntary "good practice" security guidelines over several years of work. In response to questions, he noted that the SDT needs to address directives and chose which path or framework, in consultation with the industry, is best for reliability and industry implementation. Getting CIP-002-4 will be a first step along the path and NERC will continue

to support the SDT efforts. For the foreseeable future we have to finish the SDT's efforts to address the FERC 706 directives. This other best practice guidelines effort is more long-term with the hope that over a few years we can develop consensus on a voluntary tool kit that will not replace the standards. We will have to wait on experience in developing the guidelines before moving towards any corresponding standards development. The Chair thanked Gerry Cauley and he thanked the Team again for its hard work. On Wednesday afternoon, the SDT discussed Gerry Cauley's comments in relation to future CIP framework for the Team. The comments focused on completing the Version 5 work and clarifying the nature of the parallel process Mr. Cauley outlined.

Scott Mix provided an update on the recent ballot for updates to CIP-005-4 regarding remote access. The ballot concluded with an 84.46% quorum, but a 42.89% approval rating. Approximately 100 pages of comments were filed from both the comment period and the ballot process. The team will be meeting to start responding to comments and modifying the requirement in response to comments. Mr. Mix is also looking into whether a Compliance Application Notice (CAN) can be written to address some of the "double jeopardy" issues identified in the comments (i.e., indicating that some "global" requirements in existing standards will need to be applied to remote access if they are not already). The desire is for the revised standard to be passed by industry and be submitted to FERC in time for the commission to act concomitantly with the CIP-002-4 action. Failing that, the guidance document developed for the standards revision will be handed over to NERC staff for posting as a document in support of the FOUO VPN Alert, and the standard requirement and industry comments will be turned over to the 706 team for its deliberation and consideration in the future version of the CIP standards.

Scott Mix noted that the CAN 005 Remote Access has been noticed as withdrawn and would be undergoing revisions and then reposted.

Howard Gugel reported that the successive ballot of the Cyber Security 706 CIP Version 4 standards was conducted from December 1-10, 2010 and achieved a quorum of 86.83% and a weighted segment approval of 77.04%. Howard provided information on the difference between a successive vs. a recirculation ballot.

During the course of the three-day meeting, the SDT reviewed each industry comment and considered and refined strawman responses and agreed on final responses and on any changes to the standard documents. Each response was either unanimously agreed to by the SDT or the level of consensus was tested with the use of straw polling that helped direct refinements that built sufficient consensus (i.e. support of at least a 2/3's of the SDT members). Below are the key straw polls that lead to refined responses.

On Thursday morning, the SDT, following input from NERC Counsel, moved *(Tom Stevenson with Doug Johnson as 2nd)* to accept the proposed nuclear language with the motion carrying unanimously. Following that, the SDT moved *(Sharon Edwards with Bill Winters as a 2nd)* to approve the package of CIP 002-4 documents (including, Cyber Security — Critical Cyber Asset Identification CIP 002-4, Implementation Plan for Version 4 of Cyber Security Standards CIP-002-4 through CIP-009-4, CIP-002-4 Rational and Implementation Reference Document, Consideration of Comments on Successive Ballot for Cyber Security 706 – CIP Version 4 Standards, and Consideration of Comments on Project 2008-06). The motion passed 17 - 0 with 1 abstention.

Phil Huff reviewed the work of the Framework Team since the SDT meeting in Chicago in August. Since the Baltimore meeting the Team has developed a strawman meeting schedule, a style guide, and a communication plan.

In terms of the overall schedule, Mr. Huff noted that the SDT will begin next month with a possible posting late June or in July. The Framework Team believes that continuing with a sub-team approach may not be the most effective way forwards. Instead they are recommending drafting assignments to Team members and utilizing the full team monthly meetings to review and refine strawman drafts.

The Framework Team has developed a "Style Guide" for drafting results based standards. The Framework Team is recommending a BES cyber system identification using several impact levels: A (high) and B (medium) and a baseline level for low. Part of the communication plan that NERC will work with the Team to implement will include a change document providing rationales for the proposed changes and mapping back to the existing CIP structure. Where possible the existing structure will be retained and justification will be provided for changes are needed. The following are the SDT areas of discussion of the Framework: Clarify Format and Organization; Clarify Proposed CIP 11 "Organization Requirements; Clarify How Many Levels of Impact; Clarify the Scope; and Consider Independent Certification Process.

In preparation for the Version 5 drafting challenges, the SDT engaged in a results based standards review and training conducted by Keith Heidrich FRCC, on Thursday of the meeting. Mr. Heidrich has participated on an ad hoc NERC team convened by Gerry Cauley which has been developing the concept of a results based standards approach. The training objectives were to: Identify and give examples of the elements that define a results-based standard; Analyze the current standards and requirements for weaknesses; Identify the needs, goals, and objectives for this; Create an initial draft of this standard and requirements using result-based methods; and Create measures and necessary supporting material for the standard and requirements. The training covered: Results-based standards/requirements – what are they and why they matter; Scope–what you need to know before writing requirements; Standard requirements – observations and improvements; and Where information is recorded – templates.

On Thursday, Phil Huff noted that based on the review and discussion at this meeting the Framework team would be proposing two impact levels with all other being those items falling outside BES system definition. The Team will present a refined proposal in January taking the SDT input into consideration. For those in those covered in one of these two levels there will be multiple types of controls to be applied. It will get down to the drafting requirements in a consistent format. We recognize detail still needs to be worked out.

The Chair and Vice Chair noted that the expectation is that following the January session the Framework Team would dissolve and an open set of SDT meetings will be used to refine the proposed framework through review of strawman drafts of requirements. The Framework Team will set up conference calls in January in advance of the Columbus meeting.

The Team reviewed the steps and assignments leading up to the Columbus meeting. The Framework Team will be meeting in early January 2011 to prepare documents for the SDT to review at the January 2011 meeting. The recirculation Ballot is expected to close on Friday, December 31 COB. NERC staff will notify the SDT of the ballot results. The Chair thanked Rich Kinas and the OAS for the hosting of the SDT in Orlando.

The meeting adjourned at 4:40 on Thursday, December 16, 2010

Cyber Security Order 706 SDT- Project 2008-06
DRAFT 29TH MEETING SUMMARY
December 14-16, 2010
Orlando, Florida

I. AGENDA REVIEW, WORKPLAN SCHEDULE, REMARKS AND UPDATES

A. Agenda, Milestone Schedule Review

John Lim, Chair of the CSO 706 SDT welcomed members and other participants to Orlando and thanked member Rich Kinas at Orlando Utility Commission for hosting the meeting. Howard Gugel, NERC, conducted a roll call and reviewed the antitrust and public meeting guidelines at the beginning of each day. On Wednesday morning, the SDT unanimously adopted the November 16-18, 2010 Baltimore meeting summary.

The chair outlined the objectives the SDT sought to accomplish by the end of the meeting that included review of and agreement on the response to industry comments as well any changes to CIP 002-4 and its related documents, initial review of strawman documents from the Framework team and training on results based standards development. Bob Jones reviewed the timed agenda which included reviewing ballot and comments on Tuesday, look at remaining 706 directives and the framework effort moving forward on Wednesday, and engaging in a training effort for members on result based approach on Thursday.

B. Overview of the Ballot Results

The Chair reported to that Team that the successive industry ballot on the CIP 002-4 received a quorum (86%) and received 77% support of the industry which was a significant improvement from the support for the first ballot (43%).

Howard Gugel, NERC, reviewed the revised comment process clarifying the distinction between a successive ballot and a recirculation ballot. He noted that if there were significant substantive changes made in Orlando, it would require a new ballot process. He suggested the SDT should consider and weigh whether any changes in the standard would help change a "no" vote to a "yes", would help to retain the "yes" votes, and keep from turning abstentions into "no" votes. He explained that the successive and recirculation ballots are part of the ANSI process intended to everyone give chance to reevaluate their votes based on the Team's clarifications and answers. The Team will need to draft responses to both the negative and positive comments.

C. NERC CEO Gerry Cauley Remarks to the SDT on Cyber Security

Gerry Cauley addressed the SDT by telephone at the beginning of its meeting. He started by congratulating the team for its hard work under pressure and in responding to his request to bring CIP 002-4 to the industry for balloting in 2010. He noted it has proved useful in discussions with Congressional staff and has had a positive impact on NERC's reputation and credibility in terms of standards development.

He wanted to clarify for the SDT what his thinking was on the path forward for the Team consistent with its SAR in addressing the FERC Order 706 directives. He suggested that it might be possible to address those directives in the CIP 10-11 framework the SDT has been developing or within the CIP 003-009 framework. He noted that many CEOs have expressed to him concerns about shifting away from CIP 003-009 and the documentation necessary for compliance, but stated that it is up to the Team under the standards development process to bring the proposal to the industry for comment and balloting.

He reviewed his comments to CIPC the past week which he characterized as exploratory in terms of consideration of a more coordinated and comprehensive approach to the goal of security of the BES among efforts such as the the CIP standards, the NIST smart grid initiative etc.. He noted he is considering possible approaches including putting together a team that might be in partnership with NIST to address this broader concept and that might lead to a comprehensive set or suite of voluntary "good practice" security guidelines over several years of work.

SDT Questions and Answers with Gerry Cauley

- The SDT is working under its SAR with directions to address FERC Order 706 directives. Is this still our charter?
- A: Yes, the SDT needs to address directives and chose which path or framework, in consultation with the industry, is best for reliability and industry implementation.
- The Team's concern is that every six months, we have had to change horses distracting us from addressing the core issues in FERC Order 706. Can you do anything to help us complete our task?
- A: That is consistent with my comments. Getting CIP-002-4 is a first step along the path and NERC will continue to support your efforts as a team.
- What will the collaboration with other areas of security look like?
- A: This is still in early discussions. It might involve forming a team to include industry, NIST, DOE, DHS and others under the NIST umbrella. The current CIP effort should continue and this is a longer-term prospect that will not conflict with the CIP effort. This possible set of guidelines might cover the entire electric system but would not supersede the CIP.
- The SDT has considered and tried to include aspects of the NIST approach. If the guidelines can bolster our effort, will they create the basis for a standard that has more credibility across the cyber security industry?
- A: Yes, both more credibility and acceptance. Your focus though presumes bulk power and the need to develop enforceable standards. I am suggesting a broader set of robust guidelines not limited to bulk power and enforceable standards.
- The SDT team has been frustrated by the limitations on standards writing in our efforts to address cyber security. Perhaps a more comprehensive set of guidelines would help industry.
- We need to ask if in five years whether we will have a more secure electric system? How will we get there? Our standards approach may be too narrow and leave industry exposed.
- How will a non-mandatory guidelines approach connect with 706 Order and compliance/audit system? Will the guidelines be subject to NERC audits?
- A: Nothing is enforceable under 215 unless it has gone through NERC standards process and approved by industry ballot and the BOT.
- The guideline may not be mandatory, but once written will it become industry practice and quasi-mandatory as best practice?

- A: This is a clear concern and a good point. We would rather have guidelines for good protection and address the audit/compliance fear through discussion with industry and improvements of our audit practice.
- Would NERC consider a certification model? There is concern about vendors implementing standards into products. There could be consideration of formal systems within the industry in parallel with the guidelines?
- A: Guidelines may help with the expectation of the industry to the vendors. There could be possible work with national labs on setting benchmarks for the vendors – exploring possibility of doing some testing through national labs to be sure vendors are meeting the expectations. This would be a separate initiative to investigate capabilities of the national lab – want vendors involved in developing the guidelines, then set up a testing system to ensure they are meeting the industry needs.
- We have fifty- plus directives in the order yet to be addressed in another version that will be out for industry review in the face of the implementation schedule for 002-4, assuming it is passed by the industry. Have you considered how all this will come together and address industry concern about changing landscape every year?
- A: For the foreseeable future we have to finish the SDT's efforts to address the FERC 706 directives. This other effort is more long-term with the hope that over a few years we can develop consensus on a voluntary tool kit that will not replace the standards. We will have to wait on experience in developing the guidelines before moving towards any corresponding standards development.
- There is a concern that once CIP 002-4 is approved by industry, FERC may direct us to answer additional questions. There is also a concern or perception that the industry may be more concerned about documenting compliance ("proper documentation") than in establishing better security. What happens if FERC remands 002-4?
- A: A dialogue with FERC would be a better approach as we have common purposes. Recent FERC orders have been clearer about their concerns with our standards and what we need to address, but we cannot rule out further questions about compliance. NERC hopes it will not be remanded, as it is far superior to the current standard.
- A NIST representative recently talked to an industry group about a new effort at collaboration – is this the same effort or different?
- A: Sounds possibly like the same concept.

The Chair thanked Gerry Cauley and he thanked the Team again for its hard work. The Chair asked members to reflect on this overnight and the Team can discuss further as needed on Wednesday.

On Wednesday afternoon the SDT discussed of Gerry Cauley's comments in relation to future CIP framework for the Team. The comments focused on completing the Version 5 work and clarifying the nature of the parallel process Mr. Cauley outlined. Below is a summary of the SDT comments:

SDT Version 5 Work and NERC Assistance

- The SDT needs to focus on and finish the Order 706 effort.
- The SDT believes that addressing the 706 directives will produce so many changes that if CIP 003-009 numbering were retained, that could be the only common feature remaining between the current CIP and Version 5.
- There is a lack of clarity on how the SDT could check with the industry other than developing the Version 5 and putting it out for comment and balloting.

- NERC needs to engage in a significant and serious marketing effort to rally the industry to whatever approach the SDT takes.
- The other issue is how to complete our work – apply appropriate and correct controls, no matter what we call it in terms of format. Now when we delete a requirement, it changes all the following numbers and that has been very confusing too.
  It is likely that after our 706 work, the only thing that will be left is the title. We are also trying to put in new items and address new issues. Simply putting new issues into a new 10 will confuse industry who now thinks 10 is a new High-Medium-Low strategy.
- We have the opportunity of announcing CIP 002-4's adoption by providing info on that and explaining the SDT's approach to the remainder with justification for the decision and the fact there will be heavy revisions to the current CIP. NERC should use this opportunity to begin preparing the industry for the SDT's release in the summer of 2011.
- Perception is everything, and we have a perceived problem with EEI who wants to stay with CIP 003-009. Members in the past have indicated the format is less critical than getting the substance correct.
- We are and will continue getting questions about what we are doing. We all, including NERC, need to help educate the industry.
- NERC should clarify the political support this group needs to get its job done.
- We have a NERC plan for communication which we should refine and send to him.

Potential Parallel Best Practice Initiative

- There is a need beyond the Team for NERC and FERC to review the proposed parallel effort;
- There are many excellent "best practice" guides that already exist in cyber security area that should not be reproduced through this effort.
- This needs further work and is presently confusing the industry and could district the SDT from its effort to complete the 706 work.
- Distinguish between national security concerns and standards development which has financial penalties attached;
- Gerry Cauley proposed two things in this parallel effort and we need to keep them separate. One addresses guidance and recommendations from retail metering to transmission. The other deals with how to secure it given perceived threat and vulnerabilities which NIST has done a good job of characterizing. The reality is that
  much of the good guidelines out there can be misapplied in the real world. The key question of what is right for our environment.
- The good news is that the puzzle is bigger than how NERC has approached this through standards. We need to move forward with producing the nitty-gritty cyber security standards. Focus on the detail work without worrying about the container. NSA and DHS have an agreement and there are several bills floating around Congress. The smart grid is being developed and the practical part is about to hit us on the head. We need broader thinking because of the financial realities – write good access controls and other baseline stuff. CIP 002-4 gave Congress perception of a broader scope. We need to get various parties talking to each other about the broader concept, while the SDT figures out what the requirements need to be.
- At recent conference a NIST representative suggested a new working group (not formed yet) will be looking for opportunities for coordination across standards for smart grid and its relationship to CIP standards. This should not change what we do – as far as CIP standards. We should not minimize the changes in the organization of the standards on the industry.

Companies now have multiple version folders trying to figure out what applies to what and when.
- For the last month and a half, there have been discussions about coordination between NIST and NERC. There is a shared interest by all parties in producing a more coordinated effort. They are looking at pretty much everything on the grid and the interactions needed to minimize inconsistencies. A working group may be formed at a December 15 meeting at NIST.
- Standards we are working on are trying to bolt security onto existing model. That may be different from the direction smart grid is working on. We are working with existing system focusing on reliability and there is the potential for big gaps between the approaches – FERC is most concerned about confidentiality – we need to understand their direction.
- For each interface NISTR defines what is the most important aspect and addresses from that perspective. There may be more in common than expected.

D. Related Cyber Security Initiative Update- CIP 005-4 Urgent Action

Scott Mix provided an update on the recent ballot for updates to CIP-005-4 regarding remote access. The ballot concluded with an 84.46% quorum, but a 42.89% approval rating. Approximately 100 pages of comments were filed from both the comment period and the ballot process. The team will be meeting to start responding to comments and modifying the requirement in response to comments.

Mr. Mix is also looking into whether a Compliance Application Notice (CAN) can be written to address some of the "double jeopardy" issues identified in the comments (i.e., indicating that some "global" requirements in existing standards will need to be applied to remote access if they are not already).

The desire is for the revised standard to be passed by industry and be submitted to FERC in time for the commission to act concomitantly with the CIP-002-4 action. Failing that, the guidance document developed for the standards revision will be handed over to NERC staff for posting as a document in support of the FOUO VPN Alert, and the standard requirement and industry comments will be turned over to the 706 team for its deliberation and consideration in the future version of the CIP standards.

Member Questions
- Will we file a CIP 005-4 in our next posting?
- A: Yes that had been the plan to include the conforming changes and request FERC to act on both petitions in the same order.

E. Related Cyber Security Initiative Update- CAN 005 Remote Access

Scott Mix noted that this has been noticed as withdrawn and would be undergoing revisions and then reposted.

Member Questions and Comments
- Mike Moon has indicated that the errors in the CAN needed to be fixed and that it is being withdrawn for redrafting.
- Heard several utilities are engaging lawyers to challenge the CAN.
- CIP 004 R4.2 CAN- problems noted include: it goes beyond the scope of requirement in CAN; revocation of access of secondary access systems- must be included in the revocation of access plan. Auditors audit to requirements and use the CANs in the audit.

II. REVIEW OF CIP-002-4 INDUSTRY COMMENTS AND SDT RESPONSES

Howard Gugel reported that the successive ballot of the Cyber Security 706 CIP Version 4 standards was conducted from December 1-10, 2010 and achieved a quorum of 86.83% and a weighted segment approval of 77.04%. Howard provided information on the difference between a successive vs. a recirculation ballot.

During the course of the three-day meeting, the SDT reviewed each industry comment and considered and refined strawman responses and agreed on final responses and on any changes to the standard documents. Each response was either unanimously agreed to by the SDT or the level of consensus was tested with the use of straw polling that helped direct refinements that built sufficient consensus (i.e. support of at least a 2/3's of the SDT members). Below are the key straw polls that lead to refined responses.

On Thursday morning, the SDT, following input from NERC Counsel, the SDT moved *(Tom Stevenson with Doug Johnson as 2nd)* to accept the proposed nuclear language with the motion carrying unanimously. Following that, the SDT moved *(Sharon Edwards with Bill Winters as a 2nd)* to approve the package of CIP 002-4 documents (including, Cyber Security — Critical Cyber Asset Identification CIP 002-4, Implementation Plan for Version 4 of Cyber Security Standards CIP-002-4 through CIP-009-4, CIP-002-4 Rational and Implementation Reference Document, Consideration of Comments on Successive Ballot for Cyber Security 706 – CIP Version 4 Standards, and Consideration of Comments on Project 2008-06). The motion passed 17 - 0 with 1 abstention.

III. REVIEW OF THE VERSION 5 FRAMEWORK

A. Framework Discussion and Review

Phil Huff reviewed the work of the Framework Team since the SDT meeting in Chicago in August. Since the Baltimore meeting the Team has developed a strawman meeting schedule, a style guide, and a communication plan. In terms of the overall schedule, Mr. Huff noted that the SDT will begin next month with a possible posting late June or in July. The Framework Team believes that continuing with a sub-team approach may not be the most effective way forwards. Instead they are recommending drafting assignments to Team members and utilizing the full team monthly meetings to review and refine strawman drafts.

The Framework Team has developed a "Style Guide" for drafting results based standards. It is recommending for the Team's consideration a BES cyber system identification using two impact levels: A (high) and B (medium) with a baseline level for low. Part of the communication plan that NERC will work with the Team to implement will include a change document that provides rationales for the proposed changes and mapping back to the existing CIP structure. Where possible the existing structure will be retained and justification will be provided for changes are needed. The following are the SDT comments seeking to clarify aspects of the Framework Team's proposal.

Clarifying Format and Organization

- Still remains to be seen what the whole package with explanatory boxes looks like as a package for filing – don't get hung up on the boxes or depend on them at this point for a final standard.

- Vegetation management is leading the charge on results based standards and establishing the format model
- Without assurance on how to use them, then they may be meaningless
- The idea is to establish a common style guideline the SDT can still use to consistently draft the requirements.

Clarifying Proposed CIP 11 "Organization Requirements

- CIP 11 are proposed as organization requirements that are not asset specific
- Everyone has to have a program. CIP 12 would look at asset impact levels of A, B and baseline – moving to a naming convention with critical assets in A, organizational in B and baseline everything else.
- Organization controls or include technical controls too in B?
- Organization controls but may need to adapt as we create. Everyone should review logs, but should access control be done on everything? This is a big issue for industry
- What about changing password? This gets into how we set and audit measures/
- The SDT will need help from enforcement to set language that is clear to both auditor and audited industry alike.
- The term "organizational" is used differently in CIP and industry depending on context.
- This proposal retains BES cyber system concept. Are we keeping critical cyber assets as a term? Are we pulling the term back?
- The idea is to make 11 level "agnostic." The bullets listed are related to the assets involved. Here you establish you must have a training program, then put details of what is required in the program in 12? Possibly.
- The list of examples here is illustrative not comprehensive. The examples here are organizational not baseline.
- Touch one system and you have touched a thousand more. The cost could be exponential for audit purposes. Keep in mind the distinction between organizational and baseline.
- The intent was organizational – across your organization, not asset specific – from audit standpoint what is the construct?
- Be sure the level of control is tied to type of asset
- Organizational focus replaces the old CIP 11 and there is no low.

Clarifying How Many Levels of Impact

- CIP 10 will identify the levels of impact
- Do we start from baseline and work up to high?
- We will have high and other? Everyone has to do the base or other even if they do not have CA's or CCA's – the high is divided into A and B as to what is required
- CIP 12+ is the devil in the details
- CIP 11 would apply to every entity
- Confused by levels A and B, and baseline. Should we have just high and other?
- Blending levels here? Organizational is not a level, it is all registered entities? Then have three impact levels of A, B and no impact with no regulatory requirement on the no impact level.
- Organizational requirements? Include controls to devices or just requirements for the organization.
- Does not suggest applying organization requirements to devices.

- Two threshold levels: high impact and those that impact reliability but are not critical assets. With a no impact level too.
- Identify every system or just A's and B's? Makes a difference for the scope of this effort.
- We need to establish a SDT consensus on levels and foundation before moving on without a common agreement.
- Level B system description – thought B was everything else that might impact A
- Need common understanding of what each level means
- As we draft controls – B is all the non-critical but some things may still need some controls.
- May help to look at specific examples. E.g. load shedding – we chose 300 mw, but in a low frequency event the end result may be it travels further than it should have and grows as it gets further from the event meaning more impact than it should have had from a cyber perspective.
- Still confused on the number of impact levels for systems? Are there three or two?
- It appears that baseline organizational requirements, may include some A's and some B's.
- This sounds like a compliance rather than a reliability concern.
- May need some baseline of control on all BES cyber systems with two levels of A (critical) and B (non-critical but connected) in terms of registered entities
- The team discussed the path of programmatic controls across programs without tying to assets. The reality is we are writing regulations, not guidance, with violations having penalties associated with them because of audits based compliance system.
- The team is thinking 2 versus 3 levels given our previous experience in trying to set medium level which was artificial. - in our business everything falls into a high that affects a lot of the BES and low that doesn't – level A is the critical or high, B is everything else in the organization.

Clarifying the Scope

- BES systems and non-BES systems – the latter not essential to running BES but the non-BES may be the avenue to attack the BES system.
- FERC does not have jurisdiction over the non-BES system such as email systems.
- CIP 10 is similar to 002-4 – anyone feel there is a need for distinction of non-BES system – favor two levels versus three levels? Just considering impact levels, not connectivity here.
- Working through three levels proved problematic – organizational level for everything and the more for high level – two level system
- We have to work off of a definition of BES system – that is the purview or scope of our work.
- What is the population of system in the scope? Those that impact the reliability of the BES system are the target, not every non-BES system.
- Connectivity determined level, but if not in the inventory of assets how do we ensure it is protected?
- Cyber system is not easily defined. It would be unfair to say it has to be defined to a common understanding. The industry will need flexibility (as cyber systems don't look alike in terms of age and functions) and security boundary is the foundation issue.
- If connected to BES cyber system then it becomes a BES cyber system component though it is not a cyber asset and it needs protection.
- It crosses a threshold that requires you to apply controls and makes it a component once connected
- That is the point in BES cyber system maintenance section in the old CIP 11.

- BES cyber systems have protections – outside cyber system there are components that need protection because they are attached to the system for purposes of maintenance but are not part of the system but a component for maintaining the system
- How are controls on system and controls on components on the system different?
- We can distinguish physical access to component but not the non-physical access.
- May have to break up into more granular level to assign appropriate protections.
- Most of the requirements are written for the cyber level – do we need a different term than "component" or at least for the ancillary ones that get plugged into the system
- Are we dealing with the physical location or type of equipment? The former may differ depending on location but the latter will not.
- Measures – the format is table with first column of requirements and next column with measures – bullets are the guidance for writing measures.
- Based on our discussion as far back as January 2010 (Tucker) we focused on what is the primary intent of the attack.
- Ultimately goes back to 10
- We assume in 002-4 that identified assets are targets in themselves as A and B's are either targets in combination with or avenues of attack to A's.
- Is it a BES cyber system if not connected to anything else – multisite attack?
- In 002-4 we based bright line on impact to BES of its loss so that A is based on impact to BES, B is combined impacts to BES, and others have no impact on BES
- We identified the high impact and those that support the high level. The rest should shake out to those in the BES system that require organizational control will be too difficult to test out all the lows in combination that may impact BES. It may be the right thing to do and appropriate, even if hard to audit. We have to allow entities the flexibility to determine. Already protecting systems to protect our assets, not just to comply with audits – mandatory compliance controls for high assets, limited controls on low and let companies figure out the middle

Independent Certification Process

- Should the SDT consider the option of standing up an independent certification body to establish what qualifies? If it doesn't fit within the SAR and scope of this SDT should we approach NERC about expanding scope to consider certification process?

B. Results Based Standards Training

In preparation for the Version 5 drafting challenges, the SDT engaged in a results based standards review and training conducted by Keith Heidrich FRCC, on Thursday of the meeting. Mr. Heidrich has participated on an ad hoc NERC team convened by Gerry Cauley which has been developing the concept of a results based standards approach.

He outlined the training objectives as:

- Identify and give examples of the elements that define a results-based standard
- Analyze the current standards and requirements for weaknesses
- Identify the needs, goals, and objectives for this
- Create an initial draft of this standard and requirements using result-based methods
- Create measures and necessary supporting material for the standard and requirements

The training covered: Results-based standards/requirements – what are they and why they matter; Scope–what you need to know before writing requirements; Standard requirements – observations and improvements; and Where information is recorded – templates.

Mr. Heidrich noted in a results based approach, the SDT needs to answer the question: *Who, under what conditions (if any), shall perform what action, to achieve what particular result or outcome?* A Standard is a portfolio of requirements designed to achieve an overall defense-in-depth strategy and comply with the quality objectives with each requirement having a role in preventing system failures. Requirements within a standard should be complementary and reinforcing. He distinguished among performance based, risk based and competency based standards.

SDT Member Questions and Comments

- Is cost an appropriate or allowed consideration? A: Yes, but not as a driver – it is an issue in almost any TFE – it is "a consideration for smaller entities but not at consequence of less than excellence in operating system reliability"
- Do we have to establish caveats as to size or cost effectiveness? FERC Order 706 asked industry to establish reasonable and appropriate measures – reliability impact is a safer argument to make for smaller entities – but if everything is connected then smaller entity can impact the BES reliability. A: The CIP 005 team struggled with this issue too and came up with a range of solutions including less costly approaches to minimum levels of protection – can't compromise requirement for cost reasons but you can carve out subsets of applicability based on impact to the BES that cover smaller entities. This is difficult to do if entities are interconnected.

C. Next Steps for Developing the Framework

On Thursday, Phil Huff noted that based on the review and discussion at this meeting the Framework team would be proposing two impact levels with all other being those items falling outside BES system definition. The Team will present a refined proposal in January taking the SDT input into consideration. For those in those covered in one of these two levels there will be multiple types of controls to be applied. It will get down to the drafting requirements in a consistent format. We recognize detail still needs to be worked out.

Member Comments

- Just because we changed labels doesn't make it easier to fix the problems.
- Do NERC standards development requirements allow blank requirements? No
- We need to retain flexibility to make course correction if industry pushes back. We will still need controls regardless of the structure – spend time wisely developing controls then put into structure at the end.
- We need to get on with technical work and worry about style and format later.
- Agree we need to move forward to writing the requirements – guidance to date allows us to use a format to capture and write the controls.
- The Access Control sub-team continued to work and the SDT could use their work as a strawman to test as an example. The sub-team worked with three levels but struggled with

- "medium." Their work as our example may help understand how the propose "two level" system would work

The Chair and Vice Chair noted that the expectation is that following the January 2011 session the Framework Team would dissolve and an open set of SDT meetings will be used to refine the proposed framework through review of strawman drafts of requirements. The Framework Team will set up conference calls in January in advance of the Columbus meeting.

IV. NEXT STEPS AND ASSIGNMENTS

The Team reviewed the steps and assignments leading up to the Columbus meeting. The Framework Team will be meeting in early January 2011 to prepare documents for the SDT to review at the January 2011 meeting. The recirculation Ballot is expected to close on Friday, December 31 COB. NERC staff will notify the SDT of the ballot results.

The Chair thanked Rich Kinas and the OAS for the hosting of the SDT in Orlando.

The meeting adjourned at 4:40 on Thursday, December 16, 2010

Appendix # 1— Meeting Agenda
Project 2008-06 Cyber Security Order 706 SDT
Draft 29th Meeting Agenda
December 14, 2010, Tuesday- 8:00 AM to 6:00 PM EST
December 15, 2010 Wednesday- 8:00 AM to 6:00 PM EST
December 16, 2010 Thursday- 8:00 AM to 6:00 PM EST
Orlando Utilities Commission Offices
6113 Pershing Avenue
Orlando FL

NOTE: 1. Agenda Times May be Adjusted as Needed during the Meeting
NOTE: 2. Drafting Sub-team Meetings May Not Have Access to Telephones and Ready Talk

Proposed Meeting Objectives/Outcomes:

- To review the results of the 2nd Ballot and test consensus on responses to industry comments on CIP 002-4 and, if needed, on any changes for inclusion in a CIP 002-4 3rd ballot.
- To review, refine and test support for recommendations of the CIP Version 5 Framework Team.
- To participate in a Results Based Standards Development Training
- To agree on next steps and assignments

Tuesday, December 14, 2010 8:00 a.m. - 6:00 p.m. EST
- Introduction, welcome -*(Morning)*
- Review meeting and milestone schedule for CIP 002-4 and CIP 010 and 011 *(Morning)*
- Review results of 2nd Ballot CIP-002-4*(Morning)*
- Draft responses to industry and consider any changes to CIP-002-4 *(Morning & Afternoon)*

Wednesday, December 15, 2010 8:00 a.m. - 6:00 p.m. EST
- Seek Motion to Adopt SDT Responses to Industry, and if needed, any changes for inclusion in the 3rd Ballot. *(Morning)*
- Overview of Results Based Standards Development and CIP Version 5- Howard Gugel NERC *(Morning)*
- Receive a Version 5 Framework report *(Morning)*
- Review Draft Strawman Documents and discuss key issues *(Afternoon)*
- Review and initial testing of the acceptability of the approach as refined *(Afternoon)*

Thursday, December 16, 2010, 8:00 a.m. - 6:00 p.m. EST
- Results Based Standards Training- Keith Heidrich, FRCC & Howard Gugel, NERC *(Morning & Afternoon)*
- Review Version 5 Framework in light of Results Based Approach
- Test SDT Support for the Version 5 Framework *(Afternoon)*
- Review Work plan for the Version 5 Framework *(Afternoon)*
- Review SDT January, 2011 Columbus Meeting Agenda (*Late Afternoon)*

Appendix # 2 Attendees List
December 14-16, 2010 Orlando

Attending in Person — SDT Members and Staff

1. Rob Antonishen	Ontario Power Generation
2. Jim Brenton	ERCOT
3. Jay S. Cribb	Southern Company Services
4. Joe Doetzl	Kansas City Pwr. & Light Co
5.Sharon Edwards	Duke Energy
6.Gerald S. Freese	America Electric Pwr.
7. Phillip Huff, Vice Chair	Arkansas Electric Coop Corporation
8. Doug Johnson	Exelon Corporation – Commonwealth Edison
9.Rich Kinas	Orlando Utilities Commission
10. John Lim, Chair	Consolidated Edison Co. NY
11. David Norton	Entergy
12. David S. Revill	Georgia Transmission Corporation
13. Tom Stevenson	Constellation
14. Keith Stouffer	National Institute of Standards & Technology
15. John Van Boxtel	WECC
16. William Winters	Arizona Public Service, Inc.

SDT Members Attending via ReadyTalk and Phone

17. Jackie Collett	Manitoba Hydro
18. William Gross	Nuclear Energy Institute
19. Scott Rosenberger	Luminant Energy
20. Kevin Sherlin	Sacramento Municipal Utility District
21. John D. Varnell	Technology Director, Tenaska Power Services Co.
Gerry Cauley	*NERC (Tu)*
Scott Mix	*NERC*
Howard Gugel	*NERC*
Ralph Anderson	*NERC*
Robert Jones	*FSU/FCRC Consensus Center*
Stuart Langton	*FSU/FCRC Consensus Center*
Hal Beardall	*FSU/FCRC Consensus Center*

SDT Members Not Participating

Jeff Hoffman	U.S. Bureau of Reclamation, Denver
Patricio Leon	Southern California Edison

Jonathan Stanford	Bonneville Power Administration
Bradley Yeates	South Nuclear Operating Company

Others Attending in Person

Robert Preston Lloyd	Southern California Edison
Jim Fletcher	American Electric Power
Jason Marshall	Midwest ISO
Roger Fradenburgh	N&ST
Brian Newell	American Electric Power
Guy Zito	NPCC
Rob Wotherspoon	OUC
Mike Keane	FERC
Kevin Ryan	FERC (Tu/W)
Mark Simon	Encari

Others Attending via Readytalk and Phone

December 14
Matthew Adeleke, Vincent Le, Lawson, Rob Gross, William Bussman, John Hofstetter, Tom Kelly, Justin Doetzl, Joe Artz, Kevin Kittey, Drew Lopez, Andres Camm, Larry Wilson, Bryn Powell, Maggy Hasha, Christine Bargen, Jan Hardiman, Rod Hoffman

December 15
Scott Hoffman, Jeff Powell, Jim Bussman, Nathan Mitchell, NathanRyan, Kevin Sherlin, Kevin Le, vincent Antonishen, Rob bargen, jan Wilson, Bryn adeleke, matthew Barry Barry Lawson, Drew Kittey, Drew Hasha, Christine Rod Hardiman, Andres Lopez

December 16
Drew Kittey, Maggy Powell, Rod Hardiman, John Bussman, , Vincent Le, Bryn Wilson, Andres Lopez, Jan Bargen, Brian Newell, Barry Lawson

Appendix #3 NERC Antitrust Compliance Guidelines

See Antitrust Compliance Guidelines read at the beginning of each day's session at:

The NERC reminder below was read at the beginning of each day's session.

NERC REMINDER FOR USE AT BEGINNING OF MEETINGS AND CONFERENCE CALLS THAT HAVE BEEN PUBLICLY NOTICED AND ARE OPEN TO THE PUBLIC

For face-to-face meeting, with dial-in capability:

Participants are reminded that this meeting is public. Notice of the meeting was posted on the NERC website and widely distributed. The notice included the number for dial-in participation. Participants should keep in mind that the audience may include members of the press and representatives of various governmental authorities, in addition to the expected participation by industry stakeholders.

Appendix #4

Final SDT CIP 002-4 Documents

http://www.nerc.com/filez/standards/Project_2008-06_Cyber_Security_PhaseII_Standards.html

Appendix #5 SDT Sub-Teams

Sub-Team	
CIP 010 BES System Categorization	John Lim (Lead), Rich Kinas, Jim Brenton, Dave Norton *(Observer Participants: Rod Hardiman, Jim Fletcher)* *(FERC: Mike Keane, Peter Kuebeck)*
Personnel and Physical Security	Doug Johnson (Lead), Rob Antonishen, Patrick Leon, Kevin Sherlin *(FERC: Drew Kittey)*
System Security and Boundary Protection	Jay Cribb (Lead), Jackie Collett, John Varnell, John Van Boxtel, Philip Huff *(Observer Participant: Brian Newell)* *(FERC: Justin Kelly)*
Incident Response and Recovery	Scott Rosenberger (Lead), Joe Doetzl, Tom Stevenson (*Observer Participant: Jason Marshall)* *(FERC: Dan Bogle)*
Access Control	Sharon Edwards (Lead), Jeff Hoffman, Jerry Freese, Bill Winters *(Observer Participants: Roger Fradenburgh, Robert Preston Lloyd)* *(FERC: Mike Keane)*
Change Management, System Lifecycle, Information Protection, Maintenance, and Governance	Dave Revill (Lead), Jon Stanford, Keith Stouffer, Bill Winters *(Observer Participant: Brian Newell)* *(FERC: Jan Bargen, Matthew Dale)*
CIP 002-4 Drafting Team	John Lim (Lead), Jim Brenton, Jackie Collett, Jay Cribb, Sharon Edwards, Doug Johnson, Rich Kinas, Dave Norton, Dave Revill, and Bill Winters *(Observer Participants: Rod Hardiman; Jim Fletcher; Bryn Wilson)* *(FERC: Mike Keane, Peter Kuebeck; NERC: Scott Mix)*
Implementation Plan CIP 002-4	Dave Revill (Lead), Sharon Edwards, Kevin Sherlin, Scott Rosenberg, Dave Norton and Phil Huff *(FERC: Mike Keane; NERC: Scott Mix)*
Framework CIP 010 &011	Dave Norton (Lead), Jim Brenton, Jay Cribb, Joe Doetzl, Phil Huff, Doug Johnson, Dave Revill, Jon Stanford, and John Van Boxtel. *(FERC: Mike Keane; NERC: Scott Mix)*

NERC

NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

30th Meeting Summary
Cyber Security Order 706 SDT — Project 2008-06

Columbus, Ohio

January 18, 2011 | Tuesday - 8 a.m. to 6 p.m. EST
January 19, 2011 | Wednesday - 8 a.m. to 6 p.m. EST
January 20, 2011 | Thursday - 8 a.m. to 6 p.m. EST

http://www.nerc.com/filez/standards/Project_2008-06_Cyber_Security.html

116-390 Village Blvd.
Princeton, NJ 08540
609.452.8060 | www.nerc.com

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Cyber Security Order 706 SDT- Project 2008-06
30TH MEETING
January 18-20, 2011
Columbus, Ohio

EXECUTIVE SUMMARY

John Lim, Chair of the CSO 706 SDT welcomed members and other participants to Columbus and thanked Jerry Freese, Jim Fletcher and Brian Newell at American Electric Power for hosting the meeting. Howard Gugel, NERC, conducted a roll call and reviewed the antitrust and public meeting guidelines at the beginning of each day. On Tuesday morning, the SDT unanimously adopted the December 14-16, 2010 Orlando meeting summary. The chair outlined the objectives the SDT sought to accomplish by the end of the meeting that included reviewing the results of the Final Ballot for CIP Version 4, developing CIP Version 5 Need, Goals and Objectives in support of the SDT's decision to adopt the results based standards format in the development of CIP V5, reviewing the current status of CIP-010 and CIP-011, and developing a communication plan for CIP V5.

The Chair announced that the FSU consensus team would no longer be participating in SDT meetings. Robert Jones from the Florida Conflict Resolution Consortium addressed the group to express their pleasure in working with the SDT and best wishes for the project moving forward. In response, the chair expressed appreciation on behalf of the SDT for the exemplary services provided by Robert Jones, Stu Langton and Hal Beardall since the inception of this SDT and best wishes in their future endeavors.

The Chair reported to that team that four members had submitted their resignation from the SDT: Jackie Collett from Manitoba Hydro, Dave Norton from Entergy, Patricio Leon-Alvarado from Southern California Edison, and Bradley (Brad) Yeates from Southern Company. The team expressed its appreciation for the participation of these members. The Chair then asked that each member actively participate in the meetings. In particular, if a member is unable to attend a SDT meeting either in person or by phone, they are asked to inform the Chair so that any possible quorum issues can be addressed prior to the meeting. If a member consistently cannot meet team meetings, they are asked to resign from the team.

The Chair expressed appreciation for the SDT's considerable work over the last quarter of 2010 in developing an industry approved version of the CIP standards that replaced the previous risk based assessment methodology in CIP-002-3 with a bright line criteria contained in CIP-002-4. On December 31, 2010, the registered ballot body approved the version 4 set of CIP standards with a 90.49% quorum, and a 80.56 % approval rating.

Scott Mix provided an update on the recent ballot for updates to CIP-005-4 regarding remote access. The team for Project 2010-15 is continuing to develop responses to comments and modify the proposed requirement in response to comments. That team is still working toward the goal of submitting the approved revised CIP-005-4 to FERC in time for the commission to act in conjunction with the CIP-002-4 action.

Based on the decision of the team to adopt the results based standard model for the next version of the CIP standards, the team chose to spend time at this meeting developing Needs, Goals, and Objectives. After spending considerable time discussing each aspect, the team unanimously adopted the document in Appendix 3.

The team then discussed the approach to developing the standards. The merits and disadvantages concerning the sub-team approach that the team has used to date were fully vetted. The team decided to continue this approach, but has chosen not to break into sub-teams during face-to-face meetings. The current makeup of each sub-team is contained in Appendix 4. The team also had a discussion on the differences between a "CIP-003 to CIP-009" approach versus a "CIP-010 and CIP-011" approach. A document detailing that discussion is in Appendix 5. At this point the team is continuing to develop CIP-010 and CIP-011, with the understanding that they could break apart CIP-011 in the future if they choose.

On Thursday, Brian Newell provided the SDT a *Lunch and Learn* presentation on the implementation of CIP Cyber Security Standards within plant networks.

The latest meeting schedule is in Appendix 6. Further discussions were held on the communication plan, which is located in Appendix 7. The team then discussed the outstanding directives of FERC Order 706, which is located in Appendix 8. The SDT then made the following assignments:

- Philip Huff is to revise the style guide based on discussions of deliverables for the February meeting.
- Everyone is to perform a review of CIP-010.
- Each sub-team is to (1) develop/review rationale statements for each requirement in CIP-011, (2) document prior version references, (3) develop change justification for each table row, and (4) review and refine requirement language and applicability.
- Howard Gugel to reach out to Mike Moon and other NERC staff to provide input during the February meeting.
- Philip Huff is to create a CIP mapping document for the February face-to-face meeting.
- NERC staff to add interpretations and CANs to the *FERC Directives by Sub-Team* document

The Chair thanked Jerry Freese, Jim Fletcher, Brian Newell and AEP for the hosting of the SDT in Columbus.

The meeting adjourned at 4:40 on Thursday, January 20, 2011

Appendix # 1— Meeting Agenda
Project 2008-06 Cyber Security Order 706 SDT
Draft 30th Meeting Agenda
January 18, 2011 Tuesday - 8:00 AM to 6:00 PM EST
January 19, 2011 Wednesday - 8:00 AM to 6:00 PM EST
January 20, 2011 Thursday - 8:00 AM to 6:00 PM EST
American Electric Power Offices
1 Riverside Plaza, Columbus OH

NOTE: Agenda Times May be Adjusted as Needed during the Meeting

Proposed Meeting Objectives/Outcomes:

- To review the results of the Final Ballot for CIP Version 4
- To review, refine and test support for CIP Version 5 Need, Goals and Objectives
- To review and discuss integration of results based standards format into CIP V5
- To agree on next steps and assignments

Tuesday, January 18, 2011 8:00 a.m. - 6:00 p.m. EST
- Introduction, welcome -*(Morning)*
- Review results of Ballot CIP Version 4 Final Ballot, comments and next steps and schedule *(Morning)*
- NERC staff support update (*Morning*)
- Industry review: (*Morning*)
    - Cyber Attack TF and Severe Impact Resilience TF
    - CIP-005-4 Update
    - Hill Update
- CIP V5 Needs, Goals and Objectives *(Afternoon)*

Wednesday, January 19, 2011 8:00 a.m. - 6:00 p.m. EST
- CIP-010 Group Review *(Morning)*
- Controls Review (*Afternoon*)

Thursday, January 20, 2011 8:00 a.m. - 6:00 p.m. EST
- Controls Review (*Morning*)
- Drafting assignments (*Morning/Afternoon*)
- Review SDT February, 2011 Taylor, TX Meeting Agenda (*Late Afternoon)*

Appendix # 2 Attendees List
January 18-20, 2011 Columbus

Attending in Person — SDT Members and Staff

1. Jay Cribb	Southern Company Services
2.Sharon Edwards	Duke Energy
3.Gerald S. Freese	America Electric Pwr.
4. Philip Huff, Vice Chair	Arkansas Electric Coop Corporation
5. Doug Johnson	Exelon Corporation – Commonwealth Edison
6. John Lim, Chair	Consolidated Edison Co. NY
7. David Revill	Georgia Transmission Corporation
8. Scott Rosenberger	Luminant Energy
9. Kevin Sherlin	Sacramento Municipal Utility District
10. Tom Stevenson	Constellation
11. John D. Varnell	Tenaska Power Services Co.

SDT Members Attending via ReadyTalk and Phone

12. Rob Antonishen	Ontario Power Generation (Tu, Th)
13. Jim Brenton	ERCOT
14. Joe Doetzl	Kansas City Pwr. & Light Co (Wed)
15. Jeff Hoffman	U.S. Bureau of Reclamation, Denver (Tu, Wed)
16.Rich Kinas	Orlando Utilities Commission (Wed)
17. William Winters	Arizona Public Service, Inc.
Scott Mix	*NERC*
Howard Gugel	*NERC*
Robert Jones	*FSU/FCRC Consensus Center (Tu)*

SDT Members Not Participating

Jonathan Stanford	Bonneville Power Administration
Bill Gross	NEI
Keith Stouffer	National Institute of Standards & Technology
John Van Boxtel	Portland General

Others Attending in Person

Robert Preston Lloyd	Southern California Edison
Jim Fletcher	American Electric Power
Jason Marshall	Midwest ISO
Roger Fradenburgh	N&ST
Brian Newell	American Electric Power
Dave Burtrum	AECI
Kevin Koloini	AMP (Tu)
Mike Keane	FERC
Tom Alrich	Matrikon
Jim Donahue	OVEC
Steven Parker	EnergySec
Nick Lauriat	N&ST

Others Attending via Readytalk and Phone

January 18
Anna Wang, Sharla Artz, Jan Bargen, Matt Dale, Ingrid Rayo, Barry Lawson, Katie Schnider, James Julien, David Gordon, Larry Camm, Patricio Leon, Drew Kittey, Vincent Le, Annette Johnston, Joe Weiss, Maggy Powell

January 19
Anna Wang, Hewitt Stuart, Vincent Le, Larry Camm, Sharla Artz, Andres Lopez, David Gordon, Annette Johnston, Jan Bargen, Katie Schnider, Ingrid Rayo

January 20
Maggy Powell, Vincent Le, Annette Johnston, Ingrid Rayo, Anna Wang, Jan Bargen, Christine Hasha, Chuck Abell, David Gordon, Andres Lopez, Larry Camm

Appendix #3

NEED, GOALS AND OBJECTIVES – PROJECT 2008-06 - CIP CYBER SECURITY STANDARDS V5

NEED

The need for Critical Infrastructure Protection (CIP) in North America has never been more compelling or necessary than it is today. This is especially true of the electricity sector. Electric power is foundational to our social and economic fabric, acknowledged as one of the most essential and among the most targeted of all the interrelated critical infrastructure sectors.

The Bulk Electric System (BES) is a complex, interconnected collection of facilities that increasingly uses standard cyber technology to perform multiple functions essential to grid reliability. These BES Cyber Systems provide operational efficiency, intercommunications and control capability. They also represent an increased risk to reliability if not equipped with proper security controls to decrease vulnerabilities and minimize the impact of malicious cyber activity.

Cyber attacks on critical infrastructure are becoming more frequent and more sophisticated. Stuxnet is a prime example of an exploit with the potential to seriously degrade and disrupt the BES with highly malicious code introduced via a common USB interface. Other types of attacks are network or Internet-based, requiring no physical presence and potentially affecting multiple facilities simultaneously. It is clear that attack vectors are plentiful, but many exploits are preventable. The common factors in these exploits are vulnerabilities in BES Cyber Systems. The common remedy is to mitigate those vulnerabilities through application of readily available cyber security measures, which include prevention, detection, response and recovery.

In the cyber world, security is truly only as good as its weakest implementation. The need to identify BES Cyber Systems and then protect them through effective cyber security measures are critical steps in helping ensure the reliability of the BES functions they perform.

In approving Version 1 of CIP Standards CIP-002-1 through CIP-009-1, FERC issued a number of directives to the ERO. Versions 2, 3 and 4 addressed the short term standards-related and Critical Asset identification issues from these directives. There are still a number of unresolved standards-related issues in the FERC directives that must be addressed. This version is needed to address these remaining directives in FERC Order 706.

GOALS AND OBJECTIVES

- **Goal 1:** To address the remaining Requirements-related directives from all CIP related FERC orders, all approved interpretations, and CAN topics within applicable existing requirements.
  - **Objective 1.** Provide a list of each directive with a description and rationale of how each has been addressed.
  - **Objective 2.** Provide a list of approved interpretations to existing requirements with a description of how each has been addressed.
  - **Objective 3.** Provide a list of CAN topics with a description of how each has been addressed.
  - **Objective 4.** Consider established security practices (e.g. DHS, NIST) when developing requirements.
  - **Objective 5.** Incorporate the work of Project 2010-15 Urgent Action SAR.
- **Goal 2:** To develop consistent identification criteria of BES Cyber Systems and application of cyber security requirements that are appropriate for the risk presented to the BES.
  - **Objective 6**: Transition from a Critical Cyber Asset framework to a BES Cyber System framework.
  - **Objective 7.** Develop criteria to identify and categorize BES Cyber Systems, leveraging industry approved bright-line criteria in CIP-002-4.
  - **Objective 8.** Develop appropriate cyber security requirements based on categorization of BES Cyber Systems.
  - **Objective 9.** Minimize writing requirements at the device specific level, where appropriate.
- **Goal 3:** To provide guidance and context for each Standard Requirement
  - **Objective 10.** Use the Results-Based Standards format to provide rationale statements and guidance for all of the Requirements.
  - **Objective 11.** Develop measures that describe specific examples that may be used to provide acceptable evidence to meet each requirement. These examples are not all inclusive ways to provide evidence of compliance, but provide assurance that they can be used by entities to show compliance.
  - **Objective 12.** Work with NERC and regional compliance and enforcement personnel to review and refine measures.
- **Goal 4:** To leverage current stakeholder investments used for complying with existing CIP requirements.

- **Objective 13.** Map each new requirement to the requirement(s) in the prior version from which the new requirement was derived.
- **Objective 14.** Justify change in each requirement which differs from the prior version.
- **Objective 15.** Minimize changes to requirements which do not address a directive, interpretation, broad industry feedback or do not significantly improve the Standards.
- **Objective 16.** Justify any other changes (e.g. removals, format)

- **Goal 5:** To minimize technical feasibility exceptions.
  - **Objective 17.** Develop requirements at a level that does not assume the use of specific technologies.
  - **Objective 18.** Allow for technical requirements to be applied more appropriately to specific operating environments (i.e. Control Centers, Generation Facilities, and Transmission Facilities). (also maps to Goal 2)
  - **Objective 19.** Allow for technical requirements to be applied more appropriately based on connectivity characteristics. (also maps to Goal 2)
  - **Objective 20.** Ensure that the words "where technically feasible" exist in appropriate requirements.
- **Goal 6:** To develop requirements that foster a "culture of security" and due diligence in the industry to complement a "culture of compliance".
  - **Objective 21.** Work with NERC Compliance Staff to evaluate options to reduce compliance impacts such as continuous improvement processes, performance based compliance processes, or SOX-like evaluation methods.
  - **Objective 22.** Write each requirement with the end result in mind, (minimizing the use of inclusive phrases such as "every device," "all devices," etc.)
  - **Objective 23.** Minimize compliance impacts due to zero-defect requirements.
- **Goal 7:** To develop a realistic and comprehensible implementation plan for the industry.
  - **Objective 24.** Avoid per device, per requirement compliance dates**.**
  - **Objective 25.** Address complexities of having multiple versions of the CIP standards in rapid succession.
  - **Objective 26.** Consider implementation issues by setting realistic timeframes for compliance.
  - **Objective 27.** Rename and modify IPFNICCAANRE to address BES Cyber System framework.

Appendix #4 SDT Sub-Teams

Sub-Team	
BES Cyber System Categorization	John Lim (Lead), Rich Kinas, Jim Brenton *(Christine Hasha ?)* *(Observer Participants: Rod Hardiman, Jim Fletcher, Robert Preston Lloyd, David Burtrum, Bryn Wilson)* *(FERC: Mike Keane,)*
Personnel and Physical Security	Doug Johnson (Lead), Rob Antonishen, Kevin Sherlin *(FERC: Drew Kittey)*
System Security and Boundary Protection	Jay Cribb (Lead), John Varnell, John Van Boxtel, Philip Huff *(Observer Participant: Brian Newell, David Burtrum)* *(FERC: Justin Kelly)*
Incident Response and Recovery	Scott Rosenberger (Lead), Joe Doetzl, Tom Stevenson (*Observer Participant: Jason Marshall)* *(FERC: Dan Bogle)*
Access Control	Sharon Edwards (Lead), Jeff Hoffman, Jerry Freese *(Observer Participants: Roger Fradenburgh, Robert Preston Lloyd)* *(FERC: Mike Keane)*
Change Management, System Lifecycle, Information Protection, Maintenance, Governance, and Vulnerability Assessments	Dave Revill (Lead), Jon Stanford, Keith Stouffer, Bill Winters *(Observer Participant: Brian Newell)* *(FERC: Jan Bargen, Matthew Dale)*
Implementation Plan CIP 002-4	Dave Revill (Lead), Sharon Edwards, Kevin Sherlin, Scott Rosenberg, Dave Norton and Phil Huff *(FERC: Mike Keane; NERC: Scott Mix)*

Appendix #5

CIP-002 to -009
Vs.
CIP-010 and 011

When we use these terms in comparison to one another, it can mean several things:

1) The *organization of requirements* split into the existing 8 standards or combined into 2 standards?

   Response: A downside of two standards is the optics of the reporting of violations for the "control" standard. "Existing eight standards" might also include one or two additional new standards.

2) The *change from a 'critical asset' method* of determining the cyber systems based on the BES asset's potential impact *to a focus on the cyber systems* themselves and their direct impact? (The 'BES Cyber System' approach – this is the 'big iron vs. cyber systems argument)

   Response: The focus is on BES Cyber Systems, scoped based on reliability functions. The issue is communicating the "position" we have adopted.

3) The *expansion of scope* from just critical assets and their associated CCA's *to all BES Cyber Systems*?

   Response: Remember, this is limited to BES Cyber Systems as scoped in "CIP-010." While we generally agree that there is a baseline of controls that need to be applied to all BES Cyber Systems, it is still to be determined what these controls are that will be proposed by the team. The challenge will be to create meaningful controls that can be practically implemented and reasonably audited for all BES Cyber Systems that will gain industry and regulatory acceptance.

4) *Leave CIP-002 to -009 as is* with changes to meet the remaining 706 directives.

   Response: Changes to the standards in response to FERC directives would be major changes that might leave only the numbers and titles intact.

Appendix 6

CSO706 SDT
Meeting Schedule and Objectives (January 2011)

Development Process

- Face-to-face meetings used to review/refine the entire Standard. Full team reviews Standards to raise issues, formulate concepts to address issues, ensure consistency across sub-teams and further develop work products.
- Sub-teams meet in open web conferences in between face-to-face meetings to address issues raised by the full team.
- Full team 2 hour web conference the 2nd Thursday from 12:00a – 2:00p after every full team meeting to receive sub-team status updates and provide initial feedback.

Meeting Location	Dates	Meeting Objective
Columbus, OH AEP	01/18 to 01/20/2011	Develop Needs, Goals and Objectives. Develop project plan.
Interim	1/20 to 2/15/2011	Sub-Teams to: (1) develop/review rationale statements for each requirement in CIP-011, (2) document prior version references, (3) develop change justification for each table row, and (4) review and refine requirement language and applicability.
Web meeting	2/3/2011	Update on work from subteams (12-2pm EST)
Taylor, TX ERCOT	2/15 to 2/17/2011	Full review of Standards requirements, rationale and change justification Discussion with NERC Compliance staff on programmatic requirements
Interim	2/17 to 3/15/2011	Sub-teams complete drafting assignments and develop measures and guidance statements.
Web meeting	3/3/2011	Update on work from subteams (12-2pm EPT)
New York, NY ConEd	3/15 to 3/17/2011	Full review of Standards requirements, measures and guidance Initial discussions on implementation plan.
Interim	3/17 to 4/12/2011	Sub-teams complete drafting assignments
Web meeting	3/31/2011	Update on work from subteams (12-2pm EPT)

Meeting Location	Dates	Meeting Objective
Sacramento, CA SMUD	4/12 to 4/14/2011	Review of Standards and implementation plan NERC and Regional audit staff review
Interim	4/14 to 5/17/2011	Sub-teams complete drafting assignments Sneak peak industry webinar(s) in early May
Web meeting	5/5/2011	Update on work from subteams (12-2pm EDT)
Little Rock, AR AECC	5/17 to 5/19/2011	Review of industry feedback Include additional NERC staff to begin quality review
Interim	5/19 to 6/21/2010	Sub-teams complete drafting assignments NERC continues quality review
Portland, OR BPA	6/21 to 6/23/2011	SDT and NERC staff quality review on documents for posting
Interim	6/23 to 7/19/2011	Posting for comment Prepare for technical workshop?
TBD	7/19 to 7/21/2011	Technical Workshop?
TBD	8/23 to 8/25/2011	Respond to comments
TBD	9/20 to 9/22/2011	Respond to comments and prepare for second posting and ballot
TBD	10/25 to 10/27	Respond to comments and prepare for third posting and ballot
TBD		
TBD		

Deliverables Needed for Posting

1. CIP Cyber Security Standards
2. Implementation Plan (Not started)
3. FERC Directives Summary (Last updated for informal comment posting)
4. CIP version 4 requirements mapping and change justification (obtained from Standards)
5. Informal Comment Summary (Reside with sub-team leads)
6. Comment Form (Not started)

Appendix 7

CSO706 SDT Communication Plan - 2011

- Develop a paragraph to be appended to communication about FERC filing for Version 4 that provides information on the SDT's plan for 2011 (1/31/2011)
- Develop a powerpoint presentation/talking points that can be used by SDT members to present information on the next version of the CIP standards to regional CIPC/Standards groups. (3/31/2011)
- Develop presentations for mini industry webinars that present various topics from "CIP-011" to solicit informal feedback prior to formal posting (4/30/2011)
- Develop information that can be included in the NERC News monthly publication (monthly in 2011)
- Develop a list of opportunities to meet with industry groups during 2nd and 3rd quarter 2011.

Appendix 8

FERC Specific directives from order 706:

The following table contains the status of all issues raised in the order that were either "direct"ed, specifically in the order, or "adopt"ed from the NOPR..

Note: Given the confusion over the SDT's inclusion of the change in CIP-008 ("Testing the Cyber Security Incident response plan does not require removing a component or system from service during the test") that the commission did not "direct", even though p 687 states: "In light of the comments received, the Commission clarifies that, with respect to full operational testing under CIP-008-1, such testing need not require a responsible entity to remove any systems from service," I did not include any issue that was not actively directed for change, such as those designated "should consider" or similar.

Paragraph	Text	Phase[1]
13	NERC is directed to develop a timetable for development of the modifications to the CIP Reliability Standards and, if warranted, to develop and file with the Commission for approval, a second implementation plan.	This compliance filing; and an implementation plan is filed with each submitted version of the standards
25	we direct NERC to address revisions to the CIP Reliability Standards CIP-002-1 through CIP-009-1 considering applicable features of the NIST framework.	Version 5
47	The Commission adopts the CIP NOPR approach regarding NERC and Regional Entity compliance	Rules of Procedure

[1] Schedule phases in this column mean one or more of the following:
- "Version 2" – complete in filed version 2
- "Version 4" – complete in version 4
- "Version 5" – planned for next major version (12-18 months plus)
- "Guideline" – stand alone guidance started after corresponding requirement is determined
- "TFE Filing" – 2009 filing on TFE proposal and Appendix 4D to RoP
- "not scheduled" – beyond Version 4
- "CMEP" – part of an existing or ongoing compliance audit, self-report or other process
- "VRF Filing(s)" – one of several already-filed (or very soon to be filed in the case of Version 2) VRF and/or VSL filings

Phase may also be self-explanatory if not one of these entries

	with the CIP Reliability Standards.	statement
49	The Commission also adopts its CIP NOPR approach and concludes that reliance on the NERC registration process at this time is an appropriate means of identifying the entities that must comply with the CIP Reliability Standards	Compliance registry process
72	We adopt our proposal in the CIP NOPR that responsible entities must comply with the substance of a Requirement.	CMEP
75	we direct the ERO to develop modifications to the CIP Reliability Standards that require a responsible entity to implement plans, policies and procedure that it must develop pursuant to the CIP Reliability Standards	Version 2
86	The Commission adopts its CIP NOPR proposal and approves NERC's implementation plan and time frames for responsible entities to achieve auditable compliance.	CMEP
89	we direct the ERO to submit a work plan for Commission approval for developing and filing for approval the modifications to the CIP Reliability Standards that we are directing in this Final Rule	This compliance filing; and an implementation plan is filed with each submitted version of the standards
90	We direct the ERO, in its development of a work plan, to consider developing modifications to CIP-002-1 and the provisions regarding technical feasibility exceptions as a first priority, before developing other modifications required by the Final Rule.	TFE Filing
96	we direct the ERO to require more frequent, semiannual, self-certifications prior to the date by which full compliance is required	CMEP program and self-certifications
97	we adopt our CIP NOPR proposals that, while an	CMEP, self-

	entity should not be subject to a monetary penalty if it is unable to certify that it is on schedule, such an entity should explain to the ERO the reason it is unable to self-certify	certification process
106	the Commission adopts the CIP NOPR proposals and directs NERC to modify the CIP Reliability Standards through the Reliability Standards development process to remove the first two Terms ["reasonable business judgment," and "acceptance of risk"], and develop specific conditions that a responsible entity must satisfy to invoke the "technical feasibility" exception	Version 2 and TFE Filing
128	the Commission directs the ERO to develop modifications to the CIP Reliability Standards that do not include this term. We note that many commenters, including NERC, agree that the reasonable business judgment language should be removed based largely on the rationale articulated by the Commission in the CIP NOPR.	Version 2
138	the Commission directs the ERO to modify the CIP Reliability Standards through its Reliability Standards development process to remove references to reasonable business judgment before compliance audits begin.	Version 2
150	The Commission, therefore, directs the ERO to remove acceptance of risk language from the CIP Reliability Standards.	Version 2
156	the Commission directs the ERO to develop through its Reliability Standards development process revised CIP Reliability Standards that eliminate references to acceptance of risk.	Version 2
178	directs the ERO to develop a set of conditions or criteria that a responsible entity must follow when relying on the technical feasibility exception contained in specific Requirements of the CIP Reliability Standards	TFE Filing
186	the Commission adopts its proposal in the CIP	TFE Filing

	NOPR that technical feasibility exceptions may be permitted if appropriate conditions are in place.	
192	the Commission adopts the CIP NOPR proposal for a three step structure to require accountability when a responsible entity relies on technical feasibility as the basis for an exception. We address mitigation and remediation in this section and direct the ERO to develop: (1) a requirement that the responsible entity must develop, document and implement a mitigation plan that achieves a comparable level of security to the Requirement; and (2) a requirement that use of the technical feasibility exception by a responsible entity must be accompanied by a remediation plan and timeline for elimination the use of the technical feasibility exception.	TFE Filing
209	The Commission thus adopts its CIP NOPR proposal that use and implementation of technical feasibility exceptions must be governed by a clear set of criteria.	TFE Filing
211	direct the ERO to include approval of the mitigation and remediation steps by the senior manager (identified pursuant to CIP-003-1) in the course of developing this framework of accountability.	TFE Filing
212	the practical considerations pointed out by a number of the comments have convinced us to adopt an approach to the issue of external oversight different from the one originally proposed.	TFE Filing
218	we direct the ERO to design and conduct an approval process through the Regional Entities and the compliance audit process.	TFE Filing
219	we direct NERC, in developing the accountability structure for the technical feasibility exception, to include appropriate provisions to assure that governmental entities that are subject to Reliability Standards as users, owners or operators of the Bulk-Power System can safeguard sensitive	TFE Filing

	information.	
220	We direct the ERO to submit an annual report to the Commission that provides a wide-area analysis regarding use of the technical feasibility exception and the effect on Bulk-Power System reliability.	TFE Filing
221	we direct the ERO to control and protect the data analysis to the extent necessary to ensure that sensitive information is not jeopardized by the act of submitting the report to the Commission.	TFE Filing
222	we direct the ERO to develop a set of criteria to provide accountability when a responsible entity relies on the technical feasibility exceptions in specific Requirements of the CIP Reliability Standards.	TFE Filing
222	We direct the ERO to develop appropriate modifications, as discussed above.	TFE Filing
233	we direct the ERO to consult with federal entities that are required to comply with both CIP Reliability Standards and NIST standards on the effectiveness of the NIST standards and on implementation issues and report these findings to the Commission.	Ongoing discussions with Drafting Team Members from USBR, BPA, NIST; Development of Version 5
253	While we adopt our CIP NOPR proposal, we recognize that the ERO has already initiated a process to develop such guidance … leave to the ERO's discretion whether to incorporate such guidance into the CIP Reliability Standard, develop it as a separate guidance document, or some combination of the two.	Guideline / Version 5
254	direct the ERO to consider these commenter concerns [how to assess whether a generator or a blackstart unit is "critical" to Bulk-Power System reliability, the proper quantification of risk and frequency, facilities that are relied on to operate or shut down nuclear generating stations, and the consequences of asset failure and asset misuse by	Guideline / Version 5

	an adversary]when developing the guidance.	
255	we direct either the ERO or its designees to provide reasonable technical support to assist entities in determining whether their assets are critical to the Bulk-Power System.	Version 4
257	we direct the ERO to consider this clarification [the meaning of the phrase "used for initial system restoration," in CIP-002-1, Requirement R1.2.4] in its Reliability Standards development process.	Guideline / Version 4
272	the Commission directs the ERO, in developing the guidance discussed above regarding the identification of critical assets, to consider the designation of various types of data as a critical asset or critical cyber asset.	Guideline / Version 5
272	The Commission directs the ERO to develop guidance on the steps that would be required to apply the CIP Reliability Standards to such data and to consider whether this also covers the computer systems that produce the data.	Guideline / Version 5
282	the Commission directs the ERO, through the Reliability Standards development process, to specifically require the consideration of misuse of control centers and control systems in the determination of critical assets	Guideline / Version 5
285	we direct the ERO to consider the comment from ISA99 Team [ISA99 Team objects to the exclusion of communications links from CIP-002-1 and non-routable protocols from critical cyber assets, arguing that both are key elements of associated control systems, essential to proper operation of the critical cyber assets, and have been shown to be vulnerable – by testing and experience].	Version 5
294	The Commission adopts its CIP NOPR proposal and directs the ERO to develop, pursuant to its Reliability Standards development process, a modification to CIP-002-1 to explicitly require that a senior manager annually review and approve the	Version 2

	risk-based assessment methodology.	
294	the Commission directs the ERO to develop a modification to CIP-002-1 to explicitly require that a senior manager annually review and approve the risk-based assessment methodology.	Version 2
322	The Commission adopts its CIP NOPR proposal to direct that the ERO develop through its Reliability Standards development process a mechanism for external review and approval of critical asset lists.	Version 4 (Note: version 4 methodology obviates the need for external review)
329	the Commission directs the ERO, using its Reliability Standards development process, to develop a process of external review and approval of critical asset lists based on a regional perspective.	Version 4 (Note: version 4 methodology obviates the need for external review)
333	we direct the ERO, in developing the accountability structure for the technical feasibility exception, to include appropriate provisions to assure that governmental entities can safeguard sensitive information	TFE Filing
355	the Commission directs the ERO to provide additional guidance for the topics and processes that the required cyber security policy should address.	Guideline
376	the Commission adopts its CIP NOPR proposal and directs the ERO to clarify that the exceptions mentioned in Requirements R2.3 and R3 of CIP-003-1 do not except responsible entities from the Requirements of the CIP Reliability Standards.	Version 5
381	The Commission adopts its CIP NOPR interpretation that Requirement R2 of CIP-003-1 requires the designation of a single manager who has direct and comprehensive responsibility and accountability for implementation and ongoing	Version 2

	compliance with the CIP Reliability Standards	
386	The Commission adopts its CIP NOPR proposal and directs the ERO to develop modifications to Reliability Standards CIP-003-1, CIP-004-1, and/or CIP-007-1, to ensure and make clear that, when access to protected information is revoked, it is done so promptly.	Version 5
397	The Commission directs the ERO to develop modifications to Requirement R6 of CIP-003-1 to provide an express acknowledgment of the need for the change control and configuration management process to consider accidental consequences and malicious actions along with intentional changes.	Version 5 / Guideline
412	The Commission therefore directs the ERO to provide guidance, regarding the issues and concerns that a mutual distrust posture must address in order to protect a responsible entity's control system from the outside world.	Guideline
431	The Commission adopts the CIP NOPR's proposal and directs the ERO to develop a modification to CIP-004-1 that would require affected personnel to receive required training before obtaining access to critical cyber assets (rather than within 90 days of access authorization), but allowing limited exceptions, such as during emergencies, subject to documentation and mitigation.	Version 2
433	we direct the ERO to consider, in developing modifications to CIP-004-1, whether identification of core training elements would be beneficial and, if so, develop an appropriate modification to the Reliability Standard.	Version 5
434	The Commission adopts the CIP NOPR's proposal to direct the ERO to modify Requirement R2 of CIP-004-1 to clarify that cyber security training programs are intended to encompass training on the networking hardware and software and other issues of electronic interconnectivity supporting	Version 5

	the operation and control of critical cyber assets.	
435	Consistent with the CIP NOPR, the Commission directs the ERO to determine what, if any, modifications to CIP-004-1 should be made to assure that security trainers are adequately trained themselves.	Version 5
443	The Commission adopts with modifications the proposal to direct the ERO to modify Requirement R3 of CIP-004-1 to provide that newly-hired personnel and vendors should not have access to critical cyber assets prior to the satisfactory completion of a personnel risk assessment, except in specified circumstances such as an emergency.	Version 2
443	We also direct the ERO to identify the parameters of such exceptional circumstances through the Reliability Standards development process	Version 5
460	The Commission adopts the CIP NOPR proposal to direct the ERO to develop modifications to CIP-004-1 to require immediate revocation of access privileges when an employee, contractor or vendor no longer performs a function that requires physical or electronic access to a critical cyber asset for any reason (including disciplinary action, transfer, retirement, or termination).	Version 5
464	We also adopt our proposal to direct the ERO to modify Requirement R4 to make clear that unescorted physical access should be denied to individuals that are not identified on the authorization list, with clarification.	Version 5
473	The Commission adopts its proposals in the CIP NOPR with a clarification. As a general matter, all joint owners of a critical cyber asset are responsible to protect that asset under the CIP Reliability Standards. The owners of joint use facilities which have been designated as critical cyber assets are responsible to see that contractual obligations include provisions that allow the responsible entity to comply with the CIP	Version 5

	Reliability Standards. This is similar to a responsible entity's obligations regarding vendors with access to critical cyber assets.	
476	we direct the ERO to modify CIP-004-1, and other CIP Reliability Standards as appropriate, through the Reliability Standards development process to address critical cyber assets that are jointly owned or jointly used, consistent	Version 5
496	The Commission adopts the CIP NOPR's proposal to direct the ERO to develop a requirement that each responsible entity must implement a defensive security approach including two or more defensive measures in a defense in depth posture when constructing an electronic security perimeter	Not scheduled System Security
502	The Commission directs that a responsible entity must implement two or more distinct security measures when constructing an electronic security perimeter, the specific requirements should be developed in the Reliability Standards development process.	Not scheduled System Security
502	The Commission also directs the ERO to consider, based on the content of the modified CIP-005-1, whether further guidance on this defense in depth topic should be developed in a reference document outside of the Reliability Standards.	Not scheduled / Guideline System Security
503	The Commission is directing the ERO to revise the Reliability Standard to require two or more defensive measures.	Not scheduled System Security
511	The Commission adopts the CIP NOPR's proposal to direct the ERO to identify examples of specific verification technologies that would satisfy Requirement R2.4, while also allowing compliance pursuant to other technically equivalent measures or technologies.	Version 5
525	The Commission adopts the CIP NOPR proposal to require the ERO to modify CIP-005-1 to require	Version 5

	logs to be reviewed more frequently than 90 days	
526	the Commission directs the ERO to modify CIP-005-1 through the Reliability Standards development process to require manual review of those logs without alerts in shorter than 90 day increments.	Version 5
526	The Commission directs the ERO to modify CIP-005-1 to require some manual review of logs, consistent with our discussion of log sampling below, to improve automated detection settings, even if alerts are employed on the logs.	Version 5
528	the Commission clarifies its direction with regard to reviewing logs. In directing manual log review, the Commission does not require that every log be reviewed in its entirety. Instead, the ERO could provide, through the Reliability Standards development process, clarification that a responsible entity should perform the manual review of a sampling of log entries or sorted or filtered logs.	Version 5
541	we adopt the ERO's proposal to provide for active vulnerability assessments rather than full live vulnerability assessments.	Version 5
542	the Commission adopts the ERO's recommendation of requiring active vulnerability assessments of test systems.	Version 5
544	the Commission directs the ERO to revise the Reliability Standard so that annual vulnerability assessments are sufficient, unless a significant change is made to the electronic security perimeter or defense in depth measure, rather than with every modification.	Version 5
544	we are directing the ERO to determine, through the Reliability Standards development process, what would constitute a modification that would require an active vulnerability assessment	Version 5
547	we direct the ERO to modify Requirement R4 to	Version 5

	require these representative active vulnerability assessments at least once every three years, with subsequent annual paper assessments in the intervening years	
560	the Commission directs the ERO to treat any alternative measures for Requirement R1.1 of CIP-006-1 as a technical feasibility exception to Requirement R1.1, subject to the conditions on technical feasibility exceptions.	TFE Filing / CMEP
572	The Commission adopts the CIP NOPR proposal to direct the ERO to modify this CIP Reliability Standard to state that a responsible entity must, at a minimum, implement two or more different security procedures when establishing a physical security perimeter around critical cyber assets.	Not scheduled Physical Security
575	The Commission also directs the ERO to consider, based on the content of the modified CIP-006-1, whether further guidance on this defense in depth topic should be developed in a reference document outside of the Reliability Standards.	Not scheduled / Guideline Physical Security
581	The Commission adopts the CIP NOPR proposal and directs the ERO to develop a modification to CIP-006-1 to require a responsible entity to test the physical security measures on critical cyber assets more frequently than every three years,	Version 5
597	Therefore, the Commission directs the ERO to eliminate the acceptance of risk language from Requirements R2.3 and R3.2.	Version 2
600	Commission therefore directs the ERO to revise Requirement R3 to remove the acceptance of risk language and to impose the same conditions and reporting requirements as imposed elsewhere in the Final Rule regarding technical feasibility.	Version 2 / TFE Filing
609	We therefore direct the ERO to develop requirements addressing what constitutes a "representative system" and to modify CIP-007-1	Version 5 / Guideline

	accordingly. The Commission directs the ERO to consider providing further guidance on testing systems in a reference document.	
610	we direct the ERO to revise the Reliability Standard to require each responsible entity to document differences between testing and production environments in a manner consistent with the discussion above.	Version 5
611	the Commission cautions that certain changes to a production or test environment might make the differences between the two greater and directs the ERO to take this into account when developing guidance on when to require updated documentation to ensure that there are no significant gaps between what is tested and what is in production.	Version 5
619	The Commission adopts the CIP NOPR proposal with regard to CIP-007-1, Requirement R4. [The Commission proposed to direct the ERO to eliminate the acceptance of risk language from Requirement R4.2, and also attach the same documentation and reporting requirements to the use of technical feasibility in Requirement R4, pertaining to malicious software prevention, as elsewhere. The Commission discussed the issues of defense in depth, technical feasibility, and risk acceptance elsewhere in the CIP NOPR and applied those conclusions here. The Commission further proposed to direct the ERO to modify Requirement R4 to include safeguards against personnel introducing, either maliciously or unintentionally, viruses or malicious software to a cyber asset within the electronic security perimeter through remote access, electronic media, or other means]	Version 5 / not scheduled
622	Therefore, the Commission directs the ERO to eliminate the acceptance of risk language from Requirement R4.2	Version 2
622	The Commission also directs the ERO to modify Requirement R4 to include safeguards against	Version 5 / not

	personnel introducing, either maliciously or unintentionally, viruses or malicious software to a cyber asset within the electronic security perimeter through remote access, electronic media, or other means, consistent with our discussion above	scheduled
628	The Commission continues to believe that, in general, logs should be reviewed at least weekly and therefore adopts the CIP NOPR proposal to require the ERO to modify CIP-007-1 to require logs to be reviewed more frequently than 90 days, but leaves it to the Reliability Standards development process to determine the appropriate frequency, given our clarification below, similar to our action with respect to CIP-005-1	Version 5
629	The Reliability Standards development process should decide the degree to which the revised CIP-007-1 describes acceptable log sampling. The ERO could also provide additional guidance on how to create the sampling of log entries, which could be in a reference document.	Version 5 / guideline
633	The Commission adopts the CIP NOPR proposal to direct the ERO to clarify what it means to prevent unauthorized retrieval of data from a cyber asset prior to discarding it or redeploying it.	Version 4
635	the Commission directs the ERO to revise Requirement R7 of CIP-007-1 to clarify, consistent with this discussion, what it means to prevent unauthorized retrieval of data.	Version 4
643	The Commission adopts its proposal to direct the ERO to provide more direction on what features, functionality, and vulnerabilities the responsible entities should address when conducting the vulnerability assessments, and to revise Requirement R8.4 to require an entity-imposed timeline for completion of the already-required action plan.	Version 5 Hodge Podge

651	We direct the ERO to revise Requirement R9 to state that the changes resulting from modifications to the system or controls shall be documented quicker than 90 calendar days.	Version 2
660	The Commission adopts the CIP NOPR proposal to direct the ERO to provide guidance regarding what should be included in the term reportable incident. … we direct the ERO to develop and provide guidance on the term reportable incident.	Guideline
661	the Commission directs the ERO to develop a modification to CIP-008-1 to: (1) include language that takes into account a breach that may occur through cyber or physical means; (2) harmonize, but not necessarily limit, the meaning of the term reportable incident with other reporting mechanisms, such as DOE Form OE 417; (3) recognize that the term should not be triggered by ineffectual and untargeted attacks that proliferate on the internet; and (4) ensure that the guidance language that is developed results in a Reliability Standard that can be audited and enforced	Version 5 / Guideline
673	The Commission adopts the CIP NOPR proposal to direct the ERO to modify CIP-008-1 to require each responsible entity to contact appropriate government authorities and industry participants in the event of a cyber security incident as soon as possible, but, in any event, within one hour of the event, even if it is a preliminary report.	Version 5 / Guideline
676	the Commission directs the ERO to modify CIP-008-1 to require a responsible entity to, at a minimum, notify the ESISAC and appropriate government authorities of a cyber security incident as soon as possible, but, in any event, within one hour of the event, even if it is a preliminary report.	Version 5/ Guideline
686	The Commission adopts the CIP NOPR proposal to direct the ERO to modify CIP-008-1, Requirement R2 to require responsible entities to maintain documentation of paper drills, full operational drills, and responses to actual incidents, all of	Version 5

	which must include lessons learned.	
686	The Commission further directs the ERO to include language in CIP-008-1 to require revisions to the incident response plan to address these lessons learned.	Version 5
694	For the reasons discussed in the CIP NOPR, the Commission adopts the proposal to direct the ERO to modify CIP-009-1 to include a specific requirement to implement a recovery plan.	Version 5
694	We further adopt the proposal to enforce this Reliability Standard such that, if an entity has the required recovery plan but does not implement it when the anticipated event or conditions occur, the entity will not be in compliance with this Reliability Standard.	Version 5
706	The Commission adopts, with clarification, the CIP NOPR proposal to direct the ERO to modify CIP-009-1 to incorporate use of good forensic data collection practices and procedures into this CIP Reliability Standard.	Not scheduled Response & Recovery
710	Therefore, we direct the ERO to revise CIP-009-1 to require data collection, as provided in the Blackout Report.	Not scheduled Response & Recovery
725	The Commission adopts, with modifications, the CIP NOPR proposal to develop modifications to CIP-009-1 through the Reliability Standards development process to require an operational exercise once every three years (unless an actual incident occurs, in which case it may suffice), but to permit reliance on table-top exercises annually in other years.	Not scheduled Response & Recovery
731	The Commission adopts the CIP NOPR proposal to direct the ERO to modify Requirement R3 of CIP-009-1 to shorten the timeline for updating	Version 2

	recovery plans.	
739	The Commission adopts the CIP NOPR proposal to direct the ERO to modify CIP- 009-1 to incorporate guidance that the backup and restoration processes and procedures required by Requirement R4 should include, at least with regard to significant changes made to the operational control system, verification that they are operational before the backups are stored or relied upon for recovery purposes	Version 5
748	The Commission adopts the CIP NOPR proposal to direct the ERO to modify CIP-009-1 to provide direction that backup practices include regular procedures to ensure verification that backups are successful and backup failures are addressed, so that backups are available for future use.	Version 5
757	Therefore, we will not allow NERC to reconsider the Violation Risk Factor designations in this instance but, rather, direct below that NERC make specific modifications to its designations.	VRF Filing(s)
759	Consistent with the Violation Risk Factor Order, the Commission directs NERC to submit a complete Violation Risk Factor matrix encompassing each Commission approved CIP Reliability Standard.	VRF Filing(s)
767	The Commission adopts the CIP NOPR proposal to direct the ERO to revise 43 Violation Risk Factors.	VRF Filing(s)

Project 2008-06 Cyber Security Order 706 SDT
Draft 30th Meeting Agenda
January 18, 2011 Tuesday - 8:00 AM to 6:00 PM EST
January 19, 2011 Wednesday - 8:00 AM to 6:00 PM EST
January 20, 2011 Thursday - 8:00 AM to 6:00 PM EST
American Electric Power Offices
1 Riverside Plaza, Columbus OH

NOTE: Agenda Times May be Adjusted as Needed during the Meeting

Proposed Meeting Objectives/Outcomes:

- To review the results of the Final Ballot for CIP Version 4
- To review, refine and test support for CIP Version 5 Need, Goals and Objectives
- To review and discuss integration of results based standards format into CIP V5
- To review and discuss communication plan for CIP V5
- To agree on next steps and assignments

Tuesday, January 18, 2011 8:00 a.m. - 6:00 p.m. EST
- Introduction, welcome -*(Morning)*
- Review results of Ballot CIP Version 4 Final Ballot, comments and next steps and schedule *(Morning)*
- NERC staff support update (*Morning*)
- Industry review: (*Morning*)
    - Cyber Attack TF and Severe Impact Resilience TF
    - CIP-005-4 Update
    - Hill Update
- CIP V5 Needs, Goals and Objectives *(Afternoon)*

Wednesday, January 19, 2011 8:00 a.m. - 6:00 p.m. EST
- Adopt CIP V5 Needs, Goals and Objectives (*Morning*)
- Review CIP V5 Project Schedule (*Morning*)
- CIP-010 Group Review *(Afternoon)*
- Controls Review (*Afternoon*)

Thursday, January 20, 2011 8:00 a.m. - 6:00 p.m. EST
- Controls Review (*Morning*)
- Drafting assignments (*Morning/Afternoon*)
- Review/Discuss communication plan for CIP V5
- Review SDT February, 2011 Taylor, TX Meeting Agenda (*Late Afternoon)*

Project 2008-06 Cyber Security Order 706 SDT
Draft 30th Meeting Agenda
January 18, 2011 Tuesday - 8:00 AM to 6:00 PM EST
January 19, 2011 Wednesday - 8:00 AM to 6:00 PM EST
January 20, 2011 Thursday - 8:00 AM to 6:00 PM EST
American Electric Power Offices
1 Riverside Plaza, Columbus OH

NOTE: Agenda Times May be Adjusted as Needed during the Meeting

Proposed Meeting Objectives/Outcomes:

- To review the results of the Final Ballot for CIP Version 4
- To review, refine and test support for CIP Version 5 Need, Goals and Objectives
- To review and discuss integration of results based standards format into CIP V5
- To review and discuss communication plan for CIP V5
- To agree on next steps and assignments

Timed Agenda

Tuesday January 18, 2011 8:00 a.m. - 6:00 p.m. EST

8:00 a.m.	**Introduction, Welcome Opening and Host remarks**- *John Lim, Chair & Phil Huff, Vice Chair, Jim Fletcher, AEP, Host* Roll Call; NERC Antitrust Compliance Guidelines- *Howard Gugel*
8:15	**Review of meeting objectives and Agenda**- *John Lim*
8:20	**Review results of CIP Version 4 Final Ballot results, comments and next steps and schedule** - *Howard Gugel, NERC*
9:00	**Meeting support** - *Howard Gugel, NERC*
9:15	**Industry review – Scott Mix and Others** o Industry Classified Briefing o Cyber Attack TF and Severe Impact Resilience TF o CIP-005-4 Update o Hill Update o Other member updates
10:00	*Break* o
10:15	**Review and discuss Needs, Goals and Objectives –** *John Lim*
12:00	*Lunch*
1:00	***Continue,* Review and discuss Needs, Goals and Objectives**
3:00	*Break*
3:15	**Finalize Needs, Goals and Objectives**
5:50	**Wednesday's agenda**
6:00	*Recess*

Project 2008-06 Cyber Security Order 706 SDT
Draft 30th Meeting Agenda
January 18, 2011 Tuesday - 8:00 AM to 6:00 PM EST
January 19, 2011 Wednesday - 8:00 AM to 6:00 PM EST
January 20, 2011 Thursday - 8:00 AM to 6:00 PM EST
American Electric Power Offices
1 Riverside Plaza, Columbus OH

NOTE: Agenda Times May be Adjusted as Needed during the Meeting

Proposed Meeting Objectives/Outcomes:

- To review the results of the Final Ballot for CIP Version 4
- To review, refine and test support for CIP Version 5 Need, Goals and Objectives
- To review and discuss integration of results based standards format into CIP V5
- To review and discuss communication plan for CIP V5
- To agree on next steps and assignments

Wednesday January 19, 2011 8:00 a.m. - 6:00 p.m. EST

8:00	**Welcome and Agenda Review, Roll Call and Antitrust Guidelines**- *John Lim, Phil Huff, Howard Gugel*
8:15	**Test support for CIP V5 Needs, Goals and Objectives** – *John Lim*
9:00	**Review CIP V5 Project Schedule** – *Howard Gugel*
10:00	*Break*
10:15	**Review CIP-010** – *John Lim*
12:00	Lunch
1:00	**Integration of Results Based standards –** *Phil Huff*
2:00	**Review of CIP-011… controls –** *Phil Huff*
3:30	*Break*
3:45	***Continue***: **Review of CIP-011… controls –** *Phil Huff*
5:50	**Review any drafting assignments and Thursday's agenda**
6:00	*Recess*

Project 2008-06 Cyber Security Order 706 SDT
Draft 30th Meeting Agenda
January 18, 2011 Tuesday - 8:00 AM to 6:00 PM EST
January 19, 2011 Wednesday - 8:00 AM to 6:00 PM EST
January 20, 2011 Thursday - 8:00 AM to 6:00 PM EST
American Electric Power Offices
1 Riverside Plaza, Columbus OH

NOTE: Agenda Times May be Adjusted as Needed during the Meeting

Proposed Meeting Objectives/Outcomes:

- To review the results of the Final Ballot for CIP Version 4
- To review, refine and test support for CIP Version 5 Need, Goals and Objectives
- To review and discuss integration of results based standards format into CIP V5
- To review and discuss communication plan for CIP V5
- To agree on next steps and assignments

Thursday January 20, 2011 8:00 a.m. - 6:00 p.m. EST

8:00	**Welcome and Agenda Review, Roll Call and Antitrust Guidelines**- *John Lim, Phil Huff, Howard Gugel*
8:15	***Continue***: **Review of CIP-011… controls –** *Phil Huff*
10:15	*Break*
10: 30	***Continue***: **Review of CIP-011… controls –** *Phil Huff*
12;00	*Lunch*
1:00	***Continue***: **Review of CIP-011… controls –** *Phil Huff*
2:30	*Break*
2:45	**Review/Discuss Communication Plan for CIP V5 –** *Howard Gugel*
4:45	**Review project schedule, next steps and drafting assignments**
5:45	**Review SDT February, 2011 Taylor, TX Meeting Agenda**
6:00	*Adjourn*

Cyber Security Order 706 Standard Drafting Team (Project 2008-06)

Chairman	John Lim, CISSP Department Manager, IT Infrastructure Planning	Consolidated Edison Co. of New York 4 Irving Place Rm 349-S New York, New York 10003	(212) 460-2712 (212) 387-2100 Fx limj@coned.com
Vice Chairman	Philip Huff Manager, IT Security and Compliance	Arkansas Electric Cooperative Corporation 1 Cooperative Way Little Rock, Arkansas 72119	(501) 570-2444 phuff@aecc.com
Members	Robert Antonishen Protection and Control Manager, Hydro Engineering Division	Ontario Power Generation Inc. 14000 Niagara Parkway Niagara-on the-Lake, Ontario L0S 1J0	(905) 262-2674 (905)262-2686 Fx rob.antonishen@ opg.com
	Jim Brenton, CISSP-ISSAP Principal, Regional Security Coordinator	Electric Reliability Council of Texas, Inc. 2705 West Lake Drive Taylor, Texas 76574	(512) 248-3043 (512) 248-3993 Fx jbrenton@ ercot.com
	Jay S. Cribb Information Security Analyst, Principal	Southern Company Services, Inc. 241 Ralph McGill Boulevard N.E. Bin 10034 Atlanta, Georgia 30308	(404) 506-3854 jscribb@ southernco.com
	Joe Doetzl Manager, Information Security	Kansas City Power & Light Co. 1201 Walnut Kansas City, Missouri 64106	(816) 556-2280 joe.doetzl@ kcpl.com
	Sharon Edwards Project Manager	Duke Energy 139 E. 4th Streets 4th & Main Cincinnati, Ohio 45202	(513) 287-1564 (513) 508-1285 Fx sharon.edwards@ duke-energy.com
	Gerald S. Freese Director, NERC CIP Compliance	American Electric Power 1 Riverside Plaza Columbus, Ohio 43215	(614) 716-2351 (614) 716-1144 Fx gsfreese@aep.com
	William Gross Project Manager, Security	Nuclear Energy Institute 1776 I Street NW, Suite 400 Washington, DC 20006	(202) 739-8123 (202) 437-2428 wrg@nei.org
	Jeffrey Hoffman Chief Architect, IT Policy and Security Division	U.S. Bureau of Reclamation Denver Federal Center Bldg. 67, Rm 380 P.O. Box 25007 (84-21200) Denver, CO 80225	(303) 445-3341 jhoffman@usbr.gov
	Doug Johnson Operations Support Group Transmission Operations & Planning	Exelon - Commonwealth Edison 1N301 Swift Road Lombard, IL 60148	(630) 691-4593 douglas.johnson@ comed.com

	Richard Kinas Manager of Standards Compliance	Orlando Utilities Commission 6113 Pershing Avenue Orlando, Florida 32822	(407) 384-4063 rkinas@ouc.com
	David S Revill Manager, Cyber Security Operations	Georgia Transmission Corporation 2100 East Exchange Place Tucker, Georgia 30084	(770) 270-7815 david.revill@ gatrans.com
	Scott Rosenberger Director, Security and Compliance	Luminant 500 North Akard Dallas, Texas 75201	(214) 812-2412 Scott.Rosenberger@ energyfutureholdings.com
	Kevin Sherlin Manager, Business Technology Operations	Sacramento Municipal Utility District 6201 S Street Sacramento, California 95817	(916) 732-6452 csherli@smud.org
	Jon Stanford Chief Information Security Officer	Bonneville Power Administration 905 NE 11th Avenue, JB-B1 Portland, Oregon 97232	(503) 230-4222 jkstanford@ bpa.gov
	Thomas Stevenson General Supervisor Engineering Projects	Constellation Energy 1005 Brandon Shores Rd Baltimore, MD 21226	(410) 787-5260 (410) 227-3728 Thomas.W.Stevenson@ constellation.com
	Keith Stouffer Program Manager, Industrial Control System Security	National Institute of Standards & Technology 100 Bureau Drive Mail Stop 8230 Gaithersburg, Maryland 20899-8230	(301) 975-3877 (301) 990-9688 keith.stouffer@nist.gov
	John Van Boxtel	Portland General Electric 121 Southwest Salmon Street Portland, Oregon 97204	(503) 464-7093 (503) 317-2464 john.vanboxtel@pgn.com
	John D. Varnell Director, Asset Operations Analysis	Tenaska Power Services Co. 1701 East Lamar Blvd. Arlington, Texas 76006	(817) 462-1037 (817) 462-1035 jvarnell@tnsk.com
	William Winters IS Senior Systems Consultant	Arizona Public Service Co. 502 S. 2nd Avenue Mail Station 2387 Phoenix, Arizona 85003	(602) 250-1117 William.Winters@ aps.com
	Bradley Yeates IT Security Analyst, Principal	Southern Nuclear Operating Company 241 Ralph McGill Boulevard Bin 10030 Atlanta, GA 30308	(404) 506-3886 (404) 314-4096 blyeates@southernco.com
NERC Staff	Tom Hofstetter Regional Compliance Auditor	North American Electric Reliability Corporation 116-390 Village Boulevard Princeton, New Jersey 08540-5721	(609) 452-8060 (609) 452-9550 fax tom.hofstetter@ nerc.net

NERC Staff	Roger Lampila Regional Compliance Auditor	North American Electric Reliability Corporation 116-390 Village Boulevard Princeton, New Jersey 08540-5721	(609) 452-8060 (609) 452-9550 fax roger.lampila@nerc.net
NERC Staff	Scott R Mix Manager Infrastructure Security	North American Electric Reliability Corporation 116-390 Village Boulevard Princeton, New Jersey 08540-5721	(215) 853-8204 (609) 452-9550 fax Scott.Mix@nerc.net
NERC Staff	Howard Gugel Standards Development Coordinator	North American Electric Reliability Corporation 116-390 Village Boulevard Princeton, New Jersey 08540-5721	(609) 651-2269 howard.gugel@nerc.net

CSO706 SDT
Meeting Schedule and Objectives (DRAFT 12-14-10)

Meeting Location	Dates	Meeting Objective
Columbus, OH AEP	01/18 to 01/20/2011	Full review of CIP-011 requirements in response to industry comment (first of several development iterations for posting in late June)
Interim	1/20 to 2/15/2011	Designated individuals complete drafting assignments on CIP-011
Taylor, TX ERCOT	2/15 to 2/17/2011	Begin review of CIP-010, BES Cyber System Identification Full review of CIP-011 (requirements, measures, change rationale, guidance)
Interim	2/17 to 3/15/2011	Designated individuals complete drafting assignments on CIP-010 and CIP-011 Begin developing implementation plan
New York, NY ConEd	3/15 to 3/17/2011	Review of CIP-011 (requirements, measures, change rationale, guidance) Review of CIP-010 Initial review of implementation plan
Interim	3/17 to 4/12/2011	Designated individuals complete drafting assignments on CIP-010, CIP-011 and implementation plan
Pomona, CA SCE	4/12 to 4/14/2011	Review of CIP-010, CIP-011 and implementation plan
Interim	4/14 to 5/17/2011	Designated individuals complete drafting assignments on CIP-010, CIP-011 and implementation plan Sneak peak industry webinar in early May
Little Rock, AR AECC	5/17 to 5/19/2011	Review of industry feedback Review of change rationale and guidance
Interim	5/19 to	Designated individuals complete drafting

Meeting Location	Dates	Meeting Objective
	6/21/2010	assignments on CIP-010, CIP-011 and implementation plan NERC begins QA
Portland, OR BPA	6/21 to 6/23/2011	SDT and NERC QA on document for posting
Interim	6/23 to 7/19/2011	Posting for comment Prepare for technical workshop?
TBD	7/19 to 7/21/2011	Technical Workshop?
TBD	8/23 to 8/25/2011	Respond to comments
TBD	9/20 to 9/22/2011	Respond to comments and prepare for second posting and ballot
TBD	10/11 to 10/13	

CYBER SECURITY FOR ORDER 706 STANDARD DRAFTING TEAM

CSO 706 SDT Consensus Guidelines*)*

(Adopted, November, 2008, Revised June 2010, Revised July, 2010)

The Cyber Security for Order 706 Standard Drafting Team (Team) will seek consensus on its recommendations for any revisions to the CIP standards.

Consensus Defined. Consensus is a participatory process whereby, on matters of substance, the Team strives for agreements which all of the members can accept, support, live with or agree not to oppose. In instances where, after vigorously exploring possible ways to enhance the members' support for posting CIP standards documents for industry comment or balloting, and the Team finds that 100% acceptance or support of the members present is not achievable, decisions to adopt standards documents for balloting will require at least 2/3rds favorable vote of all members present and voting.

Quorum Defined. The Team will make decisions only when a quorum is present. A quorum shall be constituted by at least 2/3 of the appointed members being present in person or by telephone.

Electronic Mail Voting. Electronic voting will only be used when a decision needs to be made between regular meetings under the following conditions:

- It is not possible to coordinate and schedule a conference call for the purpose of voting, or;
- Scheduling a conference call solely for the purpose of voting would be an unnecessary use of time and resources, and the item is considered a small procedural issue that is likely to pass without debate.

Electronic voting will not be used to decide on issues that would require a super majority vote or have been previously voted on during a regular meeting or for any issues that those with opposing views would feel compelled to want to justify and explain their position to other team members prior to a vote. The Electronic Voting procedure shall include the following four steps:

1. The SDT Chair or Vice-Chair in his absence will announce the vote on the SDT mailing list and include the following written information: a summary of the issue being voted on and the vote options; the reason the electronic voting is being conducted; the deadline for voting (which must be at least 4 hours after the time of the announcement).
2. Electronic votes will be tallied at the time of the deadline and no further votes will be counted. If quorum is not reached by the deadline then the vote on the proposal will not pass and the deadline will not be extended.
3. Electronic voting results will be summarized and announced after the voting deadline back to the SDT+ mailing list.
4. Electronic voting results will be recapped at the beginning of the next regular

meeting of the SDT.

Consensus Building Techniques and Robert's Rules of Order. The Team will develop its recommendations using consensus-building techniques with the leadership of the Chair and Vice Chair and the assistance of the facilitators. Techniques such as brainstorming, ranking and prioritizing approaches will be utilized. The Team's consensus process will be conducted as a facilitated consensus-building process. Only Team members may participate in consensus ranking or votes on proposals and recommendations. Observers/members of the public are welcome to speak when recognized by the Chair, Vice Chair or Facilitator. The Team will utilize Robert's Rules of Order *(as per the NERC Reliability Standards Development Procedure),* as modified by the Team's adopted procedural guidelines, to make and approve motions. However, the 2/3's voting requirement will supersede the normal voting requirements used in Robert's Rules of Order for decision-making on substantive motions and amendments to motions. The Team will develop substantive written materials and options using their adopted facilitated consensus-building procedures, and will use Robert's Rules of Order only for formal motions once the Chair determines that a facilitated discussion is completed.

Project 2008-06 Cyber Security Order 706 SDT
31st Meeting Agenda
February 15, 2011 Tuesday - 8:00 AM to 6:00 PM CST
February 16, 2011 Wednesday - 8:00 AM to 6:00 PM CST
February 17, 2011 Thursday - 8:00 AM to 6:00 PM CST
ERCOT
800 Airport Drive, Taylor, TX

NOTE: Agenda Times May be Adjusted as Needed during the Meeting

Proposed Meeting Objectives/Outcomes:

- To agree on whether to post CIP Version 5 as a single standard or multiple standards
- To evaluate options with NERC compliance staff to minimize excessive compliance costs while improving cyber security
- To review and refine CIP Version 5 BES Cyber System identification and security requirements
- To agree on next steps and assignments

Timed Agenda

Tuesday February 15, 2011 8:00 a.m. - 6:00 p.m. CST

8:00 a.m.	**Introduction, Welcome Opening and Host remarks**- *John Lim, Chair & Phil Huff, Vice Chair, Jim Brenton, ERCOT, Host* Roll Call; NERC Antitrust Compliance Guidelines- *Howard Gugel, NERC*
8:15	**Review of meeting objectives and Agenda**- *John Lim*
8:20	**Industry Review**- *Scott Mix, NERC, Mike Keane, FERC and others* o DOE Audit Report o FERC Technical Conference o Cyber Attack TF and Severe Impact Resilience TF o CIP-005-4 Update
8:50	**Discussion on format for posting** – *John Lim*
10:00	*Break*
10:15	***Continue,* Discussion on format for posting**
11:30	**Motion on format for posting next version of CIP Cyber Security Standards**
12:00	*Lunch*
1:00	**Evaluate writing programmatic requirements –** *Mike Moon, NERC and other NERC compliance staff*
3:00	*Break*
3:15	**Evaluate minimizing zero-defect requirements –** *Mike Moon and compliance staff*
4:30	**Evaluate options for improving the TFE process -** *Mike Moon and compliance staff*
5:50	**Review any Drafting Assignments and Wednesday's agenda**
6:00	*Recess*

Project 2008-06 Cyber Security Order 706 SDT
31st Meeting Agenda
February 15, 2011 Tuesday - 8:00 AM to 6:00 PM CST
February 16, 2011 Wednesday - 8:00 AM to 6:00 PM CST
February 17, 2011 Thursday - 8:00 AM to 6:00 PM CST
ERCOT
800 Airport Drive, Taylor, TX

NOTE: Agenda Times May be Adjusted as Needed during the Meeting

Proposed Meeting Objectives/Outcomes:

- To agree on whether to post CIP Version 5 as a single standard or multiple standards
- To evaluate options with NERC compliance staff to minimize excessive compliance costs while improving cyber security
- To review and refine CIP Version 5 BES Cyber System identification and security requirements
- To agree on next steps and assignments

Wednesday February 16, 2011 8:00 a.m. - 6:00 p.m. CST

8:00 a.m.	**Welcome and Agenda Review, Roll Call and Antitrust Guidelines** – *John Lim, Philip Huff, Howard Gugel*
8:15	**Review Project Schedule –** *Philip Huff*
8:40	**Review and Refine BES Cyber System Identification** – *John Lim*
10:00	*Break*
10:15	***Continue,* Review and Refine BES Cyber System Identification**
12:00	*Lunch*
1:00	**Review modifications to style guide for security requirements –** *Philip Huff*
1:30	**Review and Refine Security Policy, Change Management, Information Protection and Maintenance Requirements –** *Dave Revill, Georgia Transmission*
3:00	*Break*
3:15	***Continue,* Review and Refine Security Policy, Change Management, Information Protection and Maintenance Requirements**
3:30	**Review and Refine Personnel and Physical Security Requirements –** *Doug Johnson, ComEd*
5:50	**Review any Drafting Assignments and Thursday's agenda**
6:00	*Recess*

Project 2008-06 Cyber Security Order 706 SDT
31st Meeting Agenda
February 15, 2011 Tuesday - 8:00 AM to 6:00 PM CST
February 16, 2011 Wednesday - 8:00 AM to 6:00 PM CST
February 17, 2011 Thursday - 8:00 AM to 6:00 PM CST
ERCOT
800 Airport Drive, Taylor, TX

NOTE: Agenda Times May be Adjusted as Needed during the Meeting

Proposed Meeting Objectives/Outcomes:

- To agree on whether to post CIP Version 5 as a single standard or multiple standards
- To evaluate options with NERC compliance staff to minimize excessive compliance costs while improving cyber security
- To review and refine CIP Version 5 BES Cyber System identification and security requirements
- To agree on next steps and assignments

Thursday February 17, 2011 8:00 a.m. - 6:00 p.m. CST

8:00 a.m.	**Welcome and Agenda Review, Roll Call and Antitrust Guidelines** – *John Lim, Philip Huff, Howard Gugel*
8:15	**Review and Refine Electronic Access Control Requirements** – *Sharon Edwards, Duke Energy*
10:00	*Break*
10:15	**Review and Refine System and Boundary Protection Requirements –** *Jay Cribb, Southern Company*
12:00	*Lunch*
1:00	**Review and Refine Response and Recovery Requirements –** *Scott Rosenberger, Luminant*
3:00	*Break*
3:15	**Review project schedule and agree to next steps**
4:30	**Review Communication Plan –** *Howard Gugel*
5:00	**Review SDT March 2011 New York, NY Meeting**
6:00	*Adjourn*

Cyber Security Order 706 Standard Drafting Team (Project 2008-06)

Chairman	John Lim, CISSP Department Manager, IT Infrastructure Planning	Consolidated Edison Co. of New York 4 Irving Place Rm 349-S New York, New York 10003	(212) 460-2712 (212) 387-2100 Fx limj@coned.com
Vice Chairman	Philip Huff Security Analyst	Arkansas Electric Cooperative Corporation 1 Cooperative Way Little Rock, Arkansas 72119	(501) 570-2444 phuff@aecc.com
Members	Robert Antonishen Protection and Control Manager, Hydro Engineering Division	Ontario Power Generation Inc. 14000 Niagara Parkway Niagara-on the-Lake, Ontario L0S 1J0	(905) 262-2674 (905)262-2686 Fx rob.antonishen@ opg.com
	Jim Brenton, CISSP-ISSAP Principal, Regional Security Coordinator	Electric Reliability Council of Texas, Inc. 2705 WCST Lake Drive Taylor, Texas 76574	(512) 248-3043 (512) 248-3993 Fx jbrenton@ ercot.com
	Jay S. Cribb Information Security Analyst, Principal	Southern Company Services, Inc. 241 Ralph McGill Boulevard N.E. Bin 10034 Atlanta, Georgia 30308	(404) 506-3854 jscribb@ southernco.com
	Joe Doetzl Manager, Information Security	Kansas City Power & Light Co. 1201 Walnut Kansas City, Missouri 64106	(816) 556-2280 joe.doetzl@ kcpl.com
	Sharon Edwards Project Manager	Duke Energy 139 E. 4th Streets 4th & Main Cincinnati, Ohio 45202	(513) 287-1564 (513) 508-1285 Fx sharon.edwards@ duke-energy.com
	Gerald S. Freese Director, NERC CIP Compliance	American Electric Power 1 Riverside Plaza Columbus, Ohio 43215	(614) 716-2351 (614) 716-1144 Fx gsfreese@aep.com
	William Gross Project Manager, Security	Nuclear Energy Institute 1776 I Street NW, Suite 400 Washington, DC 20006	(202) 739-8123 (202) 437-2428 wrg@nei.org
	Jeffrey Hoffman Chief Architect, IT Policy and Security Division	U.S. Bureau of Reclamation Denver Federal Center Bldg. 67, Rm 380 P.O. Box 25007 (84-21200) Denver, CO 80225	(303) 445-3341 jhoffman@usbr.gov
	Doug Johnson Operations Support Group Transmission Operations & Planning	Exelon - Commonwealth Edison 1N301 Swift Road Lombard, IL 60148	(630) 691-4593 douglas.johnson@ comed.com

	Richard Kinas Manager of Standards Compliance	Orlando Utilities Commission 6113 Pershing Avenue Orlando, Florida 32822	(407) 384-4063 rkinas@ouc.com
	David S Revill Manager, Cyber Security Operations	Georgia Transmission Corporation 2100 East Exchange Place Tucker, Georgia 30084	(770) 270-7815 david.revill@ gatrans.com
	Scott Rosenberger Director, Security and Compliance	Luminant 500 North Akard Dallas, Texas 75201	(214) 812-2412 Scott.Rosenberger@ energyfutureholdings.com
	Kevin Sherlin Manager, Business Technology Operations	Sacramento Municipal Utility District 6201 S Street Sacramento, California 95817	(916) 732-6452 csherli@smud.org
	Jon Stanford Chief Information Security Officer	Bonneville Power Administration 905 NE 11th Avenue, JB-B1 Portland, Oregon 97232	(503) 230-4222 jkstanford@ bpa.gov
	Thomas Stevenson General Supervisor Engineering Projects	Constellation Energy 1005 Brandon Shores Rd Baltimore, MD 21226	(410) 787-5260 (410) 227-3728 Thomas.W.Stevenson@ constellation.com
	Keith Stouffer Program Manager, Industrial Control System Security	National Institute of Standards & Technology 100 Bureau Drive Mail Stop 8230 Gaithersburg, Maryland 20899-8230	(301) 975-3877 (301) 990-9688 keith.stouffer@nist.gov
	John Van Boxtel	Portland General Electric 121 SouthwCST Salmon Street Portland, Oregon 97204	(503) 464-7093 (503) 317-2464 john.vanboxtel@pgn.com
	John D. Varnell Director, Asset Operations Analysis	Tenaska Power Services Co. 1701 East Lamar Blvd. Arlington, Texas 76006	(817) 462-1037 (817) 462-1035 jvarnell@tnsk.com
	William Winters IS Senior Systems Consultant	Arizona Public Service Co. 502 S. 2nd Avenue Mail Station 2387 Phoenix, Arizona 85003	(602) 250-1117 William.Winters@ aps.com
NERC Staff	Tom Hofstetter Regional Compliance Auditor	North American Electric Reliability Corporation 116-390 Village Boulevard Princeton, New Jersey 08540-5721	(609) 452-8060 (609) 452-9550 fax tom.hofstetter@ nerc.net
NERC Staff	Roger Lampila Regional Compliance Auditor	North American Electric Reliability Corporation 116-390 Village Boulevard Princeton, New Jersey 08540-5721	(609) 452-8060 (609) 452-9550 fax roger.lampila@ nerc.net

NERC Staff	Scott R Mix Manager Infrastructure Security	North American Electric Reliability Corporation 116-390 Village Boulevard Princeton, New Jersey 08540-5721	(215) 853-8204 (609) 452-9550 fax Scott.Mix@ nerc.net
NERC Staff	Howard Gugel Standards Development Coordinator	North American Electric Reliability Corporation 116-390 Village Boulevard Princeton, New Jersey 08540-5721	(609) 651-2269 howard.gugel@ nerc.net

CSO706 SDT
Meeting Schedule and Objectives

Meeting Location	Dates	Meeting Objective
Columbus, OH AEP	01/18 to 01/20/2011	Full review of CIP-011 requirements in response to industry comment (first of several development iterations for posting in late June)
Interim	1/20 to 2/15/2011	Designated individuals complete drafting assignments on CIP-011
Taylor, TX ERCOT	2/15 to 2/17/2011	Begin review of CIP-010, BES Cyber System Identification Full review of CIP-011 (requirements, measures, change rationale, guidance)
Interim	2/17 to 3/15/2011	Designated individuals complete drafting assignments on CIP-010 and CIP-011 Begin developing implementation plan
New York, NY ConEd	3/15 to 3/17/2011	Review of CIP-011 (requirements, measures, change rationale, guidance) Review of CIP-010 Initial review of implementation plan
Interim	3/17 to 4/12/2011	Designated individuals complete drafting assignments on CIP-010, CIP-011 and implementation plan
Sacramento, CA SMUD	4/12 to 4/14/2011	Review of CIP-010, CIP-011 and implementation plan
Interim	4/14 to 5/17/2011	Designated individuals complete drafting assignments on CIP-010, CIP-011 and implementation plan Sneak peak industry webinar in early May
Little Rock, AR AECC	5/17 to 5/19/2011	Review of industry feedback Review of change rationale and guidance
Interim	5/19 to	Designated individuals complete drafting

Meeting Location	Dates	Meeting Objective
	6/21/2010	assignments on CIP-010, CIP-011 and implementation plan NERC begins QA
????????	6/21 to 6/23/2011	SDT and NERC QA on document for posting
Interim	6/23 to 7/19/2011	Posting for comment Prepare for technical workshop?
TBD	7/19 to 7/21/2011	Technical Workshop?
TBD	8/23 to 8/25/2011	Respond to comments
TBD	9/20 to 9/22/2011	Respond to comments and prepare for second posting and ballot
TBD	10/11 to 10/13	

CSO 706 SDT DRAFTING SUB-TEAMS

Sub-Team	
CIP 010 BES System Categorization	John Lim (Lead), Rich Kinas, Jim Brenton *(Observer Participants: Rod Hardiman, Jim Fletcher, Dave Burtrum)* *(FERC: Mike Keane, Peter Kuebeck)*
Personnel and Physical Security	Doug Johnson (Lead), Rob Antonishen, Kevin Sherlin *(FERC: Drew Kittey)*
System Security and Boundary Protection	Jay Cribb (Lead), John Varnell, John Van Boxtel, Philip Huff *(Observer Participant: Brian Newell)* *(FERC: Justin Kelly)*
Incident Response and Recovery	Scott Rosenberger (Lead), Joe Doetzl, Tom Stevenson (*Observer Participant: Jason Marshall)* *(FERC: Dan Bogle)*
Access Control	Sharon Edwards (Lead), Jeff Hoffman, Jerry Freese *(Observer Participants: Roger Fradenburgh, Sam Merrell)* *(FERC: Mike Keane)*
Change Management, System Lifecycle, Information Protection, Maintenance, and Governance	Dave Revill (Lead), Jon Stanford, Keith Stouffer, Bill Winters *(Observer Participant: Brian Newell)* *(FERC: Jan Bargen, Matthew Dale)*
Framework CIP 010 &011	Jay Cribb (Lead), Joe Doetzl, Phil Huff, Doug Johnson, Dave Norton, Dave Revill, Jon Stanford and John Van Boxtel. Mike Keane FERC and Scott Mix, NERC

NEED, GOALS AND OBJECTIVES – PROJECT 2008-06 - CIP CYBER SECURITY STANDARDS V5 – ADOPTED JANUARY 2011

NEED

The need for Critical Infrastructure Protection (CIP) in North America has never been more compelling or necessary than it is today. This is especially true of the electricity sector. Electric power is foundational to our social and economic fabric, acknowledged as one of the most essential and among the most targeted of all the interrelated critical infrastructure sectors.

The Bulk Electric System (BES) is a complex, interconnected collection of facilities that increasingly uses standard cyber technology to perform multiple functions essential to grid reliability. These BES Cyber Systems provide operational efficiency, intercommunications and control capability. They also represent an increased risk to reliability if not equipped with proper security controls to decrease vulnerabilities and minimize the impact of malicious cyber activity.

Cyber attacks on critical infrastructure are becoming more frequent and more sophisticated. Stuxnet is a prime example of an exploit with the potential to seriously degrade and disrupt the BES with highly malicious code introduced via a common USB interface. Other types of attacks are network or Internet-based, requiring no physical presence and potentially affecting multiple facilities simultaneously. It is clear that attack vectors are plentiful, but many exploits are preventable. The common factors in these exploits are vulnerabilities in BES Cyber Systems. The common remedy is to mitigate those vulnerabilities through application of readily available cyber security measures, which include prevention, detection, response and recovery.

In the cyber world, security is truly only as good as its weakest implementation. The need to identify BES Cyber Systems and then protect them through effective cyber security measures are critical steps in helping ensure the reliability of the BES functions they perform.

In approving Version 1 of CIP Standards CIP-002-1 through CIP-009-1, FERC issued a number of directives to the ERO. Versions 2, 3 and 4 addressed the short term standards-related and Critical Asset identification issues from these directives. There are still a number of unresolved standards-related issues in the FERC directives that must be addressed. This version is needed to address these remaining directives in FERC Order 706.

GOALS AND OBJECTIVES

- **Goal 1:** To address the remaining Requirements-related directives from all CIP related FERC orders, all approved interpretations, and CAN topics within applicable existing requirements.
    - **Objective 1.** Provide a list of each directive with a description and rationale of how each has been addressed.
    - **Objective 2.** Provide a list of approved interpretations to existing requirements with a description of how each has been addressed.
    - **Objective 3.** Provide a list of CAN topics with a description of how each has been addressed.
    - **Objective 4.** Consider established security practices (e.g. DHS, NIST) when developing requirements.
    - **Objective 5.** Incorporate the work of Project 2010-15 Urgent Action SAR.
- **Goal 2:** To develop consistent identification criteria of BES Cyber Systems and application of cyber security requirements that are appropriate for the risk presented to the BES.
    - **Objective 6**: Transition from a Critical Cyber Asset framework to a BES Cyber System framework.
    - **Objective 7.** Develop criteria to identify and categorize BES Cyber Systems, leveraging industry approved bright-line criteria in CIP-002-4.
    - **Objective 8.** Develop appropriate cyber security requirements based on categorization of BES Cyber Systems.
    - **Objective 9.** Minimize writing requirements at the device specific level, where appropriate.
- **Goal 3:** To provide guidance and context for each Standard Requirement
    - **Objective 10.** Use the Results-Based Standards format to provide rationale statements and guidance for all of the Requirements.

- **Objective 11.** Develop measures that describe specific examples that may be used to provide acceptable evidence to meet each requirement. These examples are not all inclusive ways to provide evidence of compliance, but provide assurance that they can be used by entities to show compliance.
- **Objective 12.** Work with NERC and regional compliance and enforcement personnel to review and refine measures.

- **Goal 4:** To leverage current stakeholder investments used for complying with existing CIP requirements.
  - **Objective 13.** Map each new requirement to the requirement(s) in the prior version from which the new requirement was derived.
  - **Objective 14.** Justify change in each requirement which differs from the prior version.
  - **Objective 15.** Minimize changes to requirements which do not address a directive, interpretation, broad industry feedback or do not significantly improve the Standards.
  - **Objective 16.** Justify any other changes (e.g. removals, format)
- **Goal 5:** To minimize technical feasibility exceptions.
  - **Objective 17.** Develop requirements at a level that does not assume the use of specific technologies.
  - **Objective 18.** Allow for technical requirements to be applied more appropriately to specific operating environments (i.e. Control Centers, Generation Facilities, and Transmission Facilities). (also maps to Goal 2)
  - **Objective 19.** Allow for technical requirements to be applied more appropriately based on connectivity characteristics. (also maps to Goal 2)
  - **Objective 20.** Ensure that the words "where technically feasible" exist in appropriate requirements.
- **Goal 6:** To develop requirements that foster a "culture of security" and due diligence in the industry to compliment a "culture of compliance".
  - **Objective 21.** Work with NERC Compliance Staff to evaluate options to reduce compliance impacts such as continuous improvement processes, performance based compliance processes, or SOX-like evaluation methods.
  - **Objective 22.** Write each requirement with the end result in mind, (minimizing the use of inclusive phrases such as "every device," "all devices," etc.)
  - **Objective 23.** Minimize compliance impacts due to zero-defect requirements.

- **Goal 7:** To develop a realistic and comprehensible implementation plan for the industry.
    - **Objective 24.** Avoid per device, per requirement compliance dates**.**
    - **Objective 25.** Address complexities of having multiple versions of the CIP standards in rapid succession.
    - **Objective 26.** Consider implementation issues by setting realistic timeframes for compliance.
    - **Objective 27.** Rename and modify IPFNICCAANRE to address BES Cyber System framework.

CYBER SECURITY FOR ORDER 706 STANDARD DRAFTING TEAM

CSO 706 SDT Consensus Guidelines*)*

(Adopted, November, 2008, Revised June 2010, Revised July, 2010)

The Cyber Security for Order 706 Standard Drafting Team (Team) will seek consensus on its recommendations for any revisions to the CIP standards.

Consensus Defined. Consensus is a participatory process whereby, on matters of substance, the Team strives for agreements which all of the members can accept, support, live with or agree not to oppose. In instances where, after vigorously exploring possible ways to enhance the members' support for posting CIP standards documents for industry comment or balloting, and the Team finds that 100% acceptance or support of the members present is not achievable, decisions to adopt standards documents for balloting will require at least 2/3rds favorable vote of all members present and voting.

Quorum Defined. The Team will make decisions only when a quorum is present. A quorum shall be constituted by at least 2/3 of the appointed members being present in person or by telephone.

Electronic Mail Voting. Electronic voting will only be used when a decision needs to be made between regular meetings under the following conditions:

- It is not possible to coordinate and schedule a conference call for the purpose of voting, or;
- Scheduling a conference call solely for the purpose of voting would be an unnecessary use of time and resources, and the item is considered a small procedural issue that is likely to pass without debate.

Electronic voting will not be used to decide on issues that would require a super majority vote or have been previously voted on during a regular meeting or for any issues that those with opposing views would feel compelled to want to justify and explain their position to other team members prior to a vote. The Electronic Voting procedure shall include the following four steps:

1. The SDT Chair or Vice-Chair in his absence will announce the vote on the SDT mailing list and include the following written information: a summary of the issue being voted on and the vote options; the reason the electronic voting is being conducted; the deadline for voting (which must be at least 4 hours after the time of the announcement).
2. Electronic votes will be tallied at the time of the deadline and no further votes will be counted. If quorum is not reached by the deadline then the vote on the proposal will not pass and the deadline will not be extended.
3. Electronic voting results will be summarized and announced after the voting deadline back to the SDT+ mailing list.
4. Electronic voting results will be recapped at the beginning of the next regular

meeting of the SDT.

Consensus Building Techniques and Robert's Rules of Order. The Team will develop its recommendations using consensus-building techniques with the leadership of the Chair and Vice Chair and the assistance of the facilitators. Techniques such as brainstorming, ranking and prioritizing approaches will be utilized. The Team's consensus process will be conducted as a facilitated consensus-building process. Only Team members may participate in consensus ranking or votes on proposals and recommendations. Observers/members of the public are welcome to speak when recognized by the Chair, Vice Chair or Facilitator. The Team will utilize Robert's Rules of Order *(as per the NERC Reliability Standards Development Procedure),* as modified by the Team's adopted procedural guidelines, to make and approve motions. However, the 2/3's voting requirement will supersede the normal voting requirements used in Robert's Rules of Order for decision-making on substantive motions and amendments to motions. The Team will develop substantive written materials and options using their adopted facilitated consensus-building procedures, and will use Robert's Rules of Order only for formal motions once the Chair determines that a facilitated discussion is completed.

Project 2008-06 Cyber Security Order 706 SDT
32nd Meeting Agenda
March 15, 2011 Tuesday - 8:00 AM to 6:00 PM EST
March 16, 2011 Wednesday - 8:00 AM to 6:00 PM EST
March 17, 2011 Thursday - 8:00 AM to 6:00 PM EST
Con Edison
4 Irving Place, New York, NY 10003

NOTE: Agenda Times May be Adjusted as Needed during the Meeting

Proposed Meeting Objectives/Outcomes:

- To review and assess CIP V5 multiple standard format (CIP-002 – CIP-00X)
- To finalize concepts and number of impact levels
- To finalize concepts on minimum requirements and drafting level of requirements
- To review and refine CIP Version 5 BES Cyber System identification and security requirements
- To agree on next steps and assignments

Timed Agenda

Tuesday March 15, 2011 8:00 a.m. - 6:00 p.m. EST

8:00 a.m.	**Introduction, Welcome Opening and Host remarks**- *John Lim, Chair & Phil Huff, Vice Chair,* Roll Call; NERC Antitrust Compliance Guidelines- *Howard Gugel, NERC*
8:15	**Review of meeting objectives and Agenda**- *John Lim*
8:20	**Industry Review**- *Scott Mix, NERC, Mike Keane, FERC and others* o Cyber Attack TF Report o CIPC Report o CIP-005-4 Update o Other Cyber Security business
8:50	**Review of CIP V5 Multiple Standard Format** – *John Lim*
10:00	*Break*
10:15	**Discussion on CIP-002-5 impact levels**
12:00	*Lunch*
1:00	**Discussion on minimum requirements for all BES Cyber Systems**
3:00	*Break*
3:15	**Discussion on level of requirements (high level or detailed/prescriptive, environment, communication protocol)**
5:50	**Review any Drafting Assignments and Wednesday's agenda**
6:00	*Recess*

Project 2008-06 Cyber Security Order 706 SDT
32nd Meeting Agenda
March 15, 2011 Tuesday - 8:00 AM to 6:00 PM EST
March 16, 2011 Wednesday - 8:00 AM to 6:00 PM EST
March 17, 2011 Thursday - 8:00 AM to 6:00 PM EST
Con Edison
4 Irving Place, New York, NY 10003

NOTE: Agenda Times May be Adjusted as Needed during the Meeting

Proposed Meeting Objectives/Outcomes:

- To review and assess CIP V5 multiple standard format (CIP-002 – CIP-00X)
- To finalize concepts and number of impact levels
- To finalize concepts on minimum requirements and drafting level of requirements
- To review and refine CIP Version 5 BES Cyber System identification and security requirements
- To agree on next steps and assignments

Wednesday February 16, 2011 8:00 a.m. - 6:00 p.m. EST

8:00 a.m.	**Welcome and Agenda Review, Roll Call and Antitrust Guidelines** – *John Lim, Philip Huff, Howard Gugel*
8:15	**Review Project Schedule –** *Philip Huff*
8:40	**Review and Refine BES Cyber System Identification (CIP-002-5)** – *John Lim*
10:00	*Break*
10:15	***Continue,* Review and Refine BES Cyber System Identification**
12:00	*Lunch*
1:00	**Review modifications to style guide for security requirements –** *Philip Huff*
1:30	**Review and Refine CIP-003-5 (Security Policy, Change Management, Information Protection and Maintenance Requirements) –** *Dave Revill, Georgia Transmission*
3:00	*Break*
3:15	***Continue,* Review and Refine CIP-003-5 (Security Policy, Change Management, Information Protection and Maintenance Requirements)**
3:30	**Review and Refine CIP-004-5 (Personnel) and CIP-006-5 (Physical Security Requirements) –** *Doug Johnson, ComEd*
5:50	**Review any Drafting Assignments and Thursday's agenda**
6:00	*Recess*

Project 2008-06 Cyber Security Order 706 SDT
32nd Meeting Agenda
March 15, 2011 Tuesday - 8:00 AM to 6:00 PM EST
March 16, 2011 Wednesday - 8:00 AM to 6:00 PM EST
March 17, 2011 Thursday - 8:00 AM to 6:00 PM EST
Con Edison
4 Irving Place, New York, NY 10003

NOTE: Agenda Times May be Adjusted as Needed during the Meeting

Proposed Meeting Objectives/Outcomes:

- To review and assess CIP V5 multiple standard format (CIP-002 – CIP-00X)
- To finalize concepts and number of impact levels
- To finalize concepts on minimum requirements and drafting level of requirements
- To review and refine CIP Version 5 BES Cyber System identification and security requirements
- To agree on next steps and assignments

Thursday February 17, 2011 8:00 a.m. - 6:00 p.m. CST

8:00 a.m.	**Welcome and Agenda Review, Roll Call and Antitrust Guidelines** – *John Lim, Philip Huff, Howard Gugel*
8:15	**Review and Refine CIP-004-5 (Electronic Access Control Requirements)** – *Sharon Edwards, Duke Energy*
10:00	*Break*
10:15	**Review and Refine CIP-005-4 and CIP-007-4 (System and Boundary Protection Requirements) –** *Jay Cribb, Southern Company*
12:00	*Lunch*
1:00	**Review and Refine (CIP-008-5) Response and CIP-009-4 (Recovery Requirements) –** *Scott Rosenberger, Future Holdings*
3:00	*Break*
3:15	**Review project schedule and agree to next steps**
4:30	**Review Communication Plan –** *Howard Gugel/Joe Bucciero*
5:00	**Review SDT April 2011 Sacramento, CA (SMUD) Meeting**
6:00	*Adjourn*

Cyber Security Order 706 Standard Drafting Team (Project 2008-06)

Chairman	John Lim, CISSP Department Manager, IT Infrastructure Planning	Consolidated Edison Co. of New York 4 Irving Place Rm 349-S New York, New York 10003	(212) 460-2712 (212) 387-2100 Fx limj@coned.com
Vice Chairman	Philip Huff Security Analyst	Arkansas Electric Cooperative Corporation 1 Cooperative Way Little Rock, Arkansas 72119	(501) 570-2444 phuff@aecc.com
Members	Robert Antonishen Protection and Control Manager, Hydro Engineering Division	Ontario Power Generation Inc. 14000 Niagara Parkway Niagara-on the-Lake, Ontario L0S 1J0	(905) 262-2674 (905)262-2686 Fx rob.antonishen@ opg.com
	Jim Brenton, CISSP-ISSAP Principal, Regional Security Coordinator	Electric Reliability Council of Texas, Inc. 2705 WCST Lake Drive Taylor, Texas 76574	(512) 248-3043 (512) 248-3993 Fx jbrenton@ ercot.com
	Jay S. Cribb Information Security Analyst, Principal	Southern Company Services, Inc. 241 Ralph McGill Boulevard N.E. Bin 10034 Atlanta, Georgia 30308	(404) 506-3854 jscribb@ southernco.com
	Joe Doetzl Manager, Information Security	Kansas City Power & Light Co. 1201 Walnut Kansas City, Missouri 64106	(816) 556-2280 joe.doetzl@ kcpl.com
	Sharon Edwards Project Manager	Duke Energy 139 E. 4th Streets 4th & Main Cincinnati, Ohio 45202	(513) 287-1564 (513) 508-1285 Fx sharon.edwards@ duke-energy.com
	Gerald S. Freese Director, NERC CIP Compliance	American Electric Power 1 Riverside Plaza Columbus, Ohio 43215	(614) 716-2351 (614) 716-1144 Fx gsfreese@aep.com
	Jeffrey Hoffman Chief Architect, IT Policy and Security Division	U.S. Bureau of Reclamation Denver Federal Center Bldg. 67, Rm 380 P.O. Box 25007 (84-21200) Denver, CO 80225	(303) 445-3341 jhoffman@usbr.gov
	Doug Johnson Operations Support Group Transmission Operations & Planning	Exelon - Commonwealth Edison 1N301 Swift Road Lombard, IL 60148	(630) 691-4593 douglas.johnson@ comed.com

	Richard Kinas Manager of Standards Compliance	Orlando Utilities Commission 6113 Pershing Avenue Orlando, Florida 32822	(407) 384-4063 rkinas@ouc.com
	David S Revill Manager, Cyber Security Operations	Georgia Transmission Corporation 2100 East Exchange Place Tucker, Georgia 30084	(770) 270-7815 david.revill@ gatrans.com
	Scott Rosenberger Director, Security and Compliance	Luminant 500 North Akard Dallas, Texas 75201	(214) 812-2412 Scott.Rosenberger@ energyfutureholdings.com
	Kevin Sherlin Manager, Business Technology Operations	Sacramento Municipal Utility District 6201 S Street Sacramento, California 95817	(916) 732-6452 csherli@smud.org
	Thomas Stevenson General Supervisor Engineering Projects	Constellation Energy 1005 Brandon Shores Rd Baltimore, MD 21226	(410) 787-5260 (410) 227-3728 Thomas.W.Stevenson@ constellation.com
	Keith Stouffer Program Manager, Industrial Control System Security	National Institute of Standards & Technology 100 Bureau Drive Mail Stop 8230 Gaithersburg, Maryland 20899-8230	(301) 975-3877 (301) 990-9688 keith.stouffer@nist.gov
	John Van Boxtel	Portland General Electric 121 SouthwCST Salmon Street Portland, Oregon 97204	(503) 464-7093 (503) 317-2464 john.vanboxtel@pgn.com
	John D. Varnell Director, Asset Operations Analysis	Tenaska Power Services Co. 1701 East Lamar Blvd. Arlington, Texas 76006	(817) 462-1037 (817) 462-1035 jvarnell@tnsk.com
	William Winters IS Senior Systems Consultant	Arizona Public Service Co. 502 S. 2nd Avenue Mail Station 2387 Phoenix, Arizona 85003	(602) 250-1117 William.Winters@ aps.com
NERC Staff	Tom Hofstetter Regional Compliance Auditor	North American Electric Reliability Corporation 116-390 Village Boulevard Princeton, New Jersey 08540-5721	(609) 452-8060 (609) 452-9550 fax tom.hofstetter@ nerc.net
NERC Staff	Roger Lampila Regional Compliance Auditor	North American Electric Reliability Corporation 116-390 Village Boulevard Princeton, New Jersey 08540-5721	(609) 452-8060 (609) 452-9550 fax roger.lampila@ nerc.net
NERC Staff	Scott R Mix Manager Infrastructure Security	North American Electric Reliability Corporation 116-390 Village Boulevard Princeton, New Jersey 08540-5721	(215) 853-8204 (609) 452-9550 fax Scott.Mix@ nerc.net

NERC Staff	Howard Gugel Standards Development Coordinator	North American Electric Reliability Corporation 116-390 Village Boulevard Princeton, New Jersey 08540-5721	(609) 651-2269 howard.gugel@nerc.net

CSO706 SDT
Meeting Schedule and Objectives

Meeting Location	Dates	Meeting Objective
Columbus, OH AEP	01/18 to 01/20/2011	Full review of CIP-011 requirements in response to industry comment (first of several development iterations for posting in late June)
Interim	1/20 to 2/15/2011	Designated individuals complete drafting assignments on CIP-011
Taylor, TX ERCOT	2/15 to 2/17/2011	Begin review of CIP-010, BES Cyber System Identification Full review of CIP-011 (requirements, measures, change rationale, guidance)
Interim	2/17 to 3/15/2011	Designated individuals complete drafting assignments on CIP-010 and CIP-011 Begin developing implementation plan
New York, NY ConEd	3/15 to 3/17/2011	Review of CIP V5 (requirements, measures, change rationale, guidance) Initial review of implementation plan
Interim	3/17 to 4/12/2011	Designated individuals complete drafting assignments on CIP V5 and implementation plan
Sacramento, CA SMUD	4/12 to 4/14/2011	Review of CIP V5 and implementation plan
Interim	4/14 to 5/17/2011	Designated individuals complete drafting assignments on CIP V5 and implementation plan Sneak peak industry webinar in early May
Little Rock, AR AECC	5/17 to 5/19/2011	Review of industry feedback Review of change rationale and guidance
Interim	5/19 to 6/21/2010	Designated individuals complete drafting assignments on CIP V5 and implementation plan NERC begins QA

Meeting Location	Dates	Meeting Objective
????????	6/21 to 6/23/2011	SDT and NERC QA on document for posting
Interim	6/23 to 7/19/2011	Posting for comment Prepare for technical workshop?
TBD	7/19 to 7/21/2011	Technical Workshop?
TBD	8/23 to 8/25/2011	Respond to comments
TBD	9/20 to 9/22/2011	Respond to comments and prepare for second posting and ballot
TBD	10/11 to 10/13	

CSO 706 SDT DRAFTING SUB-TEAMS

Sub-Team	
CIP 010 BES System Categorization	John Lim (Lead), Rich Kinas, Jim Brenton *(Observer Participants: Rod Hardiman, Jim Fletcher, Dave Burtrum)* *(FERC: Mike Keane, Peter Kuebeck)*
Personnel and Physical Security	Doug Johnson (Lead), Rob Antonishen, Kevin Sherlin *(FERC: Drew Kittey)*
System Security and Boundary Protection	Jay Cribb (Lead), John Varnell, John Van Boxtel, Philip Huff *(Observer Participant: Brian Newell)* *(FERC: Justin Kelly)*
Incident Response and Recovery	Scott Rosenberger (Lead), Joe Doetzl, Tom Stevenson (*Observer Participant: Jason Marshall)* *(FERC: Dan Bogle)*
Access Control	Sharon Edwards (Lead), Jeff Hoffman, Jerry Freese *(Observer Participants: Roger Fradenburgh, Sam Merrell)* *(FERC: Mike Keane)*
Change Management, System Lifecycle, Information Protection, Maintenance, and Governance	Dave Revill (Lead), Jon Stanford, Keith Stouffer, Bill Winters *(Observer Participant: Brian Newell)* *(FERC: Jan Bargen, Matthew Dale)*
Framework CIP 010 &011	Jay Cribb (Lead), Joe Doetzl, Phil Huff, Doug Johnson, Dave Norton, Dave Revill, Jon Stanford and John Van Boxtel. Mike Keane FERC and Scott Mix, NERC

NEED, GOALS AND OBJECTIVES – PROJECT 2008-06 - CIP CYBER SECURITY STANDARDS V5 – ADOPTED JANUARY 2011

NEED

The need for Critical Infrastructure Protection (CIP) in North America has never been more compelling or necessary than it is today. This is especially true of the electricity sector. Electric power is foundational to our social and economic fabric, acknowledged as one of the most essential and among the most targeted of all the interrelated critical infrastructure sectors.

The Bulk Electric System (BES) is a complex, interconnected collection of facilities that increasingly uses standard cyber technology to perform multiple functions essential to grid reliability. These BES Cyber Systems provide operational efficiency, intercommunications and control capability. They also represent an increased risk to reliability if not equipped with proper security controls to decrease vulnerabilities and minimize the impact of malicious cyber activity.

Cyber attacks on critical infrastructure are becoming more frequent and more sophisticated. Stuxnet is a prime example of an exploit with the potential to seriously degrade and disrupt the BES with highly malicious code introduced via a common USB interface. Other types of attacks are network or Internet-based, requiring no physical presence and potentially affecting multiple facilities simultaneously. It is clear that attack vectors are plentiful, but many exploits are preventable. The common factors in these exploits are vulnerabilities in BES Cyber Systems. The common remedy is to mitigate those vulnerabilities through application of readily available cyber security measures, which include prevention, detection, response and recovery.

In the cyber world, security is truly only as good as its weakest implementation. The need to identify BES Cyber Systems and then protect them through effective cyber security measures are critical steps in helping ensure the reliability of the BES functions they perform.

In approving Version 1 of CIP Standards CIP-002-1 through CIP-009-1, FERC issued a number of directives to the ERO. Versions 2, 3 and 4 addressed the short term standards-related and Critical Asset identification issues from these directives. There are still a number of unresolved standards-related issues in the FERC directives that must be addressed. This version is needed to address these remaining directives in FERC Order 706.

GOALS AND OBJECTIVES

- **Goal 1:** To address the remaining Requirements-related directives from all CIP related FERC orders, all approved interpretations, and CAN topics within applicable existing requirements.
    - **Objective 1.** Provide a list of each directive with a description and rationale of how each has been addressed.
    - **Objective 2.** Provide a list of approved interpretations to existing requirements with a description of how each has been addressed.
    - **Objective 3.** Provide a list of CAN topics with a description of how each has been addressed.
    - **Objective 4.** Consider established security practices (e.g. DHS, NIST) when developing requirements.
    - **Objective 5.** Incorporate the work of Project 2010-15 Urgent Action SAR.
- **Goal 2:** To develop consistent identification criteria of BES Cyber Systems and application of cyber security requirements that are appropriate for the risk presented to the BES.
    - **Objective 6**: Transition from a Critical Cyber Asset framework to a BES Cyber System framework.
    - **Objective 7.** Develop criteria to identify and categorize BES Cyber Systems, leveraging industry approved bright-line criteria in CIP-002-4.
    - **Objective 8.** Develop appropriate cyber security requirements based on categorization of BES Cyber Systems.
    - **Objective 9.** Minimize writing requirements at the device specific level, where appropriate.
- **Goal 3:** To provide guidance and context for each Standard Requirement
    - **Objective 10.** Use the Results-Based Standards format to provide rationale statements and guidance for all of the Requirements.

- **Objective 11.** Develop measures that describe specific examples that may be used to provide acceptable evidence to meet each requirement. These examples are not all inclusive ways to provide evidence of compliance, but provide assurance that they can be used by entities to show compliance.
- **Objective 12.** Work with NERC and regional compliance and enforcement personnel to review and refine measures.

- **Goal 4:** To leverage current stakeholder investments used for complying with existing CIP requirements.
  - **Objective 13.** Map each new requirement to the requirement(s) in the prior version from which the new requirement was derived.
  - **Objective 14.** Justify change in each requirement which differs from the prior version.
  - **Objective 15.** Minimize changes to requirements which do not address a directive, interpretation, broad industry feedback or do not significantly improve the Standards.
  - **Objective 16.** Justify any other changes (e.g. removals, format)
- **Goal 5:** To minimize technical feasibility exceptions.
  - **Objective 17.** Develop requirements at a level that does not assume the use of specific technologies.
  - **Objective 18.** Allow for technical requirements to be applied more appropriately to specific operating environments (i.e. Control Centers, Generation Facilities, and Transmission Facilities). (also maps to Goal 2)
  - **Objective 19.** Allow for technical requirements to be applied more appropriately based on connectivity characteristics. (also maps to Goal 2)
  - **Objective 20.** Ensure that the words "where technically feasible" exist in appropriate requirements.
- **Goal 6:** To develop requirements that foster a "culture of security" and due diligence in the industry to compliment a "culture of compliance".
  - **Objective 21.** Work with NERC Compliance Staff to evaluate options to reduce compliance impacts such as continuous improvement processes, performance based compliance processes, or SOX-like evaluation methods.
  - **Objective 22.** Write each requirement with the end result in mind, (minimizing the use of inclusive phrases such as "every device," "all devices," etc.)
  - **Objective 23.** Minimize compliance impacts due to zero-defect requirements.

- **Goal 7:** To develop a realistic and comprehensible implementation plan for the industry.
    - **Objective 24.** Avoid per device, per requirement compliance dates**.**
    - **Objective 25.** Address complexities of having multiple versions of the CIP standards in rapid succession.
    - **Objective 26.** Consider implementation issues by setting realistic timeframes for compliance.
    - **Objective 27.** Rename and modify IPFNICCAANRE to address BES Cyber System framework.

CYBER SECURITY FOR ORDER 706 STANDARD DRAFTING TEAM

CSO 706 SDT Consensus Guidelines*)*

(Adopted, November, 2008, Revised June 2010, Revised July, 2010)

The Cyber Security for Order 706 Standard Drafting Team (Team) will seek consensus on its recommendations for any revisions to the CIP standards.

Consensus Defined. Consensus is a participatory process whereby, on matters of substance, the Team strives for agreements which all of the members can accept, support, live with or agree not to oppose. In instances where, after vigorously exploring possible ways to enhance the members' support for posting CIP standards documents for industry comment or balloting, and the Team finds that 100% acceptance or support of the members present is not achievable, decisions to adopt standards documents for balloting will require at least 2/3rds favorable vote of all members present and voting.

Quorum Defined. The Team will make decisions only when a quorum is present. A quorum shall be constituted by at least 2/3 of the appointed members being present in person or by telephone.

Electronic Mail Voting. Electronic voting will only be used when a decision needs to be made between regular meetings under the following conditions:

- It is not possible to coordinate and schedule a conference call for the purpose of voting, or;
- Scheduling a conference call solely for the purpose of voting would be an unnecessary use of time and resources, and the item is considered a small procedural issue that is likely to pass without debate.

Electronic voting will not be used to decide on issues that would require a super majority vote or have been previously voted on during a regular meeting or for any issues that those with opposing views would feel compelled to want to justify and explain their position to other team members prior to a vote. The Electronic Voting procedure shall include the following four steps:

1. The SDT Chair or Vice-Chair in his absence will announce the vote on the SDT mailing list and include the following written information: a summary of the issue being voted on and the vote options; the reason the electronic voting is being conducted; the deadline for voting (which must be at least 4 hours after the time of the announcement).
2. Electronic votes will be tallied at the time of the deadline and no further votes will be counted. If quorum is not reached by the deadline then the vote on the proposal will not pass and the deadline will not be extended.
3. Electronic voting results will be summarized and announced after the voting deadline back to the SDT+ mailing list.
4. Electronic voting results will be recapped at the beginning of the next regular

meeting of the SDT.

Consensus Building Techniques and Robert's Rules of Order. The Team will develop its recommendations using consensus-building techniques with the leadership of the Chair and Vice Chair and the assistance of the facilitators. Techniques such as brainstorming, ranking and prioritizing approaches will be utilized. The Team's consensus process will be conducted as a facilitated consensus-building process. Only Team members may participate in consensus ranking or votes on proposals and recommendations. Observers/members of the public are welcome to speak when recognized by the Chair, Vice Chair or Facilitator. The Team will utilize Robert's Rules of Order *(as per the NERC Reliability Standards Development Procedure),* as modified by the Team's adopted procedural guidelines, to make and approve motions. However, the 2/3's voting requirement will supersede the normal voting requirements used in Robert's Rules of Order for decision-making on substantive motions and amendments to motions. The Team will develop substantive written materials and options using their adopted facilitated consensus-building procedures, and will use Robert's Rules of Order only for formal motions once the Chair determines that a facilitated discussion is completed.