BEFORE THE
RÉGIE DE L'ÉNERGIE
THE PROVINCE OF QUÉBEC

NORTH AMERICAN ELECTRIC	**)**
RELIABILITY CORPORATION	**)**

NOTICE OF FILING OF THE NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION OF CRITICAL INFRASTRUCTURE PROTECTION RELIABILITY STANDARDS VERSION 5

Gerald W. Cauley
President and Chief Executive Officer
North American Electric Reliability Corporation
3353 Peachtree Road, N.E.
Suite 600, North Tower
Atlanta, GA 30326
(404) 446-2560
(404) 446-2595– facsimile

Charles A. Berardesco
Senior Vice President and General Counsel
Holly A. Hawkins
Assistant General Counsel
Willie L. Phillips
Attorney
North American Electric Reliability Corporation
1325 G Street, N.W., Suite 600
Washington, D.C. 20005
(202) 400-3000
(202) 644-8099– facsimile
charlie.berardesco@nerc.net
holly.hawkins@nerc.net
willie.phillips@nerc.net

Counsel for North American Electric Reliability Corporation

February 7, 2013

TABLE OF CONTENTS

BEFORE THE
RÉGIE DE L'ÉNERGIE
THE PROVINCE OF QUÉBEC

NORTH AMERICAN ELECTRIC)
RELIABILITY CORPORATION)

NOTICE OF FILING OF THE NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION OF CRITICAL INFRASTRUCTURE PROTECTION RELIABILITY STANDARDS VERSION 5

The North American Electric Reliability Corporation ("NERC") hereby provides notice of the following ten proposed Critical Infrastructure Protection ("CIP") Reliability Standards ("CIP Version 5"), as they are just, reasonable, not unduly discriminatory or preferential and in the public interest:

- CIP–002–5 — Cyber Security — BES Cyber System Categorization
- CIP–003–5 — Cyber Security — Security Management Controls
- CIP–004–5 — Cyber Security — Personnel and Training
- CIP–005–5 — Cyber Security — Electronic Security Perimeter(s)
- CIP–006–5 — Cyber Security — Physical Security of BES Cyber Systems
- CIP–007–5 — Cyber Security — Systems Security Management
- CIP–008–5 — Cyber Security — Incident Reporting and Response Planning
- CIP–009–5 — Cyber Security — Recovery Plans for BES Cyber Systems
- CIP–010–1 — Cyber Security — Configuration Change Management and Vulnerability Assessments
- CIP–011–1 — Cyber Security — Information Protection

NERC also provides notice of the proposed definitions of terms used in the proposed CIP Version 5, the associated implementation plan, and the proposed Violation Risk Factors

("VRFs") and Violation Severity Levels ("VSLs").[1] This filing also addresses all remaining standards-related issues and directives from Federal Energy Regulatory Commission ("FERC") Order No. 706.[2]

CIP Version 5 will become effective as provided in the Implementation Plan. The requested effective date: (1) is just and reasonable; (2) properly balances the urgency to implement the standards with time allowed to develop necessary procedures, software, facilities, staffing or other relevant capabilities; and (3) allows applicable entities adequate time to ensure compliance with the requirements.

After a successful industry ballot with the CIP Version 5 standards achieving approval ranging from to 78.59% to 95.67%, the NERC Board of Trustees approved the CIP Version 5 standards and related documents on November 26, 2012.

Exhibit A to this filing sets forth the proposed CIP Version 5 standards and associated modifications to the Glossary of Terms used in NERC Reliability Standards. **Exhibit B** contains the Implementation Plan for CIP Version 5. **Exhibit C** contains the Standard Drafting Team Roster for Project 2008-06 Cyber Security Order 706, which is the technical team responsible for developing CIP Version 5. **Exhibit D** contains the Consideration of Comments Reports for CIP Version 5. **Exhibit E** contains a table of CIP Version 5 VRFs and VSLs proposed for approval and Commission guideline analyses. **Exhibit F** contains the development record for CIP Version 5. **Exhibit G** addresses the Order No. 672 Criteria for Approving Proposed Reliability Standards. **Exhibit H** contains the Consideration of Issues and Directives.

---

[1] Unless otherwise specified, capitalized terms used herein have the meanings specified in the *NERC Glossary of Terms*, available at: http://www.nerc.com/files/Glossary_of_Terms.pdf.

[2] *Mandatory Reliability Standards for Critical Infrastructure Protection*, Order No. 706, 122 FERC ¶ 61,040, *denying reh'g and granting clarification*, Order No. 706-A, 123 FERC ¶ 61,174 (2008), *order on clarification*, Order No. 706-B, 126 FERC ¶ 61,229 (2009), *order denying clarification*, Order No. 706-C, 127 FERC ¶ 61,273 (2009) ("Order No. 706").

NERC filed the proposed CIP Version 5 standards and associated documents, and is also filing the proposed CIP Version 5 standards and associated documents with the other applicable governmental authorities in Canada.

I. EXECUTIVE SUMMARY

Taking into consideration four years of experience since the first NERC CIP Cyber Security Reliability Standards were implemented, NERC developed the proposed CIP Version 5 standards to better protect the reliability of the nation's Bulk Electric System ("BES")[3] from cyber-attacks.

The proposed CIP Version 5 standards were overwhelmingly supported by industry, with the industry ballot averaging nearly 90% approval. The standards also present a significant improvement over the existing CIP Version 3[4] and the CIP Version 4 standards.[5]

With respect to concerns expressed by Responsible Entities regarding the transition from CIP Version 3 to Version 4 to Version 5 Reliability Standards, NERC understands that the transition could be complicated. For this reason, NERC stands ready to work with industry to address transition issues as they arise.

The proposed implementation plan for CIP Version 5, included with this filing as **Exhibit B,** provides language that would allow entities to transition from CIP Version 3 to CIP Version 5, thereby bypassing implementation of CIP Version 4 completely. The proposed implementation plan specifically states:

[3] In this petition, the terms "Bulk Power System" and "Bulk Electric System" are used interchangeably. "Bulk Electric System" is defined in the NERC Glossary of Terms, and generally includes facilities operated at voltages at and above 100 kV. *See* NERC Glossary of Terms Used in Reliability Standards at 2. "Bulk-Power System" is defined in section 215 of the FPA, and does not include a voltage threshold. *See* 16 U.S.C. 824o(a)(1).
[4] CIP Version 3 Reliability Standards were filed on January 21, 2010.
[5] CIP Version 4 Reliability Standards were filed on June 8, 2011 (Noting CIP Version 4 Implementation date of April 1, 2014).

> Notwithstanding any order to the contrary, CIP-002-4 through CIP-009-4 do not become effective, and CIP-002-3 through CIP-009-3 remain in effect and are not retired until the effective date of the Version 5 CIP Cyber Security Standards under this implementation plan.

To help the industry implement the CIP Version 4 and 5 standards, NERC will initiate a series of industry workshops that will be presented across North America beginning in 2013.

The improvements included in CIP Version 5 reflect a maturity of the NERC CIP program. While the general framework of the proposed standards follow the organization of the previous CIP versions, a new process is introduced in proposed CIP-002-05 for identifying and classifying BES Cyber Systems according to "Low-Medium-High" impact.[6] Once BES Cyber Systems are identified, a Responsible Entity must then comply with proposed CIP-003-5 to CIP-011-1, according to specific criteria relating to impact and other characteristics such as communications connectivity. As such, NERC and its stakeholders have proposed the most comprehensive set of mandatory cybersecurity standards ever utilized on a widespread basis in the electric industry.

Key features of the comprehensive approach taken in CIP Version 5 include:

- Utilizing a National Institute of Standards and Technology ("NIST") based approach to categorize all cyber systems which impact the BES as "Low-Medium-High" (at the system level) and requiring at least a minimum classification of "Low Impact" for all BES Cyber Systems.
- Building on the implementation experience from prior CIP Reliability Standard versions.
- Addressing all applicable directives in FERC Order No. 706.
- Eliminating unnecessary documentation requirements to allow entities to focus on the reliability and security of the Bulk Power System.
- Providing guidance and context within each CIP Version 5 standard.

[6] BES Cyber Systems, discussed herein, is a proposed addition to the *Glossary of Terms used in NERC Reliability Standards*.

The identification of cyber assets has evolved through the various CIP Reliability Standards versions. Building on the prior "Risk-Based Assessment Methodology" in CIP-002-3 and the "Bright-line Criteria" in CIP-002-4, the proposed CIP Version 5 standards focus on all cyber system assets that have an impact on Bulk Power System reliability, and characterizes that impact as either high, medium or low.

In Order No. 761, FERC directed NERC to file CIP Version 5 addressing all remaining directives from Order No. 706, by March 31, 2013. With the strong support of industry, and the efforts of the diverse standard drafting team, this filing satisfies FERC's directives.

II. NOTICES AND COMMUNICATIONS

Notices and communications with respect to this filing may be addressed to the following:

Gerald W. Cauley
President and Chief Executive Officer
North American Electric Reliability Corporation
3353 Peachtree Road, N.E.
Suite 600, North Tower
Atlanta, GA 30326
(404) 446-2560
(404) 446-2595– facsimile

Charles A. Berardesco
Senior Vice President and General Counsel
Holly A. Hawkins
Assistant General Counsel
Willie L. Phillips
Attorney
North American Electric Reliability Corporation
1325 G Street, N.W., Suite 600
Washington, D.C. 20005
(202) 400-3000
(202) 644-8099– facsimile
charlie.berardesco@nerc.net
holly.hawkins@nerc.net
willie.phillips@nerc.net

III. JUSTIFICATION OF THE PROPOSED RELIABILITY STANDARDS

In this section we will discuss the following: a) the basis of the proposed Reliability Standards; b) significant improvements to previous CIP standards; c) new proposed Reliability

Standards CIP-010-1and CIP-011-1; d) proposed definitions of glossary terms used in CIP Version 5; e) enforceability of the proposed CIP Version 5; f) VRF and VSL assignments; and g) NERC Reliability Standards Development Procedure.

This section summarizes the development of proposed CIP Version 5 and demonstrates that the proposed modifications and enhancements provided in CIP Version 5 ensure that the proposed standards are just, reasonable, not unduly discriminatory or preferential and in the public interest.

The proposed CIP Version 5 standards, which were overwhelmingly approved by industry, are a significant improvement over the existing CIP standards and help protect the reliability of the BES.

a. Basis of Proposed Reliability Standards

The technical expertise of the ERO is derived from a standards drafting team consisting of participants that are considered experts in the cybersecurity arena. The members of the CIP Version 5 standard drafting team also provided a diversity of experience, ranging across North America, including both the continental United States and Canada. Detailed biographical information for each of the members is included with the standards drafting team roster in **Exhibit C**.

The proposed CIP Version 5 serves the important reliability goal of providing a cybersecurity framework for the identification and protection of BES Cyber Systems (discussed below) to support the reliable operation of the Bulk Power System. Generally, the framework of CIP Version 5 can be divided into two groups:

1) Categorization of risk (based on "Low-Medium-High" impact to BES reliability)

- CIP–002–5 — BES Cyber System Categorization

2) Risk mitigation lifecycle (implement, evaluate, monitor, and update)

- CIP–003–5 — Security Management Controls
- CIP–004–5 — Personnel and Training
- CIP–005–5 — Electronic Security Perimeter(s)
- CIP–006–5 — Physical Security of BES Cyber Systems
- CIP–007–5 — Systems Security Management
- CIP–008–5 — Incident Reporting and Response Planning
- CIP–009–5 — Recovery Plans for BES Cyber Systems
- CIP–010–1 — Configuration Change Management and Vulnerability Assessments
- CIP–011–1 — Information Protection

The proposed CIP Version 5 takes a more comprehensive approach to categorizing risk, and requires Responsible Entities to identify BES Cyber Systems, but generally maintains the cybersecurity protection framework contained in previous CIP versions. Key features of the comprehensive approach taken in CIP Version 5 include:

- Utilizing a NIST-based approach to categorize all cyber systems which impact the BES as "Low-Medium-High" (at the system level) and requiring at least a minimum classification of "Low Impact" for all BES Cyber Systems.
- Building on the implementation experience from prior CIP versions.
- Addressing all applicable directives in FERC Order No. 706.
- Eliminating unnecessary documentation requirements to allow entities to focus on the reliability and security of the Bulk Power System.
- Providing guidance and context within each CIP Version 5 standard.

The proposed CIP-002-5 Reliability Standard is the first step in identifying BES Cyber Systems. If a Responsible Entity does not identify any BES Cyber Systems – that ends the compliance review under proposed CIP-003-5 to CIP-011-1. However, a Responsible Entity that identifies BES Cyber Systems must comply with proposed CIP-003-5 to CIP-011-1, according to specific criteria that characterize the impact of the identified BES Cyber Systems.

Specifically, as discussed and analyzed in detail below, proposed CIP Version 5 uses CIP-002-5 "Attachment 1 – Impact Rating Criteria" to identify three categories of BES Cyber

Systems: 1) the High Impact category that covers large Control Centers, similar to those control centers identified as Critical Assets in CIP-002-4; 2) the Medium Impact category that covers generation and transmission facilities, similar to those identified as Critical Assets in CIP-002-4, along with other control centers not identified as Critical Assets in CIP-002-4; and 3) the Low Impact category that covers all other BES Cyber Systems. In addition, the Low Impact category provides protections for systems not included in CIP Version 4 (*i.e.*, CIP-002-4).

Generally, modifications to the existing CIP Reliability Standards included in the proposed CIP Version 5 standards can be described as follows:

- **CIP-002-5** will require the identification and categorization of BES Cyber Systems according to specific criteria that characterize their impact for the application of cyber security requirements commensurate with the adverse impact that loss, compromise, or misuse of those BES Cyber Systems could have on the reliable operation of the BES.

- **CIP-003-5** will require approval of the documented cybersecurity policies related to CIP-004-5 through CIP-009-5, CIP-010-1, and CIP-011-1. CIP-003-5, Requirement 2, will require implementation of programmatic controls related to cybersecurity awareness, physical security controls, electronic access controls, and incident response to a Cyber Security Incident for those assets that have low impact BES Cyber Systems according to CIP-002-5's categorization process. The requirement that a Cyber Security Policy be "readily available" has been deleted because of general confusion around that term and because training requirements in CIP-004-5 provide for knowledge of policy. Several portions of requirements related to information protection in previous CIP versions have been moved to CIP-011-1 and therefore deleted from CIP-003-5.

- **CIP-004-5** will require documented processes or programs for security awareness, cyber security training, personnel risk assessment, and access management. In Requirement R2, CIP-004-5 adds specific training roles for visitor control programs, electronic interconnectivity supporting the operation and control of BES Cyber Systems, and storage media as part of the handling of BES Cyber System Information. The requirements surrounding personnel risk assessments and access management were modified in response to lessons learned from implementing previous versions. Proposed CIP-004-5, Requirement R3, now specifies that the seven year criminal history check covers all locations where the individual has resided for six consecutive months or more without specifying school, work, etc., and regardless of official residence. In Requirement R4, the primary change was in combining the access management requirements from CIP-003-4, CIP-004-4, CIP-

006-4 and CIP-007-4 into a single requirement. The requirements from Version 4 remain largely unchanged except to clarify some terminology. The purpose for combining these requirements is to improve consistency in the authorization and review process. The requirement in CIP-004-4 Requirement R4 to maintain a list of authorized personnel has been removed because the list represents only one form of evidence to demonstrate compliance that only authorized persons have access. Requirement R5 specifies revocation of access for a termination action concurrent with termination, to be completed within 24 hours.

- **CIP-005-5**, Requirement R1, focuses more on the discrete Electronic Access Points rather than the logical "perimeter." CIP-005-1 through CIP-005-4's Requirement R1.2 has been deleted from CIP Version 5. This requirement was definitional in nature and was used to bring dial-up modems using non-routable protocols into the scope of previous versions of CIP-005. The non-routable protocol exclusion no longer exists as a blanket CIP-002 filter for applicability in CIP Version 5; therefore, there is no need for this requirement. CIP-005-1 through CIP-005-4's Requirements R1.1 and R1.3 were also definitional in nature, and they have been deleted from Version 5 as separate requirements; however, the concepts were integrated into the definitions of Electronic Security Perimeter ("ESP") and Electronic Access Point ("EAP"). CIP-005-5, Requirement R2, related to interactive remote access, is a new requirement to continue the efforts of the NERC Urgent Action team for Project 2010-15: Expedited Revisions to CIP-005-3.

- **CIP-006-5** is intended to manage physical access to BES Cyber Systems by specifying a physical security plan to protect BES Cyber Systems against compromise that could lead to misoperation or instability. CIP-006-4, Requirements R8.2 and R8.3, concerning the retention of testing records, has been removed, and the retention period is specified in the compliance section of CIP-006-5.

- **CIP-007-5** will address system security by specifying technical, operational, and procedural requirements in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability of the BES. CIP-007-5 is modified in several places to conform to the formatting approach of CIP Version 5, along with changes to address several Commission directives and to make the requirements less dependent on specific technology so that they will remain relevant for future, yet-unknown developing technologies (for example, in Requirement R3, the requirement is a competency-based requirement where the Responsible Entity must document how the malware risk is handled for each BES Cyber System, but the requirement does not prescribe a particular technical method in order to account for potential technological advancement).

- **CIP-008-5** will mitigate the risk to the reliable operation of the BES as the result of a Cyber Security Incident by specifying incident response requirements. Proposed Requirement R1 now includes an obligation to report Cyber Security Incidents within 1 hour of recognition. Requirement R2 adds testing requirements to verify response plan effectiveness and consistent application in responding to a Cyber Security

Incident. Requirement R3 includes provisions for an after-action review for tests or actual incidents, along with a requirement to update the Cyber Security Incident response plan based on those lessons learned. In Requirement R3, a single timeline now combines several timelines for concurrent activities related to lessons learned and updates to recovery plans in previous CIP versions, although the total time to complete the related activities remains the same. Additionally, where previous CIP versions specified "30 calendar days" for performing lessons learned, followed by additional time for updating recovery plans and notification, this requirement combines those activities into a single timeframe.

- **CIP-009-5** is intended to recover reliability functions performed by BES Cyber Systems by specifying recovery plan requirements in support of the continued stability, operability, and reliability of the BES. Requirement R1, adds provisions to protect data that would be useful in the investigation of an event that results in the need for a Cyber System recovery plan to be utilized. Requirement R2 adds operational testing for recovery of BES Cyber Systems. In Requirement R3, timelines for several concurrent activities related to lessons learned and updates to recovery plans in previous versions were combined to provide one timeline, similar to CIP-009-5.

- **CIP-010-1** is a new standard that consolidates the configuration change management and vulnerability assessment-related requirements from previous versions of CIP-003, CIP-005 and CIP-007. Requirement R1 specifies the configuration change management requirements, Requirement R2 specifies the configuration monitoring requirements intended to detect unauthorized modifications to BES Cyber Systems, and Requirement R3 specifies the vulnerability assessment requirements intended to ensure proper implementation of cyber security controls along with promoting continuous improvement of cyber security posture.

- **CIP-011-1** is a new standard that consolidates the information protection requirements from previous versions of CIP-003 and CIP-007. Requirement R1 specifies information protection requirements to prevent unauthorized access to BES Cyber System Information. Requirement R2 specifies reuse and disposal provisions intended to prevent unauthorized dissemination of protected information.

All ten of the proposed CIP Version 5 standards provide a comprehensive set of requirements to protect the BES from malicious cyber-attacks. Because there are unique aspects of cyber protection for each Responsible Entity and its assets, proposed CIP Version 5 requires Bulk Power System owners, operators, and users to identify and categorize BES Cyber Systems (which are comprised of BES Cyber Assets) as described in the proposed new defined terms provided below:

BES Cyber Asset

A Cyber Asset that if rendered unavailable, degraded, or misused would, within 15 minutes of its required operation, misoperation, or non-operation, adversely impact one or more Facilities, systems, or equipment, which, if destroyed, degraded, or otherwise rendered unavailable when needed, would affect the reliable operation of the Bulk Electric System. Redundancy of affected Facilities, systems, and equipment shall not be considered when determining adverse impact. Each BES Cyber Asset is included in one or more BES Cyber Systems. (A Cyber Asset is not a BES Cyber Asset if, for 30 consecutive calendar days or less, it is directly connected to a network within an ESP, a Cyber Asset within an ESP, or to a BES Cyber Asset, and it is used for data transfer, vulnerability assessment, maintenance, or troubleshooting purposes.)

BES Cyber System

One or more BES Cyber Assets logically grouped by a responsible entity to perform one or more reliability tasks for a functional entity.

As noted, once Responsible Entities identify BES Cyber Systems, the CIP Version 5 requirements are then applied according to the impact that loss, compromise, or misuse of those BES Cyber Systems could have on the reliable operation of the BES, in accordance with proposed CIP-002-5.

Additionally, proposed CIP Version 5 requires responsible entities to establish plans, protocols, and controls to safeguard physical and electronic access (CIP-003-5 – CIP-011-1), to train personnel on security matters (CIP-004-5), to report security incidents (CIP-008-5), and to be prepared for recovery actions (CIP-009-5).[7]

[7] The extensive development record includes successive drafts of the CIP Reliability Standards, the ballot pool, the final ballot results by registered ballot body members, and stakeholder comments received during the development of the proposed standards, as well as a discussion regarding how those comments were considered in developing them.

b. CIP Version 5 presents significant improvements to previous CIP standards.

Modifying CIP-002-5 to require responsible entities to use a new approach to categorize all cyber systems impacting the BES as "Low-Medium-High" is the most significant improvement to the existing CIP Reliability Standards. This new approach effectively moves away from the CIP Version 4 "bright-line" approach of only identifying Critical Assets (and applying CIP requirements only to their associated Critical Cyber Assets), to requiring a minimum classification of "Low Impact" for all BES Cyber Systems.[8]

The shift to identifying and categorizing "High-Medium-Low" BES Cyber Systems (according to their impact on the BES) resulted from a review of the NIST Risk Management Framework for categorizing and applying security controls, a review that was directed by FERC in Order No. 706.[9]

The following discussion is an analysis of each of the criterion included in Attachment 1 used to determine impact categories of BES Cyber Systems.

> **Criterion 1. High Impact Rating (H)**
> Each BES Cyber System used by and located at any of the following:
>
> **1.1.** Each Control Center or backup Control Center used to perform the functional obligations of the Reliability Coordinator.
>
> **1.2.** Each Control Center or backup Control Center used to perform the functional obligations of the Balancing Authority: 1) for generation equal to or greater than an aggregate of 3000 MW in a single Interconnection, or 2) for one or more of the assets that meet criterion 2.3, 2.6, or 2.9.
>
> **1.3.** Each Control Center or backup Control Center used to perform the functional obligations of the Transmission Operator for one or more of the assets that meet criterion 2.2, 2.4, 2.5, 2.7, 2.8, 2.9, or 2.10.
>
> **1.4.** Each Control Center or backup Control Center used to perform the functional obligations of the Generator Operator for one or more of the assets that meet criterion 2.1, 2.3, 2.6, or 2.9.

[8] Proposed CIP-003-5 through CIP-009-5 are consistent with the organization of CIP Versions 1 through 4.
[9] Order No. 706 at P 25.

The High Impact rating category generally includes those BES Cyber Systems used by and at Control Centers that perform the functional obligations of the Reliability Coordinator ("RC"), Balancing Authority ("BA"), Transmission Operator ("TOP"), or Generator Operator ("GOP"), as defined under the NERC Functional Model.[10]

Based on stakeholder comments, the standards drafting team made significant changes to Attachment 1, Criteria 1.1 to 1.4. Specifically, the standards drafting team tailored the definition of Control Center to refer to real-time reliability tasks for applicable functional entities from the functional model, which includes those necessary for situational awareness.

During the development process, one commenter noted that the proposed High Impact rating criteria do not consider the inter-connected nature of the BES Cyber Assets or BES Cyber Systems when defining threshold-based criteria. The standards drafting team responded that using inter-connections as an impact criterion ultimately scopes in all inter-connected systems in a single impact level. In addition, the standards drafting team recognized the concept of security zones, used heavily in the NIST Risk Management Framework, which allows the implementation of cybersecurity controls commensurate with the level of impact within a security boundary.

For proposed CIP Version 5, BES Cyber Systems of all impact levels, with routable or dial-up connectivity, are required to be within a security zone that provides protection from outside influences using a posture of "mutual distrust". As such, no communication crossing the perimeter is trusted, regardless of where that communication originates. Therefore, BES Cyber Systems at High, Medium, and Low impact levels would be required to implement electronic perimeter protections for all routable and dial-up communications, regardless of inter-connectivity.

[10] NERC Reliability Functional Model, available at: http://www.nerc.com/page.php?cid=2%7C247%7C108.

The 3,000 MW threshold in criterion 1.2 and the corresponding 1,500 MW threshold in criterion 2.13 for Control Centers performing BA functions were based on the NERC 2012 Control Performance Standard 2 Bounds Report.[11] This report lists the estimated peak demand for each BA, and the standards drafting team determined that a 3,000 MW and 1,500 MW threshold would capture roughly 90% and 96%, respectively, of the peak demand.

Criterion 2. Medium Impact Rating (M)
Each BES Cyber System, not included in Section 1 above, associated with any of the following:

2.1. Commissioned generation, by each group of generating units at a single plant location, with an aggregate highest rated net Real Power capability of the preceding 12 calendar months equal to or exceeding 1500 MW in a single Interconnection. For each group of generating units, the only BES Cyber Systems that meet this criterion are those shared BES Cyber Systems that could, within 15 minutes, adversely impact the reliable operation of any combination of units that in aggregate equal or exceed 1500 MW in a single Interconnection.

2.2. Each BES reactive resource or group of resources at a single location (excluding generation Facilities) with an aggregate maximum Reactive Power nameplate rating of 1000 MVAR or greater (excluding those at generation Facilities). The only BES Cyber Systems that meet this criterion are those shared BES Cyber Systems that could, within 15 minutes, adversely impact the reliable operation of any combination of resources that in aggregate equal or exceed 1000 MVAR.

2.3. Each generation Facility that its Planning Coordinator or Transmission Planner designates, and informs the Generator Owner or Generator Operator, as necessary to avoid an Adverse Reliability Impact in the planning horizon of more than one year.

2.4. Transmission Facilities operated at 500 kV or higher. For the purpose of this criterion, the collector bus for a generation plant is not considered a Transmission Facility, but is part of the generation interconnection Facility.

2.5. Transmission Facilities that are operating between 200 kV and 499 kV at a single station or substation, where the station or substation is connected at 200 kV or higher voltages to three or more other Transmission stations or substations and has an "aggregate weighted value" exceeding 3000 according to the table below. The "aggregate weighted value" for a single station or substation is determined by summing the "weight value per line" shown in the table below for each incoming

[11] NERC, *2012 CPS2 Bounds*, available at: http://www.nerc.com/docs/oc/rs/2012%20CPS2%20Bounds%20Report%20Final(Update20120419).pdf.

and each outgoing BES Transmission Line that is connected to another Transmission station or substation. For the purpose of this criterion, the collector bus for a generation plant is not considered a Transmission Facility, but is part of the generation interconnection Facility.

Voltage Value of a Line	Weight Value per Line
less than 200 kV (not applicable)	(not applicable)
200 kV to 299 kV	700
300 kV to 499 kV	1300
500 kV and above	0

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

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

2.8. Transmission Facilities, including generation interconnection Facilities, providing the generation interconnection required to connect generator output to the Transmission Systems that, if destroyed, degraded, misused, or otherwise rendered unavailable, would result in the loss of the generation Facilities identified by any Generator Owner as a result of its application of Attachment 1, criterion 2.1 or 2.3.

2.9. 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 or cause a reduction in one or more IROLs if destroyed, degraded, misused, or otherwise rendered unavailable.

2.10. Each system or group of Elements that performs automatic Load shedding under a common control system, without human operator initiation, of 300 MW or more implementing undervoltage load shedding (UVLS) or underfrequency load shedding (UFLS) under a load shedding program that is subject to one or more requirements in a NERC or regional reliability standard.

2.11. Each Control Center or backup Control Center, not already included in High Impact Rating (H) above, used to perform the functional obligations of the Generator Operator for an aggregate highest rated net Real Power capability of the preceding 12 calendar months equal to or exceeding 1500 MW in a single Interconnection.

2.12. Each Control Center or backup Control Center used to perform the functional obligations of the Transmission Operator not included in High Impact Rating (H), above.

2.13. Each Control Center or backup Control Center, not already included in High Impact Rating (H) above, 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.

- **Generation – Criteria 2.1, 2.3, 2.6, 2.9, 2.11, and 2.13 (Medium Impact Rating)**

Criteria 2.1, 2.3, 2.6, 2.9, and 2.11 of Attachment 1's Medium Impact rating category apply to Generation Owners ("GOs") and Generation Operators ("GOPs"). Criterion 2.13 is applicable to Balancing Authority ("BA") Control Centers.

Criterion 2.1 designates as Medium Impact those BES Cyber Systems that Medium Impact generation with a net Real Power capability exceeding 1500 MW. The 1500 MW criterion is sourced partly from the Contingency Reserve requirements in NERC Reliability Standard BAL-002, whose purpose is to ensure the BA is able to utilize its Contingency Reserve to balance resources and demand, and return Interconnection frequency within defined limits following a Reportable Disturbance.

In Criterion 2.3, the standards drafting team sought to ensure that BES Cyber Systems for those generation Facilities that have been designated by the Planning Coordinator or Transmission Planner as necessary to avoid BES Adverse Reliability Impacts in the planning horizon of one year or more are categorized as medium impact.

Criterion 2.6 includes BES Cyber Systems for those Generation Facilities that have been identified as critical to the derivation of Interconnection Reliability Operating Limits ("IROLs") and their associated contingencies, as specified by FAC-014-2, Establish and Communicate System Operating Limits, R5.1.1 and R5.1.3.

Criterion 2.9 categorizes BES Cyber Systems for Special Protection Systems ("SPS") and Remedial Action Schemes ("RAS") as medium impact. SPS and RAS's may be implemented to prevent disturbances that would result in exceeding IROLs if they do not provide the function required at the time it is needed or if it operates outside of the designed parameters. GOs and GOPs that own BES Cyber Systems for such Systems and schemes designate them as Medium Impact.

Criterion 2.11 categorizes as Medium Impact BES Cyber Systems used by and at Control Centers that perform the functional obligations of the Generator Operator for an aggregate generation of 1500 MW or higher in a single interconnection, and that have not been included in Part 1. The 1500 MW threshold omits facilities that have little impact on BES reliability, but would otherwise be captured under the newly defined term for Control Center.

Criterion 2.13 categorizes as Medium Impact those BA Control Centers that "control" 1500 MW of generation or more in a single interconnection and that have not already been included in Part 1. The 1500 MW threshold is consistent with the impact level and rationale specified for Criterion 2.1.

- **Transmission – Criteria 2.2, 2.4, 2.5, 2.6, 2.7, 2.8, 2.9, 2.10, and 2.12 (Medium Impact Rating)**

Criteria 2.2, 2.4 through 2.10, and 2.12 in Attachment 1 are applicable to Transmission Owners and Operators.

Criterion 2.2 includes BES Cyber Systems for those Facilities in Transmission Systems that provide reactive resources to enhance and preserve the reliability of the BES. The nameplate value is used here because there is no NERC requirement to verify actual capability of these Facilities. The 1000 MVARs value used in this criterion was a value deemed reasonable

for the purpose of determining criticality by the standards drafting team. Criterion 2.2 is consistent with the criteria in CIP Version 4.

Criterion 2.4 includes BES Cyber Systems for any Transmission Facility at a substation operated at 500 kV or higher, because these are single facility locations and would not have the same overall grid impact as higher rated Control Centers. Criterion 2.4 is consistent with the criteria in CIP Version 4.

It should be noted that if the collector bus for a generation plant, which is smaller in aggregate than the threshold set for generation in Criterion 2.1, is operated at 500kV, the collector bus should be considered a Generation Interconnection Facility, and not a Transmission Facility, according to the "Final Report from the Ad Hoc Group for Generation Requirements at the Transmission Interface."[12] However, such a collector bus would not be considered Medium Impact because it does not significantly affect the 500kV Transmission grid; it only affects a plant which is below the generation threshold.

Criterion 2.5 includes BES Cyber Systems for facilities at the mid-range of BES Transmission with qualifications for inclusion if they are deemed highly likely to have significant impact on the BES. While the criterion has been specified as part of the rationale for requiring protection for significant impact on the BES, the standards drafting team included, in this criterion, additional qualifications that would ensure the required level of impact to the BES. The standards drafting team:

- Excluded radial facilities that would only provide support for single generation facilities.
- Specified interconnection to at least three transmission stations or substations to ensure that the level of impact is consistent with a medium categorization.

[12] NERC, *Final Report from the Ad Hoc Group for Generation Requirements at the Transmission Interface* (Nov. 16, 2009), available at: http://www.nerc.com/files/GO-TO_Final_Report_Complete_2009Nov16.pdf.

The standard drafting team sought to: a) ensure inclusion of BES Transmission Facilities that perform high impact BES reliability operations, including those in large geographical areas where such Facilities operate above 200 kV, but below 300 kV; and b) provide a threshold based on existing technical studies that would be applicable to Facilities operating in the range of 200 kV to 499 kV (primarily 230 kV and 345 kV Facilities).

The total aggregated weighted value of 3,000 (utilized in criterion 2.5) was derived from weighted values related to three connected 345 kV lines or five connected 230 kV lines at a transmission station or substation. The total aggregated weighted value is used to account for the true impact to the BES, without taking into account the line kV rating and a mix of multiple kV rated lines. This is in contrast to the similar criterion in CIP Version 4, which used a simple count of the lines above a certain voltage level.

Criterion 2.6 include BES Cyber Systems for those Transmission Facilities that have been identified as critical to the derivation of IROLs and their associated contingencies, as specified by FAC-014-2, Establish and Communicate System Operating Limits, R5.1.1 and R5.1.3.

Criterion 2.7 is sourced from the NUC-001 Reliability Standard, Requirement R9.2.2, for the support of Nuclear Facilities. NUC-001 ensures that reliability of the Nuclear Plant Interface Requirements ("NPIRs") is harmonized through adequate coordination between the Nuclear Generator Owner/Operator and its Transmission Service Provider "for the purpose of ensuring nuclear plant safe operation and shutdown."[13] In particular, there are specific requirements to coordinate physical and cyber security protection of these interfaces.

[13] NERC Reliability Standard NUC-001-2.1 — Nuclear Plant Interface Coordination, available at: http://www.nerc.com/page.php?cid=2|20.

Criterion 2.8 designates as Medium Impact those BES Cyber Systems that impact Transmission Facilities necessary to directly support generation that meet the criteria in Criteria 2.1 (generation Facilities with output greater than 1500 MW) and 2.3 (generation Facilities generally designated as "must run" for wide area reliability in the planning horizon). The Responsible Entity can request a formal statement from the Generation Owner as to the qualification of generation Facilities connected to their Transmission systems.

Criterion 2.9 designates as Medium Impact those BES Cyber Systems for those SPS, RAS, or automated switching Systems installed to ensure BES operation within IROLs. The degradation, compromise or unavailability of these BES Cyber Systems would result in exceeding IROLs if they fail to operate as designed. By the definition of IROL, the loss or compromise of any of these have Wide Area impacts.[14]

Criterion 2.10 designates as Medium Impact those BES Cyber Systems for systems or Elements that perform automatic Load shedding, without human operator initiation, of 300 MW or more. The standards drafting team sought to include only those Systems that did not require human operator initiation, and targeted in particular those underfrequency load shedding ("UFLS") systems and undervoltage load shedding ("UVLS") systems that would be subject to a regional Load shedding requirement to prevent Adverse Reliability Impact. These include automated UFLS systems or UVLS systems that are capable of Load shedding 300 MW or more.

Criterion 2.12 categorizes as Medium Impact those BES Cyber Systems used by and at Control Centers performing the functional obligations of a Transmission Operator and that have not already been categorized as high impact. Because Control Center is a defined term, Criterion 2.12 is only applicable to the extent that a Control Center meets the standard set in the proposed definition. Control Centers that are used to perform certain functional obligations of a

[14] NERC Glossary of Terms at p. 63.

Transmission Operator are categorized as high impact under criterion 1.3. All other Control Centers used to perform the functional obligations of the Transmission Operator, not otherwise categorized as high impact, are categorized as Medium Impact under Criterion 2.12.

Criterion 2.13 categorizes as Medium Impact those BA Control Centers that "control" 1500 MW of generation or more in a single Interconnection. The 1500 MW threshold is consistent with the impact level and rationale specified for Criterion 2.1.

> **Criterion 3. Low Impact Rating (L)**
>
> BES Cyber Systems not included in Sections 1 or 2 above that are associated with any of the following assets and that meet the applicability qualifications in Section 4 - Applicability, part 4.2 – Facilities, of this standard:
>
> **3.1.** Control Centers and backup Control Centers.
>
> **3.2.** Transmission stations and substations.
>
> **3.3.** Generation resources.
>
> **3.4.** Systems and facilities critical to system restoration, including Blackstart Resources and Cranking Paths and initial switching requirements.
>
> **3.5.** Special Protection Systems that support the reliable operation of the Bulk Electric System.
>
> **3.6.** For Distribution Providers, Protection Systems specified in Applicability section 4.2.1 above.

- **Restoration Facilities (Low Impact Rating)**

Criterion 3 would require that all remaining BES Cyber Systems (not included under Criterion 1 or Criterion 2) be designated as Low Impact. For example, under Criterion 3.4, restoration facilities are considered as Low Impact. However, such an assignment will not relieve asset owners of all CIP-related responsibilities, as would have been the case under CIP-002-4 (since only Cyber Assets with routable connectivity which are essential to restoration

assets are included in CIP Version 4). With the Low Impact categorization, restoration facilities will be protected in the areas of cybersecurity awareness, physical security controls, and electronic access control, and will have obligations under CIP-003-5 regarding incident response to Cyber Security Incidents.

Restoration facilities are needed in the event of a partial or complete shutdown of facilities not used for daily activities. Notably, EPAct 2005 does not authorize NERC or FERC to order the construction of additional generation facilities.[15] Thus, consistent with EPAct 2005, assigning a Low Impact rating to restoration facilities appropriately balances the need for timely restoration response with focused requirements for these particular types of facilities.[16]

In addition, there is no mandatory requirement that a Responsible Entity have specific restoration facilities essential to BES reliability, including Blackstart Resources and Cranking Paths. Therefore, it is imperative that NERC continues to promote availability of such resources.

- **Control Centers (Low Impact Rating)**

Under Criterion 3.1, certain Control Centers have been designated as Low Impact, according to the impact of the Control Centers on the reliability of the BES. During the development process, several commenters noted that the proposed definition for "Control Center" would include some facilities that had very little impact on BES reliability. For example, the Control Center for a BA with a scope of less than 1500 MW has a reliability impact similar to the control system managing a generating plant of roughly the same size. Since the generating plant control system does not meet the criteria to be classified as a Medium Impact BES Cyber System, it is inconsistent to require that the BA Control Center be held to a higher

[15] 16 USCS § 824o(i)(2).
[16] *See* Guidelines and Technical Basis section of CIP-002-5.

impact level solely because it is a Control Center. Still, at the Low Impact rating, there are requirements for electronic perimeter protections required in proposed CIP-003-5, and the concept of "mutual distrust" attaches even to Low Impact BES Cyber Systems, which utilize either routable or dial-up communications.

c. New Proposed Reliability Standards CIP-010-1and CIP-011-1.

Proposed CIP-010-1 is a new standard that contains the configuration change management and vulnerability assessment requirements previously defined across several CIP standards in prior versions. The purpose of CIP-010-1 is to prevent and detect unauthorized changes to BES Cyber Systems by specifying configuration change management and vulnerability assessment requirements in support of protecting BES Cyber Systems from compromise that could lead to misoperation or instability in the BES.

Similarly, proposed CIP-011-1 is a new standard that defines information protection requirements previously defined across many standards in previous versions. The purpose of CIP-011-1 is to prevent unauthorized access to BES Cyber System Information by specifying information protection requirements in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the BES.

d. Modifications to the Glossary of Terms used in NERC Reliability Standards

In proposed CIP Version 5, NERC also introduces 15 newly defined terms,[17] and makes modifications to four existing definitions in Glossary of Terms used in NERC Reliability

[17] 1) BES Cyber Asset, 2) BES Cyber System, 3) BES Cyber System Information, 4) CIP Exceptional Circumstance, 5) CIP Senior Manager, 6) Control Center, 7) Dial-up Connectivity, 8) Electronic Access Control or Monitoring Systems ("EACMS"), 9) Electronic Access Point ("EAP"), 10) External Routable Connectivity, 11) Intermediate System, 12) Physical Access Control Systems ("PACS"), 13) Protected Cyber Assets ("PCA"), 14) Interactive Remote Access, and 15) Reportable Cyber Security Incident.

Standards.[18] The newly defined terms reduce the variable application of many existing concepts from previous CIP versions. For example, the term "Control Center" is defined under CIP Version 5, although "control center" has been used since CIP Version 1 standards were submitted, and the term has been subject to differing interpretations by implementing entities.

e. Enforceability of the Proposed CIP Version 5 Reliability Standards

The proposed CIP Version 5 standards are designed to be clear and unambiguous. Indeed, CIP-002-05 was modified to address FERC directives in Orders No. 706. Proposed CIP-003-5 through CIP-009-5 are generally consistent with the organization of CIP Versions 1 through 4. New proposed standards CIP-010-1 and CIP-011-1 further enhance BES reliability.

In addition, the "Guidelines and Technical Basis" set forth in the CIP Version 5 standards provides Responsible Entities with sufficient information to understand their compliance obligations.

f. Violation Risk Factor and Violation Severity Level Assignments

CIP Version 4 VSLs and VRFs served as a basis for the new CIP Version 5 VRFs and VSLs. For those requirements from CIP Version 4 that were retained in CIP Version 5 (*see* mapping document included in **Exhibit F**) NERC provides a VRF and VSL Commission Guideline Analysis, included as **Exhibit E**. NERC also proposes several new VRFs and VSLs for CIP Version 5 standards developed using the FERC guidelines.

Detailed explanations for these VRF and VSL assignments are also included in the VRF and VSL Commission Guideline Analysis in **Exhibit E**.

[18] 1) Cyber Assets, 2) Cyber Security Incident, 3) Electronic Security Perimeter, and 4) Physical Security Perimeter. Available at: http://www.nerc.com/docs/standards/sar/CIP_V5_Definitions_clean_4_(2012-1024-1613).pdf.

g. NERC Reliability Standards Development Procedure

NERC develops Reliability Standards in accordance with Section 300 (Reliability Standards Development) of the NERC Rules of Procedure and the NERC Standard Processes Manual, which is Appendix 3A to the NERC Rules of Procedure. NERC's proposed rules provide for reasonable notice and opportunity for public comment, due process, openness, and a balance of interests in developing Reliability Standards and thus satisfies certain of the criteria for approving Reliability Standards.

The work culminating in this filing originated in FERC Order No. 706, which directed the ERO to develop modifications to Standard CIP-002-1 Cyber Security – Critical Cyber Asset Identification to address 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.[19]

Prior to the development of the proposed CIP Version 5 Reliability Standards, the standard drafting team developed the CIP-002-2 through CIP-009-2 standards to comply with the near-term, specific directives of FERC Order No. 706. That version of the standards was approved by FERC on September 30, 2009, with additional directives to be addressed within 90 days of the order.[20] In response, the standard drafting team developed the CIP-003-3 through CIP-009-3 standards, which were filed on January 21, 2010.

The standard drafting team for CIP Version 4 limited the scope of requirements in the development of CIP-002-4 through CIP-009-4 as an interim step to address the more immediate

[19] *Id.* at P 236.
[20] *Order Approving Revised Reliability Standards for Critical Infrastructure Protection and Requiring Compliance Filing*, 128 FERC ¶ 61,291 (September 30, 2009) ("September 30, 2009 Order").

concerns raised in Order No. 706.[21] CIP-002-4 included "bright-line criteria" used to identify Critical Assets in lieu of an entity-defined risk-based assessment methodology. On April 19, 2012, FERC issued Order No. 761 approving CIP Version 4. In that order, FERC also directed NERC to file the next version addressing all remaining directives from Order No. 706 by March 31, 2013.[22]

A phased approach to meeting the directives in FERC Order No. 706 has consistently built upon prior versions of the CIP-002 through CIP-009 standards to enhance the reliability of the Bulk Electric System. Accordingly, the proposed CIP Version 5 standards build on the CIP-002-4 establishment of uniform criteria for the identification of assets.

The standards development process is open to any person or entity with a legitimate interest in the reliability of the Bulk Power System. NERC considers the comments of all stakeholders, and a vote of stakeholders and the NERC Board of Trustees is required to approve a Reliability Standard before the Reliability Standard is submitted to the applicable governmental authorities. The proposed CIP Version 5 standards were approved by the NERC Board of Trustees on November 16, 2012.

IV. CIP VERSION 5 SATISFIES ALL FERC DIRECTIVES AND CONCERNS

FERC, in Order Nos. 706 and 761, approved prior versions the CIP standards and directed NERC to address numerous issues in future versions of the CIP standards. Specifically, in Order No. 761, FERC also directed NERC to consider the application of the NIST Risk Management Framework, regional perspective, and connectivity in developing CIP Version 5.

[21] *Version 4 Critical Infrastructure Protection Reliability Standards*, 139 FERC ¶ 61,058, at P 236 (2012) ("Order No. 761").
[22] Order No 761 at P 111.

As discussed below, proposed CIP Version 5 includes enhancements to the CIP standards that are responsive to all remaining FERC directives and concerns.

a. Order No. 706 Directives

In Order No. 761, FERC directed NERC to develop the CIP Version 5 standards to address all remaining directives from Order No. 706 by March 31, 2013.

> We recognize, as numerous commenters discuss, that the current schedule for completing CIP Version 5 is aggressive. We also understand that the volume of industry discussion is high and we agree that industry input should not be artificially rushed or curtailed. In its reply comments, NERC indicated that it anticipates filing the Version 5 CIP Reliability Standards by the third quarter of 2012. Accordingly, to allow for sufficient time beyond what NERC estimates, we establish a deadline that is 6 months from the end of the third quarter of 2012 (i.e., March 31, 2013). NERC must also submit reports at the beginning of each quarter in which the ERO is to explain whether it is on track to meet the deadline and describe the status of its standard development efforts."[23]

The proposed CIP Version 5 addresses all applicable FERC directives in Order No. 706, and **Exhibit H** provides a summary response for each of FERC's directives and guidance statements.

b. Application of NIST Risk Management Framework

In Order No. 706, FERC directed NERC to apply applicable features of the NIST Risk Management Framework to CIP Version 5. Order No. 761 also urged NERC to review relevant NIST standards for guidance in developing effective cybersecurity standards for the electric industry.[24]

Pursuant to Order Nos. 706 and 761, the standards drafting team for CIP Version 5 reviewed the NIST Risk Management Framework and incorporated five key features:

[23] Order No 761 at P 111.
[24] Order No. 761 at P 94 (The Commission stated: "We view the approach of incorporating these applicable features of the NIST Framework into the CIP Reliability Standards as a positive step in improving cyber security for the Bulk-Power System.").

1. ensuring that all BES Cyber Systems associated with the Bulk Power System, based on their function, receive some level of protection;

2. a tiered approach to security controls, which specifies the level of protection appropriate for systems based upon their importance to the reliable operation of the Bulk Power System;

3. tailoring protection to the mission and operating environment (*e.g.*, communications connectivity) of the cyber systems subject to protection;

4. the concept of the BES Cyber System, and

5. the inclusion of "Assess" and "Monitor" steps by adding requirement language for "identifying, assessing, and correcting" deficiencies in controls as part of the requirements' expected performance.

Proposed CIP Version 5 achieves reliability excellence by incorporating the above features of the NIST Risk Management Framework.[25] The NIST Risk Management Framework defines "risk" as a measure of the extent to which an entity is threatened by a potential circumstance or event, and a function of: (i) the adverse impacts that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence.[26] NIST further explains that this risk management process "changes the traditional focus of [Certification and Accreditation] as a static, procedural activity to a more dynamic approach that provides the capability to more effectively manage information system-related security risks in highly diverse environments of complex and sophisticated cyber threats, ever-increasing system vulnerabilities, and rapidly changing missions."[27]

[25] In 2013, NERC Compliance Operations will be revising all Reliability Standard Audit Worksheets ("RSAW"), including the RSAWs for CIP Version 5. To incorporate the NIST Risk Management Framework into CIP Version 5, the standards drafting team discussed the importance of synchronizing the "identify, assess, and correct" language with associated RSAWs, and developed a sample RSAW for proposed CIP-006-5. The sample RSAW was posted for informational purposes only and the Commission is *not* being asked to approve the sample RSAW, which is available at: http://www.nerc.com/page.php?cid=3|404.

[26] *Id*. at FN 8.

[27] NIST, Special Publication 800-37, *Guide for Applying the Risk Management Framework to Federal Information Systems, A Security Life Cycle Approach*, at p. 2.

Indeed, both NERC and FERC have acknowledged the importance of identifying and correcting risks to the Bulk Power System. NERC has stated in prior proceedings that, "Reliability excellence is achieved through the ongoing identification, correction and prevention of reliability ***risks***, both big and small. Yet, accountability for reliability excellence is broader than just penalizing violations."[28] In its order accepting NERC's Find, Fix, and Track approach to enforcement, FERC agreed with NERC's assessment, stating that it "applaud[s] NERC for proposing a format that will help it and the Regional Entities focus their resources on issues that pose the greatest ***risks*** to reliability."[29]

Consistent with the NIST Risk Management Framework and FERC's guidance in prior orders, the CIP Version 5 standard drafting team incorporated within several standards (***e.g.***, proposed CIP-003-5) a requirement that Responsible Entities implement cyber policies in a manner to "identify, assess, and correct" deficiencies. The "identify, assess, and correct" language is included as a performance expectation in the requirements, not as an enforcement component. An example of this language follows below:

> Each Responsible Entity shall implement**,** in a manner that identifies, assesses, and corrects deficiencies**,** one or more documented processes (or program, etc., as specified by the requirement) that collectively include each of the applicable items in [the referenced table].

The implementation of certain CIP Version 5 requirements in a manner to "identify, assess, and correct" deficiencies emulates the ***FERC Policy Statement on Penalty Guidelines***, where FERC clarified that "[a]chieving compliance, not assessing penalties, is the central goal of

---

[28] ***NERC Petition Requesting Approval of New Enforcement Mechanisms and Submittal of Initial Find Fix and Track (FFT) Informational Filing***, at p.1, Docket No. RC11-600 (2011) (***Emphasis added***).
[29] ***Order Accepting with Conditions the Electric Reliability Organization's Petition Requesting Approval of New Enforcement Mechanisms and Requiring Compliance Filing***, 138 FERC ¶61,193 (March 15, 2012) at P 40. (***Emphasis added***).

the Commission's enforcement efforts."[30] The *FERC Policy Statement on Penalty Guidelines* also highlights the characteristics of an effective organization compliance program, which include "(1) [exercising] due diligence to prevent and detect violations; and (2) [promoting] an organizational culture that encourages a commitment to compliance with the law."[31]

The *FERC Policy Statement on Penalty Guidelines* further explains that the promotion of an "organizational culture that encourages a commitment to compliance" requires an organization to establish standards and procedures to prevent and detect violations.[32] Therefore, the organization's governing authority should be knowledgeable of the compliance program and exercise reasonable oversight with respect to the implementation and effectiveness of the compliance program by assigning a specific individual(s) within high-level personnel overall responsibility for the compliance program. To that end, the *FERC Policy Statement on Penalty Guidelines* requires organizations to "periodically assess the ***risk*** of violations and shall take appropriate steps to design, implement, or modify each requirement set forth in subsection (b) to reduce the risk of violations identified through this process."[33]

This creation of an organizational culture of compliance, with an emphasis on assessing risk, is consistent with the approach taken in CIP Version 5 and avoids a "check-the-box" mind-set that would consume valuable industry resources without any benefit to BES reliability. For example, proposed CIP-003-5 requires Responsible Entities to identify a CIP Senior Manager. Rather than verifying that a single name appears on a document, CIP-003-5 seeks to verify that the ***purpose*** of the requirement is being achieved – that a CIP Senior Manager is indeed managing the implementation of CIP Version 5.

---

[30] *Revised Policy Statement on Penalty Guidelines*, 132 FERC ¶ 61,216 at P 110 (2010).
[31] *Id*.
[32] FERC Penalty Guidelines, Chapter 1, Part B - Disgorging Gain From Violations and Effective Compliance Program, §1B2.1, Effective Compliance Program.
[33] http://www.ferc.gov/whats-new/comm-meet/2010/091610/M-1.pdf. (*Emphasis added*).

This is an example of how the lessons learned over the past four years are reflected in CIP Version 5, which includes high-level personnel (*i.e.*, the CIP Senior Manager) assessing risk. Thus, CIP Version 5 builds on the implementation and audit lessons from prior versions and is consistent with the *FERC Policy Statement on Penalty Guidelines*.

c. Regional Perspective

In Order No. 761, FERC expressed a concern that a lack of a regional review for the identification of cyber assets might result in a reliability gap. However, CIP Version 4 adopted "bright-line" criteria for Critical Asset identification, which FERC agreed may obviate the need for a regional review.[34] Building on the CIP Version 4 approach, the proposed CIP-002-5, Attachment 1 – Impact Rating Criteria was developed in consideration of a Wide Area view and eliminates the need for regional review.

However, in the event that there are BES Cyber Systems that NERC and the Regional Entities determine should be treated as critical, but do not meet the CIP Version 5 criteria, NERC has the authority under Section 810 of the NERC Rules of Procedure to issue a Level 2 (Recommendation) or Level 3 (Essential Action) notification. Section 810 of the NERC Rules of Procedure provides the following:

> **810. Information Exchange and Issuance of NERC Advisories, Recommendations and Essential Actions**
>
> **1.** Members of NERC and Bulk Power System owners, operators, and users shall provide NERC with detailed and timely operating experience information and data.
>
> **2.** In the normal course of operations, NERC disseminates the results of its events analysis findings, lessons learned and other analysis and information gathering to the industry. These findings, lessons learned and

[34] Order No. 761 at P PP 103 and 104 ("We believe that there is less need for external review where application of bright line criteria results in an objective, consistently applied approach to the identification of cyber assets.").

other information will be used to guide the Reliability Assessment Program.

3. When NERC determines it is necessary to place the industry or segments of the industry on formal notice of its findings, analyses, and recommendations, NERC will provide such notification in the form of specific operations or equipment Advisories, Recommendations or Essential Actions:

> 3.1 Level 1 (Advisories) – purely informational, intended to advise certain segments of the owners, operators and users of the Bulk Power System of findings and lessons learned;
>
> 3.2 Level 2 (Recommendations) – specific actions that NERC is recommending be considered on a particular topic by certain segments of owners, operators, and users of the Bulk Power System according to each entity's facts and circumstances;
>
> 3.3 Level 3 (Essential Actions) – specific actions that NERC has determined are essential for certain segments of owners, operators, or users of the Bulk Power System to take to ensure the reliability of the Bulk Power System. Such Essential Actions require NERC Board approval before issuance.

4. The Bulk Power System owners, operators, and users to which Level 2 (Recommendations) and Level 3 (Essential Actions) notifications apply are to evaluate and take appropriate action on such issuances by NERC. Such Bulk Power System owners, operators, and users shall also provide reports of actions taken and timely updates on progress towards resolving the issues raised in the Recommendations and Essential Actions in accordance with the reporting date(s) specified by NERC.

5. NERC will advise the Commission and other Applicable Governmental Authorities of its intent to issue all Level 1 (Advisories), Level 2 (Recommendations), and Level 3 (Essential Actions) at least five (5) business days prior to issuance, unless extraordinary circumstances exist that warrant issuance less than five (5) business days after such advice. NERC will file a report with the Commission and other Applicable Governmental Authorities no later than thirty (30) days following the date by which NERC has requested the Bulk Power System owners, operators, and users to which a Level 2 (Recommendation) or Level 3 (Essential Action) issuance applies to provide reports of actions taken in response to the notification. NERC's report to the Commission and other Applicable Governmental Authorities will describe the actions taken by the relevant owners, operators, and users of the Bulk Power System and the success of such actions taken in correcting any vulnerability or deficiency that was

> the subject of the notification, with appropriate protection for Confidential Information or Critical Energy Infrastructure Information.

Level 3 Alerts allow NERC (following NERC Board of Trustees approval) to require that specific actions that NERC has determined are essential for certain segments of owners, operators, or users of the Bulk Power System be taken to ensure the reliability of the Bulk Power System. Additionally, Rule 810 states that Bulk Power System owners, operators, and users to which Level 2 (Recommendations) and Level 3 (Essential Actions) Alerts apply shall provide reports of actions taken and timely updates on progress towards resolving the issues raised in the Recommendations and Essential Actions consistent with reporting dates specified by NERC. Therefore, NERC can use Level 2 Recommendations and Level 3 Essential Actions to address assets that NERC and Regional Entities later determine should be treated as a higher impact level than would otherwise be categorized under the CIP Version 5 impact criteria.

d. Connectivity

In Order No. 761, FERC noted that the criteria adopted for the purpose of identifying assets under CIP-002-5 should include a cyber asset's "connectivity."[35]

> We also agree with SPP RE that the CIP Reliability Standards should consider communication paths between a given cyber asset and other assets that support a reliability function. As noted by SPP RE, cyber security standards that categorize cyber systems based upon the size or scope of the assets that they control "fail to consider the interconnectivity of the BES Cyber Systems and the potential for a small control center system to be used as a vector of attack against a larger control center system." …The Commission agrees that cyber connectivity is important to address when developing future versions of the CIP Reliability Standards. That being said, we acknowledge the concern of Trade Associations that the "connectivity" and "weakest link" concepts could possess different meanings to various stakeholders. Thus, addressing connectivity should include reaching a common understanding of the term. Further, we understand and agree with the Trade Associations' concern that protection should be applied in a reasonable manner.

[35] Order No. 761at PP 88 - 91.

Order No. 761at P 88. (Citations omitted).

The CIP Version 5 standards drafting team agreed with FERC that connectivity is a relevant consideration for the application of cybersecurity controls, and comprehensively incorporated connectivity throughout CIP Version 5 by utilizing a "mutual distrust" posture, by eliminating any connectivity-based exclusions under CIP-002-5, Attachment 1, and thorough inclusion of connectivity and other characteristics in the applicability of the CIP Version 5 requirements.

If connectivity were used as an initial impact criterion, it could potentially expand the CIP Version 5 standards to a significant number of non-jurisdictional assets, such as interconnected distribution systems (*e.g.*, smart grid), market systems, and business systems. Furthermore, using connectivity as a basis for categorizing impact could continue the unintended consequences related to eliminating connectivity in certain circumstances, resulting in a decreased situational awareness ability and increased costs associated with not being able to readily gather data or perform necessary maintenance. Accordingly, proposed CIP Version 5 addresses FERC's concerns related to connectivity throughout the proposed CIP Version 5 standards.

Specifically, the standards drafting team determined that, while connectivity may affect the ability to remotely access a BES Cyber System, the impact to BES reliability is determined by the electrical characteristics of a BES asset, not by the connectivity of an associated BES Cyber System. This does not, however, diminish the importance of connectivity, as the applicability of requirements consider connectivity in proposed CIP-003-5 through CIP-011-1.

Connectivity does not inform BES impact, even if it affects likelihood or risk. The role connectivity plays in affecting likelihood or risk of access or compromise to a Cyber Asset

associated with a BES Cyber System is a significant reason why connectivity is more appropriately considered in the applicability of requirements throughout the CIP Version 5 standards. To illustrate, the loss of 1000 MW of Load would have the same impact to the BES regardless of whether it stemmed from the compromise of an asset's BES Cyber System (that is routably connected) or from the compromise of an asset's BES Cyber System that has no connectivity whatsoever. The likelihood or risk of compromise to the former is arguably higher, but the impact to BES reliability—in the instant case, 1000 MW—would be the same under both circumstances. Indeed, the likelihood or risk of compromise *is* addressed by the applicability of additional requirements where routable connectivity is used, not by characterizing the BES Cyber System to a higher impact category.

In addition, Order No. 761 encourages NERC to consider the benefits of a "mutual distrust" posture as directed by FERC in Order No. 706.[36]

> Recognizing the importance of addressing cyber connectivity in future versions of the CIP Reliability Standards, we encourage NERC to consider the benefits of a "mutual distrust" posture, or similar strategies, put forth by the ISO/RTO Council and as directed by the Commission in Order No. 706. In Order No. 706, the Commission used the term "mutual distrust" to denote how "outside world" systems are treated by those inside the control system. Specifically, a mutual distrust posture requires each responsible entity that has identified critical cyber assets to protect itself and not trust any communication crossing an electronic security perimeter, regardless of where that communication originates.
>
> Applying electronic security perimeter protections "of some form" to bulk electric system cyber systems covered by the CIP Reliability Standards will support the adoption of a "mutual distrust" posture. This posture will encourage asset owners and operators to employ sound network architectural design, thus segmenting their systems into distinct security zones protected by managed interfaces that will allow only trusted access. The managed interfaces, or electronic security perimeter access points, are intended to restrict or prohibit network access and information flow to bulk electric system cyber systems covered by the CIP Reliability Standards from unidentified, unauthenticated, and unauthorized

[36] Order No. 761 at P 89.

> connectivity to ensure security. Multiple electronic security perimeters can be established to protect cyber assets and adopted as part of a defense in depth strategy to limit the propagation of a threat.

Order No. 761at PP 89-90. (Citations omitted).

"Mutual distrust" signifies how "external" cyber assets are treated by those cyber assets local to the BES Cyber System. "Mutual distrust" also requires each Responsible Entity that has identified BES Cyber Systems to protect against any communication crossing an ESP, regardless of where the communication originates. As noted above, BES Cyber Systems of all impact levels, with routable or dial-up connectivity, are required to be within a security zone that provides protection from outside influences using a posture of "mutual distrust". Since, under CIP Version 5, BES Cyber Systems for "High-Medium-Low" impact levels are now required to implement electronic perimeter protections "of some form" for all routable and dial-up communications, the "mutual distrust" posture is implemented for all BES Cyber Systems.

FERC also stated in Order No. 761 that, "we support the elimination of the blanket exemption for non-routable connected cyber systems as highlighted in NERC's comments. A continued blanket exemption in CIP Version 5 would not adequately address risk."[37] FERC added that, "we support the concept of applying electronic security perimeter protections 'of some form' to all bulk electric system cyber systems."[38]

The standards drafting team for CIP Version 5 agreed that applying ESP protections "of some form" to BES Cyber Systems supports the "mutual distrust" posture even for low impact BES Cyber Systems that use routable or dial-up communications.[39] Ultimately, using "mutual distrust" is equally efficient and effective as considering connectivity as a basis for informing the impact categorization of BES Cyber Systems. Thus, the implementation of a "mutual distrust"

[37] Order No. 761 at P 86.
[38] Order No. 761 at 87.
[39] Order No. 761 at 87.

posture for high, medium, and low impact BES Cyber Systems, connected using routable or dial-up communications, improves security above what is required under CIP Versions 1 through 4.

Moreover, in response to stakeholder comments during development, proposed CIP-003-5, requirement R2, was added so that Responsible Entities are required to document and implement perimeter-type security controls to segment Low Impact BES Cyber Systems from public (or other less trusted) network zones and to prevent access to an aggregation of low impact BES Cyber Systems. The intent of this enhancement is to mitigate the risks associated with the aggregation of Low Impact BES Cyber Systems, in order to avoid a potential increase in the overall level of impact to the BES.

Additionally, because electronic perimeter protections are now required for BES Cyber Systems (with specific requirements for High and Medium impact categories and programmatic requirements for Low impact) CIP Version 5 adequately addresses connectivity.

V. SUMMARY OF THE RELIABILITY STANDARD DEVELOPMENT PROCEEDINGS

The development record for proposed CIP Version 5 is summarized below. **Exhibit D** contains the Consideration of Comments Reports created during the development of the Reliability Standards. **Exhibit F** contains the complete record of development for proposed CIP Version 5.

Three drafts of CIP Version 5 were posted for industry comment during the development period before being approved during recirculation ballot in draft 4. The first draft of the standards was posted for comment from November 7, 2011, through January 6, 2012. This period included twelve initial ballots (one each for the ten standards in proposed CIP Version 5, the associated definitions, and the implementation plan) that were conducted from December 16,

2011, through January 6, 2012, and they resulted in industry approvals between 22.09 and 42.06 percent.[40]

The CIP Version 5 standards drafting team then focused its efforts on preparing the next draft in response to comments received. The second draft of CIP Version 5 was posted for comment from April 12 through May 21, 2012. This period included successive ballots that were conducted from May 11 through May 21, 2012, and resulted in industry approvals between 37.37 and 67.19 percent.[41]

The standards drafting team made further refinements in an effort to address unresolved issues and to develop industry consensus in response to the second posting. The third draft of CIP Version 5 was posted for comment from September 11 through October 10, 2012. This period included successive ballots that were conducted from October 1 through October 10, 2012, and they resulted in industry approvals between 74.85 and 94.00 percent.[42]

Recirculation ballots, which constituted draft four of CIP Version 5, were conducted from October 26 through November 5, 2012, and resulted in industry approvals between 78.59 and 95.53 percent.[43] The NERC Board of Trustees approved the proposed CIP Reliability Standards on November 16, 2012.

VI. CIP VERSION 5 IMPLEMENTATION PLAN

The proposed CIP Version 5 implementation plan was overwhelmingly passed by the registered ballot body with 94.91% approval. Yet, there may be uncertainty for Responsible Entities transitioning from CIP Version 3 to CIP Version 4 to CIP Version 5. This uncertainty

[40] http://www.nerc.com/docs/standards/sar/Standards_Announcement_2008-06_ballot_results_010612_final.pdf.
[41] http://www.nerc.com/docs/standards/sar/Succ_Ballot_Results_2008-06_CIPV5_20120522_060612.pdf.
[42] http://www.nerc.com/docs/standards/sar/Succ_Ballot_Results_2008-06_CIPV5_20121012_rev1.pdf.
[43] http://www.nerc.com/docs/standards/sar/2008-06_CIPV5_Recirc_NPB_Results_Announc_110712_final.pdf.

stems from industry stakeholders not knowing whether action will be taken on CIP Version 5 prior to the CIP Version 4 effective date, April 1, 2014, which would trigger compliance obligations for Responsible Entities.

NERC will work with the industry on any potential implementation challenges. However, language included in the proposed implementation plan could help alleviate some of the uncertainty among industry. This language provides:

> Notwithstanding any order to the contrary, CIP-002-4 through CIP-009-4 do not become effective, and CIP-002-3 through CIP-009-3 remain in effect and are not retired until the effective date of the Version 5 CIP Cyber Security Standards under this implementation plan.

With prompt approval of the CIP Version 5 standards and the associated implementation plan, CIP Version 3 will be extended until CIP Version 5 becomes operative, bypassing implementation of CIP Version 4.

While there is significant support for the CIP Version 5 implementation plan, NERC stands ready to implement CIP Version 4, if action is not taken before April 1, 2014. NERC will work with industry stakeholders to address any transition issues as they arise.

Prompt approval of CIP Version 5 will provide much needed clarity for Responsible Entities transitioning from CIP Version 3 to CIP Version 4 to CIP Version 5, and the improvements contained in CIP Version 5 will provide an enormous benefit to BES reliability. However, if prompt approval of CIP Version 5 is infeasible, a timeframe for anticipated action will be needed, so that NERC and industry may develop a reasonable plan to move from CIP Version 3 to CIP Version 4 to CIP Version 5.

Respectfully submitted,

/s/ Willie L. Phillips

Gerald W. Cauley
President and Chief Executive Officer
North American Electric Reliability Corporation
3353 Peachtree Road, N.E.
Suite 600, North Tower
Atlanta, GA 30326
(404) 446-2560
(404) 446-2595– facsimile

Charles A. Berardesco
Senior Vice President and General Counsel
Holly A. Hawkins
Assistant General Counsel
Willie L. Phillips
Attorney
North American Electric Reliability Corporation
1325 G Street, N.W., Suite 600
Washington, D.C. 20005
(202) 400-3000
(202) 644-8099– facsimile
charlie.berardesco@nerc.net
holly.hawkins@nerc.net
willie.phillips@nerc.net

Counsel for North American Electric Reliability Corporation

Dated: February 7, 2013

EXHIBITS A – F and EXHIBIT H

(Available on the NERC Website at

http://www.nerc.com/fileUploads/File/Filings/Attachments_CIP_V5_Filing_Ex_A-E

http://www.nerc.com/fileUploads/File/Filings/Attachments_CIP_V5_Filing_ExF_1

http://www.nerc.com/fileUploads/File/Filings/Attachments_CIP_V5_Filing_ExF_2

http://www.nerc.com/fileUploads/File/Filings/Attachments_CIP_V5_Filing_Ex_H)

EXHIBIT G – Demonstration that the proposed Reliability Standard is just, reasonable, not unduly discriminatory or preferential and in the public interest

1. Proposed Reliability Standards are designed to achieve a specified reliability goal and contain a technically sound means to achieve that goal.

The proposed CIP Version 5 provides a cyber security framework for the identification and protection of BES Cyber Systems to support the reliable operation of the BES. These standards recognize the differing roles of each entity in the operation of the BES, the criticality and vulnerability of the assets needed to manage BES reliability, and the risks to which they are exposed. Business and operational demands for maintaining a reliable BES increasingly rely on BES Cyber Systems to support 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 BES Cyber Systems.

2. Proposed Reliability Standards are applicable only to users, owners and operators of the Bulk Power System, and are clear and unambiguous as to what is required and who is required to comply.

The proposed CIP Version 5 is applicable to Reliability Coordinators, Balancing Authorities, Interchange Authorities, Transmission Owners, Transmission Operators, Generator Owners, Generator Operators, and Distribution Providers (collectively referred to as Responsible Entities). These entities are users, owners, or operators of the Bulk Power System.

The proposed CIP Version 5 standards achieve their stated goal of providing a cyber security framework for the identification and protection of BES Cyber Systems that support reliable operation of the BES. Specifically, proposed Reliability Standard CIP-002-5 requires the identification and documentation of BES Cyber Systems for the

application of cyber security requirements commensurate with the adverse impact that loss, compromise, or misuse of those BES Cyber Systems could have on the reliable operation of the BES. Identification and categorization of BES Cyber Systems support appropriate protection against compromises that could lead to misoperation or instability in the BES. These BES Cyber Systems are to be identified through the application of the criteria included in Attachment 1 of the proposed CIP-002-5 standard.

Requirement R1 requires a process for the consideration of certain assets for the identification of high impact and medium impact BES Cyber Systems, as specified under the impact criteria in Attachment 1, at each of those assets. It also requires identification of the assets that have Low Impact BES Cyber Systems. This will ensure that entities evaluate their entire portfolio of BES assets against the criteria in Attachment 1 to determine those assets that have BES Cyber Systems that support the reliable operation of the BES.

Requirement R2 mandates that lists required by Requirement R1 are reviewed by a CIP Senior Manager on a periodic basis. The CIP Senior Manager's approval ensures proper oversight of the process by the appropriate Responsible Entity personnel.

The rest of the proposed CIP Version 5 mandates the minimum protection that must be provided to those BES Cyber Systems identified in CIP-002-5.

Reliability Standard CIP-003-5 requires each Responsible Entity, for its high impact and medium impact BES Cyber Systems, to review and obtain CIP Senior Manager Approval at least once every 15 calendar months for documented cyber security policies that collectively address topics referenced in CIP-004 through CIP-011-1. In addition, each Responsible Entity for its assets identified in CIP-002-5, Requirement R1,

Part R1.3 (those assets that have low impact BES Cyber Systems), shall implement, in a manner that identifies, assesses, and corrects deficiencies, one or more documented cyber security policies that collectively address the following topics: cyber security awareness; physical security controls; electronic access controls for external routable protocol connections and Dial-up Connectivity; and incident response to a Cyber Security Incident.

Reliability Standard CIP-004-5 requires that Responsible Entities with personnel who have authorized electronic or authorized unescorted physical access to BES Cyber Assets take action so that those personnel with such access maintain awareness of the Responsible Entity's security practices.

Reliability Standard CIP-005-5 requires Responsible Entities to manage electronic access to BES Cyber Systems by specifying a controlled ESP in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the BES. It also establishes requirements for management of secure remote access to Cyber Assets in order to provide adequate safeguards through robust identification, authentication, and encryption techniques.

Reliability Standard CIP-006-5 requires Responsible Entities to manage physical access to BES Cyber Systems by specifying a physical security plan in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the BES.

Reliability Standard CIP-007-5 requires Responsible Entities to manage system security by specifying select technical, operational, and procedural requirements in

support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the BES.

Reliability Standard CIP-008-5 requires Responsible Entities to mitigate the risk to the reliable operation of the BES in the case of a Cyber Security Incident by specifying incident response requirements.

Reliability Standard CIP-009-5 requires Responsible Entities, in order to support recovery of reliability functions performed by BES Cyber Systems, to specify recovery plans in support of the continued stability, operability, and reliability of the BES.

Reliability Standard CIP-010-1 requires Responsible Entities, for the purpose of preventing and detecting unauthorized changes to BES Cyber Systems, to meet configuration change management and vulnerability assessment requirements in support of protecting BES Cyber Systems from compromise that could lead to misoperation or instability in the BES.

Reliability Standard CIP-011-1 requires Responsible Entities, in order to prevent unauthorized access to BES Cyber System Information, to meet certain information protection requirements in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the BES.

The proposed CIP Version 5 standards have been developed by a standard drafting team with a broad base of BES and cyber security knowledge following the scope identified in the Standard Authorization Request that resulted in the initiation of NERC Project 2008-06 Cyber Security Order 706. The standard drafting team for this project adhered to NERC's regulatory-approved standards development process, which allows for industry comment and ballot of the proposed standards. Extensive industry

comments on the proposed standards were received and evaluated through several postings. Many of the comments have been incorporated into the final draft of the standards, resulting in thoroughly vetted, high quality standards.

3. Proposed Reliability Standards include clear and understandable consequences and a range of penalties (monetary and/or non-monetary) for a violation.

Each primary requirement is assigned a VRF and a VSL. These elements support the determination of an initial value range for the Base Penalty Amount regarding violations of requirements in FERC-approved Reliability Standards, as defined in the ERO Sanction Guidelines. The table included in **Exhibit F** shows the VRFs and VSLs resulting in the indicated range of penalties for violations.

4. Proposed Reliability Standards identify clear and objective criterion or measure for compliance, so that they can be enforced in a consistent and non-preferential manner.

Each of the requirements in the proposed CIP Version 5 is clear in identifying the required performance and the responsible entity. The proposed CIP Version 5 identifies clear and objective criteria in the language of the requirements so that that the standards can be enforced in a consistent and non-preferential manner. The language in the requirements is unambiguous with respect to the applicable entity expectations. Each requirement has a single associated measure.

5. Proposed Reliability Standards achieve a reliability goal effectively and efficiently — but do not reflect "best practices" without regard to implementation cost or historical regional infrastructure design.

The proposed CIP Version 5 helps the industry achieve the stated goals of identifying BES Cyber Systems and their associated BES Cyber Assets to ensure BES reliability effectively and efficiently. While there may be an increase in implementation costs as the number of assets within scope of the CIP Version 5 standards increase under the methodology in proposed CIP-002-5, the NERC Board of Trustees and the industry approved the revised methodology because there is recognition that it is needed to help ensure Bulk Power System reliability. Accordingly, the costs associated with implementing the proposed CIP-002 through CIP-011 Reliability Standards are not determined to be excessive or unreasonably burdensome.

6. Proposed Reliability Standards are not "lowest common denominator," *i.e.*, do not reflect a compromise that does not adequately protect Bulk-Power System reliability. Proposed Reliability Standards can consider costs to implement for smaller entities, but not at consequences of less than excellence in operating system reliability.

The proposed CIP Version 5 does not aim at the "lowest common denominator." The proposed CIP-002-5 standard provides clear and uniform criteria for identifying BES Cyber Systems on the Bulk Electric System. The proposed CIP-003-5 to CIP-09-5, retain the same requirement language as the previous standards, with confirming modifications, and have already been determined to meet this criterion. Proposed CIP-010-1 and CIP-011-1 are new standards that contain requirements previously defined across several CIP standards in Versions 1 through 4.

7. Proposed Reliability Standards are designed to apply throughout North America to the maximum extent achievable with a single Reliability Standard while not favoring one geographic area or regional model. They should take into account regional variations in the organization and corporate structures of transmission owners and operators, variations in generation fuel type and ownership patterns, and regional variations in market design if these affect the proposed Reliability Standard.

The requirements in the proposed CIP Version 5 apply throughout North America, with no exceptions. CIP Version 5 is a set of standards that will be universally applicable in the portions of the United States and Canada that recognize NERC as the ERO.

8. Proposed Reliability Standards cause no undue negative effect on competition or restriction of the grid beyond any restriction necessary for reliability.

The proposed CIP Version 5 enhances the operation and reliability of the grid and do not constrain competition or restrict transmission capability. The purpose of the proposed CIP Version 5 is to provide a cybersecurity framework for the identification and protection of BES Cyber Systems to support reliable operation of the Bulk Electric System.

Specifically, proposed Reliability Standard CIP-002-5 requires the identification and documentation of the BES Cyber Systems that support the reliable operation of the BES. The proposed CIP Version 5 does not have a business practice impact and thus will not result in a negative effect on competition.

9. The implementation time for the proposed Reliability Standard is reasonable.

The Implementation Plan provided in **Exhibit B** specifies how Responsible Entities should transition during the timeframe from acceptance of proposed CIP Version 5 until the Effective Date:

> 24 Months Minimum – The Version 5 CIP Cyber Security Standards, except for CIP-003-5 R2, shall become effective on the later of July 1, 2015, or the first calendar day of the ninth calendar quarter after the effective date of the order providing applicable regulatory approval. CIP-003-5, Requirement R2, shall become effective on the later of July 1, 2016, or the first calendar day of the 13th calendar quarter after the effective date of the order providing applicable regulatory approval. Notwithstanding any order to the contrary, CIP-002-4 through CIP-009-4 do not become effective, and CIP-002-3 through CIP-009-3 remain in effect and are not retired until the effective date of the Version 5 CIP Cyber Security Standards under this implementation plan.

Upon approval, the proposed implementation plan will allow Responsible Entities to transition directly to CIP Version 5, by staying the effective date for CIP Version 4. In the interim, CIP Version 3 will remain in effect.

Based on precedent and lessons learned from past practice, NERC believes the length of time between approval of the proposed CIP Version 4 standards and the effective date is reasonable. The proposed CIP Version 5 standards do not create any differentiation in requirements based on size. All entities, small and large, are expected to comply with these standards in the same manner.

In addition, NERC recognizes that it takes time to perform a thorough examination of all BES assets to determine whether they meet the criteria included in Attachment 1. Furthermore, new equipment may have to be installed, and new policies

and procedures implemented, by Responsible Entities in order to meet the requirements of the CIP-003-5 through CIP-009-5 Reliability Standards.

Several commenters questioned the need for an additional year of implementation time for low impact BES Cyber Systems. In response, the standards drafting team determined that an additional year of implementation for low impact BES Cyber Systems is needed to allow Responsible Entities to formulate and implement effective security solutions for physical and electronic perimeter protection. Despite not requiring an inventory of low impact BES Cyber Systems, entities must still implement these policy changes in applicable locations where no perimeter protection currently exists. As such, staggered implementation promotes prioritization of high and medium impact assets.

10. The Reliability Standards were developed in an open and fair manner and in accordance with the Reliability Standard development process.

NERC develops Reliability Standards in accordance with Section 300 (Reliability Standards Development) of its Rules of Procedure, the NERC *Reliability Standards Development Procedure,* and its replacement NERC *Standards Processes Manual*, which is incorporated into the Rules of Procedure as Appendix 3A. NERC's proposed rules provide for reasonable notice and opportunity for public comment, due process, openness, and a balance of interests in developing Reliability Standards. The development process is open to any person or entity with a legitimate interest in the reliability of the Bulk Power System. NERC considers the comments of all stakeholders and a vote of stakeholders and the NERC Board of Trustees is required to approve a Reliability Standard for submission to the applicable governmental authorities. The

drafting team developed this standard by following NERC's standards development process.

11. NERC explains any balancing of vital public interests in the development of proposed Reliability Standards.

NERC has identified no competing public interests regarding the request for approval of this proposed CIP Version 5. No comments were received that indicated the proposed standards conflicts with other vital public interests.

12. Proposed Reliability Standards consider any other appropriate factors.

No other factors for FERC's consideration were identified in the development of the proposed CIP Version 5.