Drafting Team Responses to "No" Votes with Comments

Carolina Power & Light Company CPL
Transmission Owners
Verne Ingersoll II

Comments:

General Comments: Since these standards as drafted will introduce additional capital expenses and ongoing operating expenses, a cost impact analysis study should be completed prior to approval by the NERC Board of Trustees to determine the overall magnitude of these costs for the amount of increased security to the impacted systems. NERC and the drafting team have not demonstrated and documented the need for each of these standards or the unnecessarily burdensome and costly documentation trail that they require to provide the required audit capability.

In reviewing the FAQ's, it is recommended that the FAQ's be attached to the standards, since in some cases, they clarify some of the wording of the standards. The FAQ's will be helpful when it is necessary to interpret the meaning of the written standards. By providing FAQ's prior to balloting, they will indirectly, at a minimum, be relied upon for deciding whether or not to approve the standards.

CIP002 -- no comments.
CIP003 -- no comments.
CIP004 -- no comments.
CIP005 -- no comments.

CIP006
R3 -- Monitoring physical access - This standard is unworkable unless the wording is clarified that "Unauthorized access attempts shall be reviewed immediately "upon discovery" and handled in accordance with the procedures specified in Requirement CIP-008."

R6.1 -- Testing of "all" physical security mechanisms. During formal audits, it is universally accepted to test a sample that should indicate problems rather than "all". CIP007 -- R8 requires a vulnerability assessment of "all" cyber assets within the ESP at least annually. During formal audits, it is universally accepted to assess a representative sample. Considering the "mission critical" nature and specialized characteristics of some of the legacy equipment involved in these environments, it is extremely labor-intensive and will unnecessarily increase the risk of outages on generating units, substations, and energy control systems to assess "all" assets within the ESP annually

Response

General:The need for Cyber Security Standards was brought to NERC from industry via a Standard Authorization Request (SAR). The SAR was developed into a scope document that was presented for public review and comment. A consensus of reviewers believed the need to move forward with developing cyber security standards per the scope of the SAR was appropriate. The Standards Development Process does not call for a cost/benefit analysis. The risk assessment process is left to the Responsible Entity, who should use reasonable business judgment when implementing these Requirements.

The FAQs will become a NERC reference document.

CIP006 R3
CIP-008, R1.2 requires Responsible Entities to define response actions. The intent of the requirement in 006 is to implement these response actions immediately, upon receipt of a alarm or other means of discovery. Please see FAQ 6 for CIP-008. The Standards Development Process does not allow for changing Standard at this time.

R6.1 This requirement addresses maintenance and testing over a period of three years, not auditing.

CIP007 -- R8 A comprehensive assessment of all Cyber Assets within the Electronic Security Perimeter is necessary to ensure the security of the Critical Cyber Assets. A weakness in one device can put all Critical Cyber Assets at risk.

without impacting operations. This requirement was not worded this way in draft 3 (i.e., using the word "all"). We either need more time (3 years) to assess all assets within the ESP or we need to be able to assess a representative sample to satisfy this requirement.

CIP008 -- no comments.
CIP009 -- no comments.

Drafting Team Responses to "No" Votes with Comments

Central Hudson Gas & Electric Corp. NYCH
Transmission Owners
Raymond J A'Brial

Comments:

Central Hudson believes the standards as written are too broad and not focused on the vulnerabilities that could exist in Control Centers in North America. There are a wide array of vulnerabilities that may exist for those assets outside of the Control Area and suggests a more prudent action would be to concentrate on Control Centers first, then expanding beyond those boundaries to more remote devices, i.e. spend the money to protect the more critical Cyber assets initially, then expand it.
Securing the Control Centers provides the best immediate Return On Investment for the security gain expected to be achieved There is a wide array of vulnerabilities affecting the Bulk Electric System Assets beyond the Control Centers. Cyber security is among these, but may not be the primary risk in many situations. At a control center there is a higher level of risk that a cyber incident could affect multiple BES facilities, as compared to the level of risk associated with a remote BES facility. Entities need the flexibility to optimize security expenditures so that all risks are best mitigated. The Standards as written will require disproportionate amount of available funds to be allocated to less significant risks, hence security of the Bulk Electric System may be reduced. Based on the experience gained from applying these Standards to the Control Centers, the industry could then focus on developing a new standard that would be more appropriate to assets beyond the Control Center. To make a cyber security standard effective beyond the control center will require collaboration between the asset owners and the equipment manufacturers in order to develop tools for managing the cyber security vulnerabilities. These Standards as written will bring high implementation costs for those Assets beyond the Control Centers and is not balanced by maintaining or increasing the Reliability of the Bulk Electric System. Applying the Standards as written to remote assets beyond the Control Center could in fact reduce the level of reliability experienced today. Microprocessor based relays and meters have provided many advantages to the industry, among them have been an ability to lengthen the maintenance cycles on these devices because they are self-monitoring. The lengthening of the maintenance cycles has minimized the human interaction with these systems, and thereby reduced the probability of an inadvertent trip on the relay systems. These standards as written require annual verification of ports (both HW and SW) and password maintenance for all devices within the electronic security perimeter. This level of human interaction with the devices on an annual basis increases the probability of inadvertent trips on the bulk electric system. As the standard is worded

Response

The scope for CIP-002 through CIP-009 includes Critical Cyber Assets outside the control center. Please see the Standard Authorization Request, dated March 8, 2004.

today, performing a once a year verification of ports in a sense leaves you no more secure the day after you perform the verification at that remote site then the day before you walked in. The security improvements expected to be achieved are minimal, and not justifiable when compared to the cost of doing the verification at all the remote critical cyber asset locations. Tools are needed that you are assured will not cause any other problems to your devices and that make it possible to perform the verification on a more frequent basis in order to truly have an improvement in security.

Drafting Team Responses to "No" Votes with Comments

Cinergy Corporation CIN
Transmission Owners
Doug Hils

Comments:

General Comment: Because so much information is contained in the FAQ's Cinergy suggests that the FAQ's be made part of the standard materials used for compliance guidance.

CIP 002
R1.1. Although NERC published a white paper describing various risk assessment methodologies, little guidance is provided in the standard or FAQ's as to specific expectations for the cyber security risk assessment. Further, sections of the standard seem to suggest physical security measures in response to cyber security threats, which might be identified in the assessment. Cinergy recommends adding a question to the FAQ's or language to the standard clarifying that participants should factor credible threat information the development of their risk assessment focusing on cyber security threats and electronic mitigating measures. It is not expected that participants should protect against all physical threats when implementing their cyber security program.

CIP 004
R4.2 The requirement states, "...Responsible Entity shall revoke such access to Critical Cyber Assets within 24 hours for personnel terminated for cause and within seven (7) calendar days for personnel who no longer require such access..." Cinergy interprets this requirement to mean that for personnel terminated NOT for cause, participants would have seven (7) calendar days to revoke access. The levels of non-compliance (Section D.2.2.4) states that any one instance of personnel termination where access is not revoked in 24 hours creates a level 2 violation. The violation seems inconsistent with the requirement as stated, and we do not believe participant should be held to this. Please explain.

D2.3.1 This section prescribes a Level 3 violation if a training program exists but has not been updated annually. In other standards Level 3 and 4 violations are for serious events/omissions which jeopardize reliability. Parts of this standard still measure documentation completeness with no relevance to actual security. We believe a level 3 violation is too severe for the situation where a training program exists and has been implemented, but has not been updated in the last year.

Response

General: The FAQs will become a NERC reference document.

CIP 002
R1.1 Industry consensus does not support a prescriptive risk assessment methodology to identify Critical Assets. Responsible Entities may consider threats when performing its risk assessment.

CIP 004
R4.2 The Drafting Team agrees that the wording in D2.2.4 is an unintentional omission of the phrase “for cause” in the language of the standard. The Drafting Team has developed an errata item correcting this error and will present it to the Standards Authorization Committee for its consideration after approval of these standards for inclusion in the NERC Approved Standards Errata Sheet.

D2.3.1
Compliance with these standards will enhance the security of Critical Assets through the protection of the Cyber Assets essential to their reliable operation, thereby contributing to the reliability of the bulk power systems. The Drafting Team made every attempt to provide tiered levels of non-compliance that reflect increasing severity to reliability. The Standards Development Process does not allow changes at this time.

CIP 006 R2, R3, R4 and R5.
Electronic measures alone are insufficient to meet the physical security Requirements of these standards. A completely enclosed (six-wall) boundary restricts access to Critical Cyber Assets, thereby limiting the number of personnel subject to the administrative requirements of CIP-004. Please refer to CIP-006 FAQ 1.

Drafting Team Responses to "No" Votes with Comments

CIP 006
R2. In each of the preceding drafts Cinergy has expressed operational concerns with implementing the expectation for a 6-wall physical security perimeter, access controls, monitoring, and logging of access, for critical cyber assets in substations that use a routable protocol to communicate outside of the electronic security perimeter. We believe the costs and operational impacts of these physical constraints are out of proportion to the probable risks and modes of cyber attack that might be used. Even though the critical cyber substation assets may represent only a small fraction of the substation assets, all employees who work in the substations would be covered under the administrative rules because it would be impossible to determine which substation employees may be required to work in the critical cyber asset substations. We ask that NERC consider adding language to the standard or to the FAQ's explaining that electronic measures may be sufficient to mitigate physical security requirements.

R3. See comments in R. 2 above.
R4 See comments in R. 2 above.
R5. See Comments in R. 2 above.

CIP 007
D.2.1. Level 1 Noncompliance: Parts of this standard still measure documentation completeness with no relevance to actual security. All levels of non-compliance in CIP 007 relate to documentation. Non-compliance should reflect "real" security issues rather than identifying whether papers have been updated or not. In this section, it is possible that the participant's systems could be fully secure but the participant would receive a non-compliance based solely on updating papers. While some documentation non-compliance may be relevant to prove compliance, this section of CIP 007 should include both actual systems security evaluation and documentation items.

D.2.2. Level 2 Noncompliance: Also, see D.2.1. Level 1 comments above.

D.2.3. Level 3 Noncompliance: In other standards, Level 3 and 4 violations are for serious events/omissions which jeopardize reliability. Also, see D.2.1. Level 1 comments above.

D.2.4 Level 4 Noncompliance: In other standards, Level 3 and 4 violations are for serious events/omissions which jeopardize reliability. Also, see D.2.1. Level 1comments above.

CIP 007
D.2.1, D.2.2, D2.3, and D2.4
Compliance with these standards will enhance the security of Critical Assets through the protection of the Cyber Assets essential to their reliable operation, thereby contributing to the reliability of the bulk power systems. The Drafting Team made every attempt to provide tiered levels of non-compliance that reflect increasing severity to reliability.

Drafting Team Responses to "No" Votes with Comments

City of Garland
Transmission Owners
David Lawrence Grubbs

Comments:

The latest version has widened the definition of Critical Asset where any transmission substation could be considered a Critial Asset. Further claification needs to be made to limit the transmission facilities considered to just those that have some pre-defined major effect not just "support the reliable operation". All substations fall into this definition.

Response

The Responsible Entity should consider each of its transmission substations in its risk assessment to determine Critical Assets, which are those that affect the reliability or operability of the Bulk Electric System. It is not expected that every substation will be deemed critical. Critical Cyber Assets support the reliable operation of the identified Critical Assets.

Drafting Team Responses to "No" Votes with Comments

FirstEnergy Corp
Transmission Owners
Raymond Morella

Comments:

CIP-002-1
R3. Critical Cyber Asset Identification -- Using the list of Critical Assets developed pursuant to Requirement R2, the Responsible Entity shall develop a list of associated Critical Cyber Assets essential to the operation of the Critical Asset. Examples at control centers and backup control centers include systems and facilities at master and remote sites that provide monitoring and control, automatic generation control, real-time power system modeling, and real-time interutility data exchange. The Responsible Entity shall review this list at least annually, and update it as necessary. For the purpose of Standard CIP-002, Critical Cyber Assets are further qualified to be those having at least one of the following characteristics: R3.1. The Cyber Asset uses a routable protocol to communicate outside the Electronic Security Perimeter; or, R3.2. The Cyber Asset uses a routable protocol within a Control Center; or, R3.3. The Cyber Asset is dial-up accessible. FE Recommendation: FE does not agree with the use of "Control Center" in CIP-002 R3.2 and suggest that it be replaced with "Electronic Security Perimeter". The standard now reads "...Critical Cyber Assets are further qualified to be those having the following characteristics: The Cyber Asset uses a routable protocol within a Control Center ..." FE's interpretation is that as stated this would include any computer or device physically located at a Control Center that has a routable protocol, including both the EMS network and the corporate network. If Control Center in R3.2 were replaced with Electronic Security Perimeter, the intent of the Critical Cyber Asset definition is retained; Facilities, systems, and equipment which, if destroyed, degraded, or otherwise rendered unavailable, would affect the reliability or operability of the Bulk Electric System. CIP-005-1 R1.2. For a dial-up accessible Critical Cyber Asset that uses a non-routable protocol, the Responsible Entity shall define an Electronic Security Perimeter for that single access point at the dial-up device. FAQ #3 (CIP-005-1 Section) Page 13 of 30 Question: I have a single RTU that controls a critical bulk electric asset in a substation, connected through a modem to my EMS communication front-end. What is the Electronic Security Perimeter in this case? There is no LAN in the substation. Answer: An Electronic Security Perimeter is required at the master station front-end but only required at the RTU if the RTU uses a routable protocol. RTUs that use a non-routable protocol with a master/slave synchronous polling method that cannot access anything on the EMS, and use SBO (select before operate) command to control devices at the RTU end, do not

Response

CIP-002-1 R3.2 is meant to further qualify or limit the number of Critical Cyber Assets. Changing the verbiage as FE recommends would have the opposite effect.

005-1 R1.2 Any reference to Critical Cyber Assets in CIP-005 refer to the list of Critical Cyber Assets identified in CIP-002. The FAQ has been corrected.

require an Electronic Security Perimeter. If a dialup modem on a critical bulk electric asset is used for configuration or polling it must be in an Electronic Security Perimeter that is just around the dialup access point (e.g., SCADA-controlled, dial-back, or other technologies that give proper access controls and logging). FE Recommendation: The FAQ stated above appears to provide an exception to CIP-005 R1.2. It is our opinion that the standard should be clear in its requirements and we recommend that the drafting team consider revising CIP-005 R1.2 to address the ambiguity that exist by incorporating the FAQ response directly into the standard.

Drafting Team Responses to "No" Votes with Comments

Hydro One Networks Inc.
Transmission Owners
Ajay Garg

Comments:

Hydro One Networks considers the CIP-002 through CIP-009 proposed standards to contain significant value to bring the cyber security in the industry to acceptable levels. However, we have decided to vote No at this time due to fundamental concerns on the applicability of the standards. The entire set of standards rest on the definition of "Critical Cyber Asset". CIP-002 R3 defines Critical Cyber Asset as all Cyber Assets "essential to the control and operation of a critical asset" that "uses a routable protocol to communicate outside the Electronic Security Perimeter" or "is dial up accessible" or "uses a routable protocol within a control centre". We have several concerns with this definition: ï‚· The determination of what is a "Critical Cyber Asset" depends on the location of the "Electronic Security Perimeter". Standard CIP-005 states that "The responsible entity will ensure that every Critical Cyber Asset resides within an Electronic Security Perimeter." This sets up a circuitous set of definitions which could lead to expedient and inappropriate location of the "Electronic Security Perimeter" which will not address key vulnerabilities. ï‚· We consider this definition to be significantly inadequate for situations outside of control centres. It does not properly consider in sufficient detail the actual risks associated with cyber assets at stations both inherently and in relation to other security risks. A station may be considered a critical asset but individual elements within a station may not be critical. Yet, certain combinations of elements may be critical. It may be that practical considerations require every digital protection in the station to be considered critical. Addressing the cost of applying 003 to 009 to all digital protections drive design implementations for substation protection and control which would be sub-optimal in terms of dollars spent for security risk mitigation accomplished. ï‚· There are very significant Cyber Security risks that this definition will not address, for example in the area of telecommunications. ï‚· The definition is based on specific technologies: routable protocols and dial up access. We understand the concerns with these technologies but are unconvinced that there are not others which should be of concern or others that will emerge in the future. Rules based on specific technologies should be moved to a guideline or other document that can be updated more rapidly than can a Standard. Hydro One has struggled with the question of whether a bad and incomplete standard is better than no standard. We are anxious to see good standard in place to protect the integrated BES from cyber attack. We have concluded that no standard is better that this standard for the following reasons: 1. This standard is viewed as a complete

Response

The drafting team sees the identification of Critical Cyber Assets as an iterative process:
1) Identify Critical Assets via a risk assessment,
2) identify Critical Cyber Assets essential to the reliable operation of the Critical Assets,
3) define the Electronic Security Perimeter(s) as described in CIP-005,
4) apply the criteria in CIP-002, R3 and its sub-requirements, and,
5) re-evaluate the Electronic Security Perimeter(s).

The scope for CIP-002 through CIP-009 excludes telecommunications. Please see the Standard Authorization Request, dated March 8, 2004.

The scope of these standards, as defined in the SAR, is limited to assets that use routable protocols or are dial-up accessible. New SARs may be necessary to address new or different technologies.

The drafting team does not intend these standards to be a “complete solution.” We fully expect new SARs to be developed to complement this suite of standards.

As the standards reflect, a risk assessment is required in CIP-002 and is the first step to implementing the rest of the requirements of these standards.

The scope for CIP-002 through CIP-009 includes Critical Cyber Assets outside the control center. Please see the Standard Authorization Request, dated March 8, 2004.

solution for the cyber security vulnerabilities on the BES. In fact, it is incomplete and provides a false sense of security. Having no standard will keep the focus on doing the proper and complete job. 2. Implementing this standard before the proper and detailed risk assessment of all vulnerabilities is done will result in money spent sub-optimally or sub-optimal designs that may need to be re-worked when full assessment is in place. For these reasons, Hydro One is voting NO. We are comfortable that the Standard can be applied to Control Centres and will provide significant return on investment for security gain. This could be achieved at this time by revising the Implementation Plan, to require compliance to only the Control Centres. Cyber Security of facilities other than Control Centres, e.g. connections, telecommunications should be addressed in a separate standard. The SAR defining the scope of the new standards should also include changes to the CIP-002 through CIP-009 to clearly separate their applicability. Concurrent with the new standards, a definition of control Centre must be incorporated to the NERC Glossary of Terms. The term is used in the CIP standards and no definition is available. We offer the following definition to be considered: Control Center: The central facility or facilities of a Responsible Entity where the remote monitoring, operating and/or controlling of elements of the Bulk Electric System are or can be performed in real time.

Drafting Team Responses to "No" Votes with Comments

Nebraska Public Power District NPPD
Transmission Owners
Alan Boesch

Comments:

CIP--005--1, Section D. Compliance, Item 2.3.1 says A document defining the Electronic Security Perimeter(s) exists, but there are one or more Critical Assets not within the defined Electronic Security Perimeter(s); It should say : A document defining the Electronic Security Perimeter(s) exists, but there are one or more Critical Cyber Assets not within the defined Electronic Security Perimeter(s). Please modify this non-compliance to be consistent with the requirements of the standard.

Response

The Drafting Team agrees that the wording in D2.3.1 is an unintentional omission of the phrase “Critical Cyber Asset” in the language of the standard. The Drafting Team has developed an errata item correcting this error and will present it to the Standards Authorization Committee for its consideration after approval of these standards for inclusion in the NERC Approved Standards Errata Sheet.

Drafting Team Responses to "No" Votes with Comments

New Brunswick Power Transmission Corporation

Transmission Owners

Wayne Snowdon

Comments:

1) the Standards (CIP-002 through CIP-009) should apply only to Control Centers, therefore modifying the implementation plan to only Control Centers would make these Standards acceptable and 2) a new Standard should be developed for the Assets beyond the Control Centers and the existing Standards (CIP-002 through CIP-009) should be modified to focus on only Control Centers.

Response

The scope for CIP-002 through CIP-009 includes Critical Cyber Assets outside the control center. Please see the Standard Authorization Request, dated March 8, 2004.

Drafting Team Responses to "No" Votes with Comments

Nova Scotia Power NSPI

Transmission Owners

David D Little

Comments:

The Standards (CIP-002 through CIP-009) should apply only to Control Centers, therefore modifying the implementation plan to apply only to Control Centers would make these Standards acceptable. A new Standard should be developed for the Assets beyond the Control Centers and the existing Standards (CIP-002 through CIP-009) should be modified to focus on only Control Centers.

Response

The scope for CIP-002 through CIP-009 includes Critical Cyber Assets outside the control center. Please see the Standard Authorization Request, dated March 8, 2004.

Drafting Team Responses to "No" Votes with Comments

Portland General Electric PGE

Transmission Owners

Earl Cahoe

Comments:

During the webcast there was ambiguity as to whether devices outside the Critical Cyber Asset perimeter but on the Corporate LAN had to be included. I would like to see an expicit statement in the standard clarifying this issue.

Response

Assets such as business networks outside the Electronic Security Perimeter are not applicable.

Drafting Team Responses to "No" Votes with Comments

Tampa Electric Company TEC
Transmission Owners
Paul Michael Davis

Comments:

See Ron Donahey's - Tampa Electric Company comments. TEC recommends that the overarching principle for developing the NERC penalties and sanctioning processes for Cyber Security Standards should be to provide effective incentives for compliance, and not merely to penalize poor performance. Moreover, since the NERC/ERO penalties and sanctions are part of the statutorily delegated enforcement powers, they should be consistent with FERC's Enforcement Policy. Therefore, the sanctions guidelines should be aligned with FERC's Enforcement Policy, which evaluates a number of factors beginning with the harm or potential harm that was caused by the violation. Other factors may also be considered, including the financial impact of a penalty on an entity and mitigating factors, such as self-reporting and an effective compliance program. Based on the FERC enforcement policy, there are factors that should be considered in assessing the appropriate penalty or sanction: How serious was the harm or potential harm to reliability? Was the entity reckless or deliberately indifferent to the results of its action? Was the action willful? Is this a repeat violation? Does the entity have a history of violations? Is this an isolated incident or part of a recurring problem? Was the violation related to actions by senior management, the result of pressure placed on employees by senior management to achieve specific results or done with the knowledge and acquiescence of senior management? Did management engage in a cover-up? How did the violation come to light? Did the entity self-report? What effect would potential penalties have on the financial viability of the entity and their ability to maintain reliable operations? Consistent with the Enforcement Policy, penalties and sanctions should be structured such that functional entities are rewarded for self-reporting and self-corrections. Processes should recognize escalating and mitigating circumstances, including for example, prevailing system conditions at the time of violation, patterns of behavior, and the length of time over which a violation took place. Such flexibility is found throughout the processes used by other self-regulating organizations.

Response

Per NERC's VP of Standards, as part of its ERO application, NERC is developing a guideline for the application of penalties. This guideline addresses most if not all of the considerations listed in this comment as suitable reasons for either increasing or decreasing the amount of a financial penalty. The compliance information in the standard itself addresses only the measures for determining whether an entity complied or not, and the levels of non-compliance that are used to determine how severely the entity failed to meet the standard. The remaining factors are general ones that are not specific to each standard, e.g. did the entity self-report, does the entity have a strong compliance program, etc. These factors, along with the financial penalty matrix will be provided in the penalty guidelines provided in the ERO application. The penalty guidelines will eventually become mandatory under approval of FERC and Canadian governmental agencies.

Drafting Team Responses to "No" Votes with Comments

Texas-New Mexico Power TNMP
Transmission Owners
Roger Dickens

Comments:

Texas-New Mexico Power Company is voting no to the proposed CIP-002-1 through CIP-009-1. The reason is the wording in CIP-002-1 R3. The standard reads "... the Responsible Entity shall develop a list of associated Critical Cyber Assets essential to the operation of the Critical Asset. ... For the purpose of the Standard CIP-002, Critical Cyber Assets are further qualified to be those having at least one of the following characteristics:" The phrase further qualified is ambiguous. The word further is defined in Merriam-Webster Online Dictionary as "going or extending beyond", and qualified is defined as "limited or modified in some way." The phrase could then be interpreted as "extending" the scope as "modified" by the characteristics in R3.1 through R3.3. This becomes problem with R3.2 "The Cyber Assets uses a routable protocol within a Control Center." Extending the list to all Cyber Assets using a routable protocol within a Control Center, would expand the reach of the Cyber Security CIPs to the corporate network. At TNMP the corporate network is not necessary in the operation our Control Center, but our SCADA network is. I understand the "intent" of the Cyber Security CIPs are to protect the Bulk Electric System, but lawyers and auditors do not care much about intent. In one of the Cyber Security workshops it was explained to us that these standards should stand on there own without a FAQ, because the FAQ is not a part of the standard and any ambiguity should be resolved before making them a permanent standard. Also in the first sentence Critical Cyber Assets are not defined as Cyber Assets essential to the operation of the Critical Asset. R3 needs to make it clear that Critical Cyber Assets are Cyber assets that are essential to the operation of the Critical Asset and have one of the three characteristics specified in R3.1 through R3.3 To remove any ambiguity I would rephrase the last sentence in CIP-002-1 R3 to read, "For the purpose of Standard CIP-002, Critical Cyber Assets are Cyber Assets, which are essential to the operation of the Critical Asset, and the Cyber Assets has at least one of the following characteristics:"

Response

The definitions do not need to be repeated as part of the requirements in this standard. However, R3 and its sub-requirements do limit the definition of Critical Cyber Asset.

Business network assets do not meet the definition of Critical Cyber Asset.

The Standards Development Process does not allow the changes to the standard at this time.

Drafting Team Responses to "No" Votes with Comments

New Brunswick System Operator
RTOs, ISOs, and RROs
Alden Briggs

Comments:

The scope of the Cyber Standards is too broad and that it would be a greater return on investment and of more potential benefit to confine this particular standard set, through revising the Implementation Plan, to only the Control Centers. Another Standard Authorization Request (SAR) would then be drafted and submitted to NERC to begin the development of a set of standards to deal specifically with those assets outside the Control Center security perimeter.

Response

The scope for CIP-002 through CIP-009 includes Critical Cyber Assets outside the control center. Please see the Standard Authorization Request, dated March 8, 2004.

Drafting Team Responses to "No" Votes with Comments

Northeast Power Coordinating Council

RTOs, ISOs, and RROs

Edward Schwerdt

Comments:

The final draft of the standard added a requirement that the Transimission Service Provider (TSP) perform reliability assessments. In the Functional Model, it is the Reliability Authority (RC in the standards) that is charged with performing reliability assessments, in as much as the TSP may lack the necessary "wide area view" to properly perform such analyses.

Response

NPCC indicated that this comment was submitted in error.

Drafting Team Responses to "No" Votes with Comments

CalpinePowerAmerica
Load-Serving Entities
Randy Jones

Comments:

I am casting a NO vote based on the lack of resolution procedures that would be necessary in the event of conflicting conclusions by different parties on whether certain assets are deemed critical.

Response

The standard requires Responsible Entities to identify Critical Assets based on its documented risk assessment methodology. Compliance will be measured as defined in the standards. Furthermore, NERC's Guidelines for Disclosure identifies a defined dispute resolution process.

Drafting Team Responses to "No" Votes with Comments

Cinergy Corporation CIN
Load-Serving Entities
Larry Edward Conrad

Comments:

General Comment: Because so much information is contained in the FAQ's Cinergy suggests that the FAQ's be made part of the standard materials used for compliance guidance.

CIP 002 R1.1. Although NERC published a white paper describing various risk assessment methodologies, little guidance is provided in the standard or FAQ's as to specific expectations for the cyber security risk assessment. Further, sections of the standard seem to suggest physical security measures in response to cyber security threats, which might be identified in the assessment. Cinergy recommends adding a question to the FAQ's or language to the standard clarifying that participants should factor credible threat information the development of their risk assessment focusing on cyber security threats and electronic mitigating measures. It is not expected that participants should protect against all physical threats when implementing their cyber security program.

CIP 004 R4.2 The requirement states, "…Responsible Entity shall revoke such access to Critical Cyber Assets within 24 hours for personnel terminated for cause and within seven (7) calendar days for personnel who no longer require such access…" Cinergy interprets this requirement to mean that for personnel terminated NOT for cause, participants would have seven (7) calendar days to revoke access. The levels of non-compliance (Section D.2.2.4) states that any one instance of personnel termination where access is not revoked in 24 hours creates a level 2 violation. The violation seems inconsistent with the requirement as stated, and we do not believe participant should be held to this. Please explain.

D2.3.1 This section prescribes a Level 3 violation if a training program exists but has not been updated annually. In other standards Level 3 and 4 violations are for serious events/omissions which jeopardize reliability. Parts of this standard still measure documentation completeness with no relevance to actual security. We believe a level 3 violation is too severe for the situation where a training program exists and has been implemented, but has not been updated in the last year.

CIP 006 R2. In each of the preceding drafts Cinergy has expressed operational

Response

General Comment: The FAQs will become a NERC reference document.

CIP 002 R1.1. Industry consensus does not support a prescriptive risk assessment methodology to identify Critical Assets. Responsible Entities may consider threats when performing its risk assessment.

CIP 004 R4.2 The Drafting Team agrees that the wording in D2.2.4 is an unintentional omission of the phrase "for cause" in the language of the standard. The Drafting Team has developed an errata item correcting this error and will present it to the Standards Authorization Committee for its consideration after approval of these standards for inclusion in the NERC Approved Standards Errata Sheet.

D2.3.1
Compliance with these standards will enhance the securityof Critical Assets through the protection of the Cyber Assets essential to their reliable operation, thereby contributing to the reliability of the bulk power systems. The Drafting Team made every attemptto provide tiered levels of non-compliance that reflect increasing severity to reliability. The Standards Development Process does not allow changes at this time.

CIP 006 R2 - 4.
Compliance with these standards will enhance the security of Critical Assets through the protection of the Cyber Assets essential to their reliable operation, thereby contributing to the reliability of the bulk power systems. The Drafting Team made every attempt to provide tiered levels of non-compliance that reflect increasing severity to reliability. The Standards Development Process does not allow changes at this time.

concerns with implementing the expectation for a 6-wall physical security perimeter, access controls, monitoring, and logging of access, for critical cyber assets in substations that use a routable protocol to communicate outside of the electronic security perimeter. We believe the costs and operational impacts of these physical constraints are out of proportion to the probable risks and modes of cyber attack that might be used. Even though the critical cyber substation assets may represent only a small fraction of the substation assets, all employees who work in the substations would be covered under the administrative rules because it would be impossible to determine which substation employees may be required to work in the critical cyber asset substations. We ask that NERC consider adding language to the standard or to the FAQ's explaining that electronic measures may be sufficient to mitigate physical security requirements.

R3. See comments in R. 2 above.
R4 See comments in R. 2 above.
R5. See comments in R. 2 above.

CIP 007
D.2.1. Level 1 Noncompliance: Parts of this standard still measure documentation completeness with no relevance to actual security. All levels of non-compliance in CIP 007 relate to documentation. Non-compliance should reflect "real" security issues rather than identifying whether papers have been updated or not. In this section, it is possible that the participant's systems could be fully secure but the participant would receive a non-compliance based solely on updating papers. While some documentation non-compliance may be relevant to prove compliance, this section of CIP 007 should include both actual systems security evaluation and documentation items.

D.2.2. Level 2 Noncompliance: Also, see D.2.1. Level 1 comments above.

D.2.3. Level 3 Noncompliance: In other standards, Level 3 and 4 violations are for serious events/omissions which jeopardize reliability. Also, see D.2.1. Level 1 comments above.

D.2.4 Level 4 Noncompliance: In other standards, Level 3 and 4 violations are for serious events/omissions which jeopardize reliability. Also, see D.2.1. Level 1 comments above.

CIP 007
Compliance with these standards will enhance the security of Critical Assets through the protection of the Cyber Assets essential to their reliable operation, thereby contributing to the reliability of the bulk power systems. The Drafting Team made every attempt to provide tiered levels of non-compliance that reflect increasing severity of impact to reliability.

FirstEnergy Solutions FESC
Load-Serving Entities
Joanne Kathleen Borrell

Comments:

CIP-002-1
R3. Critical Cyber Asset Identification — Using the list of Critical Assets developed pursuant to Requirement R2, the Responsible Entity shall develop a list of associated Critical Cyber Assets essential to the operation of the Critical Asset. Examples at control centers and backup control centers include systems and facilities at master and remote sites that provide monitoring and control, automatic generation control, real-time power system modeling, and real-time interutility data exchange. The Responsible Entity shall review this list at least annually, and update it as necessary. For the purpose of Standard CIP-002, Critical Cyber Assets are further qualified to be those having at least one of the following characteristics:

R3.1. The Cyber Asset uses a routable protocol to communicate outside the Electronic Security Perimeter; or,
R3.2. The Cyber Asset uses a routable protocol within a Control Center; or,R3.3. The Cyber Asset is dial-up accessible.

FES Recommendation: FES does not agree with the use of "Control Center" in CIP-002 R3.2 and suggest that it be replaced with "Electronic Security Perimeter".

The standard now reads "…Critical Cyber Assets are further qualified to be those having the following characteristics: The Cyber Asset uses a routable protocol within a Control Center …"

FES's interpretation is that as stated this would include any computer or device physically located at a Control Center that has a routable protocol, including both the EMS network and the corporate network. If Control Center in R3.2 were replaced with Electronic Security Perimeter, the intent of the Critical Cyber Asset definition is retained; Facilities, systems, and equipment which, if destroyed, degraded, or otherwise rendered unavailable, would affect the reliability or operability of the Bulk Electric System.

CIP-005-1 R1.2. For a dial-up accessible Critical Cyber Asset that uses a non-routable protocol, the Responsible Entity shall define an Electronic Security Perimeter for that

Response

R3.2 is meant to further qualify or limit the number of Critical Cyber Assets. Changing the verbiage as FE recommends would have the opposite effect.

Any reference to Critical Cyber Assets in CIP-005 refer to the list of Critical Cyber Assets identified in CIP-002. The FAQ has been corrected.

single access point at the dial-up device.

FAQ #3 (CIP-005-1 Section) Page 13 of 30
Question: I have a single RTU that controls a critical bulk electric asset in a substation, connected through a modem to my EMS communication front-end. What is the Electronic Security Perimeter in this case? There is no LAN in the substation.

Answer: An Electronic Security Perimeter is required at the master station front-end but only required at the RTU if the RTU uses a routable protocol. RTUs that use a non-routable protocol with a master/slave synchronous polling method that cannot access anything on the EMS, and use SBO (select before operate) command to control devices at the RTU end, do not require an Electronic Security Perimeter. If a dialup modem on a critical bulk electric asset is used for configuration or polling it must be in an Electronic Security Perimeter that is just around the dialup access point (e.g., SCADA-controlled, dial-back, or other technologies that give proper access controls and logging).

FES Recommendation: The FAQ stated above appears to provide an exception to CIP-005 R1.2. It is our opinion that the standard should be clear in its requirements and we recommend that the drafting team consider revising CIP-005 R1.2 to address the ambiguity that exist by incorporating the FAQ response directly into the standard.

Drafting Team Responses to "No" Votes with Comments

Florida Municipal Power Agency FMPA
Load-Serving Entities
Joseph Krupar

Comments:

It took six months to review comments to draft 3 and revise the standard as needed. There was a 1048 page document of comments and reponses to comments posted with the Standard on January 16 for a 30 day pre-ballot review. Additional comments should have been sought if it took six months to review comments and change the standard. Also the documentation seems excessive to assure an entity has not violated the requirements.

Response

The review of comments on Draft 3 revealed significant concensus on many of the requirements in the standards. With the concurrence of the Standards Authorization Committee, draft 4 was submitted to the industry for ballot in accordance with the Standards Development Process.

The drafting team made every attempt to reduce the amount of documentation necessary to demonstrate compliance. However, these standards do rely on documentation to demonstrate compliance, the results of which is improved security for Critical Cyber Assets.

Drafting Team Responses to "No" Votes with Comments

Florida Power Corporation FPC
Load-Serving Entities
Lee G Schuster

Comments:

Since these standards as drafted will introduce additional capital expenses and ongoing operating expenses, a cost impact analysis study should be completed prior to approval by the NERC Board of Trustees to determine the overall magnitude of these costs for the amount of increased security to the impacted systems. NERC and the drafting team have not demonstrated and documented the need for each of these standards or the unnecessarily burdensome and costly documentation trail that they require to provide the required audit capability.

In reviewing the FAQ's, it is recommended that the FAQ's be attached to the standards, since in some cases, they clarify some of the wording of the standards. The FAQ's will be helpful when it is necessary to interpret the meaning of the written standards. By providing FAQ's prior to balloting, they will indirectly, at a minimum, be relied upon for deciding whether or not to approve the standards.

CIP006 - R3 -- Monitoring physical access - This standard is unworkable unless the wording is clarified that "Unauthorized access attempts shall be reviewed immediately "upon discovery" and handled in accordance with the procedures specified in Requirement CIP-008."

R6.1 -- Testing of "all" physical security mechanisms. During formal audits, it is universally accepted to test a sample that should indicate problems rather than "all".

CIP007 -- R8 requires a vulnerability assessment of "all" cyber assets within the ESP at least annually. During formal audits, it is universally accepted to assess a representative sample. Considering the "mission critical" nature and specialized characteristics of some of the legacy equipment involved in these environments, it is extremely labor-intensive and will unnecessarily increase the risk of outages on generating units, substations, and energy control systems to assess "all" assets within the ESP annually without impacting operations. This requirement was not worded this way in draft 3 (i.e., using the word "all"). We either need more time (3 years) to assess all assets within the ESP or we need to be able to assess a representative sample to satisfy this requirement.

Response

The need for Cyber Security Standards was brought to NERC from industry via a Standard Authorization Request (SAR). The SAR was developed into a scope document that was presented for public review and comment. A consensus of reviewers believed the need to move forward with developing cyber security standards per the scope of the SAR was appropriate. The Standards Development Process does not call for a cost/benefit analysis. The risk assessment process isl eft to the Responsible Entity, who should use reasonable business judgment when implementing these Requirements.

The FAQs will become a NERC reference document.

CIP006 - R3 CIP-008, R1.2 requires Responsible Entities to define response actions. The intent of the requirement in 006 is to implement these response actions immediately, upon receipt of a alarm or other means of discovery. Please see FAQ 6 for CIP-008. The Standards Development Process does not allow for changing Standard at this time.

R6.1 This requirement addresses maintenance and testing over a period of three years, not auditing.

CIP007 -- R8 A comprehensive assessment of all Cyber Assets within the Electronic Security Perimeter is necessary to ensure the security of the Critical Cyber Assets. A weakness in one device can put all Critical Cyber Assets at risk.

Drafting Team Responses to "No" Votes with Comments

Hydro One Networks Inc
Load-Serving Entities
Mike Penstone

Comments:

Hydro One Networks considers the CIP-002 through CIP-009 proposed standards to contain significant value to bring the cyber security in the industry to acceptable levels. However, we have decided to vote No at this time due to fundamental concerns on the applicability of the standards. The entire set of standards rest on the definition of "Critical Cyber Asset". CIP-002 R3 defines Critical Cyber Asset as all Cyber Assets "essential to the control and operation of a critical asset" that "uses a routable protocol to communicate outside the Electronic Security Perimeter" or "is dial up accessible" or "uses a routable protocol within a control centre". We have several concerns with this definition: ï‚· The determination of what is a "Critical Cyber Asset" depends on the location of the "Electronic Security Perimeter". Standard CIP-005 states that "The responsible entity will ensure that every Critical Cyber Asset resides within an Electronic Security Perimeter." This sets up a circuitous set of definitions which could lead to expedient and inappropriate location of the "Electronic Security Perimeter" which will not address key vulnerabilities. ï‚· We consider this definition to be significantly inadequate for situations outside of control centres. It does not properly consider in sufficient detail the actual risks associated with cyber assets at stations both inherently and in relation to other security risks. A station may be considered a critical asset but individual elements within a station may not be critical. Yet, certain combinations of elements may be critical. It may be that practical considerations require every digital protection in the station to be considered critical. Addressing the cost of applying 003 to 009 to all digital protections drive design implementations for substation protection and control which would be sub-optimal in terms of dollars spent for security risk mitigation accomplished. ï‚· There are very significant Cyber Security risks that this definition will not address, for example in the area of telecommunications. ï‚· The definition is based on specific technologies: routable protocols and dial up access. We understand the concerns with these technologies but are unconvinced that there are not others which should be of concern or others that will emerge in the future. Rules based on specific technologies should be moved to a guideline or other document that can be updated more rapidly than can a Standard. Hydro One has struggled with the question of whether a bad and incomplete standard is better than no standard. We are anxious to see good standard in place to protect the integrated BES from cyber attack. We have concluded that no standard is better that this standard for the following reasons: 1. This standard is viewed as a complete

Response

The drafting team sees the identification of Critical Cyber Assets as an iterative process:
1)identify Critical Assets via a risk assessment,
2) identify Critical Cyber Assets essential to the reliable operation of the Critical Assets,
3) define the Electronic Security Perimeter(s) as described in CIP-005,
4) apply the criteria in CIP-002, R3 and its sub-requirements, and,
5) re-evaluate the Electronic Security Perimeter(s).

The scope for CIP-002 through CIP-009 excludes telecommunications. Please see the Standard Authorization Request, dated March 8, 2004.

The scope of these standards, as defined in the SAR, is limited to assets that use routable protocols or are dial-up accessible. New SARs may be necessary to address new or different technologies.

The drafting team does not intend these standards to be a “complete solution.” We fully expect new SARs to be developed to complement this suite of standards.

As the standards reflect, a risk assessment is required in CIP-002 and is the first step to implementing the rest of the requirements of these standards.

The scope for CIP-002 through CIP-009 includes Critical Cyber Assets outside the control center. Please see the Standard Authorization Request, dated March 8, 2004.

solution for the cyber security vulnerabilities on the BES. In fact, it is incomplete and provides a false sense of security. Having no standard will keep the focus on doing the proper and complete job. 2. Implementing this standard before the proper and detailed risk assessment of all vulnerabilities is done will result in money spent sub-optimally or sub-optimal designs that may need to be re-worked when full assessment is in place. For these reasons, Hydro One is voting NO. We are comfortable that the Standard can be applied to Control Centres and will provide significant return on investment for security gain. This could be achieved at this time by revising the Implementation Plan, to require compliance to only the Control Centres. Cyber Security of facilities other than Control Centres, e.g. connections, telecommunications should be addressed in a separate standard. The SAR defining the scope of the new standards should also include changes to the CIP-002 through CIP-009 to clearly separate their applicability. Concurrent with the new standards, a definition of control Centre must be incorporated to the NERC Glossary of Terms. The term is used in the CIP standards and no definition is available. We offer the following definition to be considered: Control Center: The central facility or facilities of a Responsible Entity where the remote monitoring, operating and/or controlling of elements of the Bulk Electric System are or can be performed in real time.

Drafting Team Responses to "No" Votes with Comments

Tampa Electric Company TEC
Load-Serving Entities
Ronald Donahey

Comments:

We wish to thank the drafting committee for the huge amount of effort that went into the drafting of these standards. We believe that a reasonable set of standards will assist in ensuring reliable cyber security for the Electric Industry and your efforts have resulted in a standard well on its way to being acceptable. Our NO vote is based on the following unacceptable items in the standard:

CIP-004 Personnel and Training R3 Personnel Risk Assessment

Since vendors are included in the requirement, Level 1 and level 2 noncompliance for one personnel risk assessment not being updated at least every seven years, or for cause is excessive and will result in a large part of the industry being non-compliant. We would suggest changing requirement R3.3 to indicate that for vendors, the utility must contractually require risk assessments from vendors. Non-compliance should be based on there being no contractual agreement requiring this assessment. However, we find unacceptable a requirement that Tampa Electric accept accountability for a vendor's failure to comply.

R4 Access Requests Level 2 noncompliance for only 1 person not meeting the 24-hour rule seems excessive and impractical and will result in a large part of the industry being non-compliant at some point. For internal personnel, revoking access requests for cause within 24 hours is doable most of the time. However, there are times when it is not. For example, job abandonment cases are considered termination for cause. We may have no way of getting "hard keys" back from these people. Theft of keys and card keys may be handled by filing a legal complaint, but cannot be resolved in 24 hours. This requirement would only be acceptable if we can write an exception to the standard that allows longer periods of time in cases of abandonment (or similar circumstances) and would not result in non-compliance. In addition, we suggest changing requirement R4.2 to say for vendors, the utility must contractually require notification in these timeframes. However, we find unacceptable a requirement that Tampa Electric accept accountability for a vendor's failure to comply.

CIP-005 Electronic Security Perimeters

Response

CIP-004 Personnel and Training R3 Personnel Risk Assessment
The Responsible Entity is expected to ensure that vendors will comply with the requirements of the Standards. A contract arrangement and evidence of compliance from the vendor will be sufficient to demonstrate compliance on the Responsible Entity's part.

The Responsible Entity must revoke authorized access within 24 hours for cause. There will be occasions when the Responsible Entity makes best effort to recover its keys within 24 hours but is unsuccessful. It is not intended that this situation cause non-compliance; the requirement is to revoke authorized access.

The Responsible Entity is expected to ensure that vendors will comply with the requirements of the Standards. A contract arrangement and evidence of compliance from the vendor will be sufficient to demonstrate compliance on the Responsible Entity's part.

CIP-005 Electronic Security Perimeters
The Drafting Team made every attempt to provide tiered levels of non-compliance that reflect increasing severity to reliability. The Standards Development Process does not allow for changes to the standards at this time.

2.3.2 Level 3 noncompliance for one non-critical cyber asset in the perimeter not documented is excessive. If not critical (thus is not essential to the managing the bulk power system), the documentation of it is of little value, especially if the asset has been protected. As a comparison, there is no non-compliance level listed in CIP-002 if one or more critical cyber assets are not on the critical cyber asset list.

2.3.3. Level 3 non-compliance for not documenting one access point is excessive, especially if they are protected. Protection should be the focus, not documentation.

Drafting Team Responses to "No" Votes with Comments

Calpine Power Management LP
Transmission Dependent Utilities
Jim Stanton

Comments:

Calpine supports the need for this Cyber Security Standard, and recognize our fleet of generators across the country can play a crucial role in supporting the integrity of the interconnected electrical systems. We feel however the Standard is deficient in that the directive for Responsible Entities to execute a risk based assessment is vague and incomplete. As the Responsible Entity for our assets in the roles of Generation Owner and Generation Operator, we are unclear that even if we could "identify and document a risk based assessment methodology" we would likely have difficulty in procuring the data necessary for the assessment. This type of data, as to the limiting elements and various ratings on the transmission system, has been deemed proprietary in our experience. We fear that even if we could identify a risk based assessment methodology, we would be unable to procure the data for the model. Also, there is no provision that we can identify in the Cyber Security Standard for the resolution of different conclusions as to the status of a Critical Asset. Our concern is that even if we can identify a risk based assessment methodology, and procure the data to model the risks, what happens if our assessment disagrees with the transmission provider and/or Regional Entity? Our concern with this is less in areas with independent transmission providers, such as RTOs, but is much greater in those areas that have declined such independence. We see a substantial risk of undue discrimination in such areas and would prefer the Standard contain guidelines to rectify conflicting conclusions of the various risk based assessment methodologies.

Response

Industry consensus does not support a prescriptive methodology to identify Critical Assets. However, these standards do not preclude coordination with the RROs or RTOs.

The standard requires Responsible Entities to identify Critical Assets based on its documented risk assessment methodology. Compliance will be measured as defined in the standards. Furthermore, NERC's Guidelines for Disclosure identifies a defined dispute resolution process.

Drafting Team Responses to "No" Votes with Comments

Seminole Electric Cooperative SEC
Transmission Dependent Utilities
Steven Wallace

Comments:

The determination of applicable Critical Cyber Assets remains ambiguous, particularly with regard to the interpretation of routable protocol use, as well as "critical facilities" subject to the standard. In addition, the proposed standard imposes an unreasonable amount of documentation and record keeping seemingly solely for the purpose of disproving non-compliance.

Response

CIP-002 R3 and its sub-requirements limit the definition of Critical Cyber Asset. CIP-002-1 FAQ 1 provides guidance on Critical Cyber Asset identification and CIP-002 FAQ 6 provides examples of routable protocols.

The drafting team made every attempt to reduce the amount of documentation necessary to demonstrate compliance. However, the compliance auditing process does rely on documentation to demonstrate compliance, the results of which is improved security for Critical Cyber Assets.

Drafting Team Responses to "No" Votes with Comments

Allegheny Energy Supply Company AETS
Electric Generators
Carol Lynn Krysevig

Comments:

CIP-002 – Critical Cyber Asset Identification

B.R1.2.3 "Generation resources that support the reliable operation of the Bulk Electric System" is extremely broad and could be interpreted to mean each and every generator. NERC's answer to a question raised in the Jan 31 Web meeting, indicating that the assessment is to be done by generation owners without any guidance from the transmission service provider is even more perplexing. Effectively, every generation owner will be responsible for developing its own guidelines for determining which generation resources are most "critical" to the support of the reliable operation of the system. Although that can certainly be done, based upon the best (albeit limited) information available to the generation owner, the audit aspects concern us. It will undoubtedly be a difficult task for an auditor to make fair and balanced assessments, across the industry, given a multitude of risk assessment methodologies and no guidelines.

B.R3 – B.R3.3 Section R.3, Critical Cyber Asset Identification, lays the foundation of the remaining standards. We can't vote "yes" without a crystal clear understanding of what constitutes a Critical Cyber Asset. The changes made to the last version raised new questions in our minds about what constitutes a Critical Cyber Asset. Therefore, based upon our understanding of what we think NERC intends in Section B.R.3, we would have suggested (given the opportunity to do so) that the section be rewritten as shown below. Please confirm or correct our understanding per the following interpretation:

****

R3. Critical Cyber Asset Identification – For each Critical Asset, using the list of Cyber Assetsfor that associated with that Critical A asset, develop a list of Critical Cyber Assets. Refer to the definition of "Critical Cyber Asset" which states these are "Cyber Assets essential to the reliable operation of Critical Assets."

R3. 1 For the purpose of Standard CIP-002, Cyber Assets that are essential to the reliable operation of the Critical Asset and meet one of the following criteria should be included as Critical additionally include Cyber Assets having

Response

CIP-002
B.R1.2.3The response given during the webcast was addressing FERC restrictions prohibiting Generation Owners from coordinating with Transmission Owners. Generators owners may be able to acquire all necessary information to support their risk assessments from RROs, ISO/RTOs, or Reliability Coordinators.

The compliance monitor will assess compliance per the measurements defined in the standards.

R3
1. Section R3.1.3 You are correct, the assets are not critical because of their location.

2. Section R3.2 This is not correct – the expectation is that an access control mechanism will be implemented between the network of Critical Cyber Assets and the corporate network in order to protect the control center network.

2.3 The Standards Development Process does not allow for changes to the standards at this time.

CIP-003 – Security Management Controls
B.R5 The Standards Development Process does not allow for changes to the standards at this time.

CIP-004 The Drafting Team modified previous drafts of the standards to reflect industry consensus that a grace period be provided. Responsible Entities may elect to implement stricter requirements.

CIP-005 The Standards Development Process does not allow for changes to the standards at this time.

R3.1.1 The Cyber Asset uses a routable protocol to communicate outside the Electronic Security Perimeter; or,
R3.1.2 The Cyber Asset is dial-up accessible.
R3.1.3 The Cyber Asset is attached to and uses a routable protocol within an Electronic Security Perimeter as defined in CIP-005 that contains other Critical Cyber Assets. (JAS – Maybe this isn't necessary.)

R3.2 Cyber Assets, not otherwise chosen as Critical Cyber Assets, providing: monitoring; supervisory control; closed loop control; automatic generation control; real-time power system modeling; or real-time inter-utility data exchange for a Critical Asset shall be considered for inclusion as Critical Cyber Assets using the definitions and reasonable business judgment.

R3.3 Cyber Assets, not otherwise chosen as Critical Cyber Assets, attached to a local area network containing other Critical Cyber Assets and protected by an Electronic Security Perimeter as defined in CIP-005 shall be considered for inclusion as Critical Cyber Assets usingthe definitions and reasonable business judgment. (JAS – This could be used instead of R3.1.3)

R3.4 The Responsible entity shall review this list at least annually, and update it as necessary.
¬¬¬¬¬¬¬¬¬¬¬¬¬¬¬¬¬¬¬

Our rationale for rewording this section, according to what we believe to be NERC's intent, is:

1. Section R3.1.3 – we removed this section because these assets are not technically "Critical Cyber Assets." Rather, they are identified and protected pursuant to CIP-005 and afforded some of the same protections as Critical Cyber Assets.

2. Section R3.2 "The Cyber Asset uses a routable protocol within a Control Center; or;" is imprecise. This section potentially forces inclusion of non-Critical Cyber Assets not protected with an Electronic Security Perimeter, thus potentially requiring an Entity'sies entire corporate network be deemed as Critical Cyber Assets.

2.3. The example in section R3 beginning "Examples at control centers and backup control centers include systems and facilities at master and remote sites that…" cannot easily be interpreted. The words "master site", "remote site", "control centers",

B.R1.2 The Standards Development Process does not allow for changes to the standards at this time.

B.R1.4 and B.R.1.5 CIP-005 R1.6 does require Responsible Entities to maintain a list of the Cyber Assets identified in R1.4 and R1.5. R5.1 requires an annual review of these assets and they are referenced on both the measures and levels of non-compliance sections, e.g D2.3.2.

Yes, for assets described in CIP-005 R1.5, compliance with CIP-006 R1 is not required. Assets used to provide access control and monitoring of the Electronic Security Perimeter are subject to the subset of requirements defined in CIP-005, R1.5. Non-critical cyber assets within the Electronic Security Perimeter must be protected per the requirements of CIP-005 and CIP-007.

B.R3.1 The Standards Development Process does not allow for changes to the standards at this time.

D. Compliance2.3 Level 3 - 2.3.3 CIP-005 addresses access points to the Electronic Security Perimeter.
The Standards Development Process does not allow for changes to the standards at this time.

CIP-006 – Physical Security
The interpretation is correct.

D. Compliance2.1 Level 1 – 2.1.3
The levels of non-compliance in CIP-006 address documentation required in CIP-006. The Standards Development Process does not
allow for changes to the standards at this time.

"systems", and "facilities" can be interpreted in different ways.

CIP-003 – Security Management Controls B.R5 The word "information" in this section could have been clarified by changing the wording to read "information as designated by CIP-003-1 R4."

CIP-004 – Personnel and Training B.R3 We would like clarification as to why a 30-day "grace" period is allowed prior to an employee's personnel risk assessment results are known. Providing up to 30-day unescorted access to critical cyber assets without proper clearance would enable someone with malicious intent to harm system reliability before the employee was known as a threat.

CIP-005 – Electronic Security Perimeter(s) B.R1.2. This section could have been clarified by changing the wording "...uses a non-routable protocol..." to read "...that doesn't use a routable protocol,...".

The reason for suggesting this clarification is that a single computer may simultaneously use more than one communications protocol. Some of the protocols may be routable and some may not be routable. This section should only apply if none of the protocols used are routable.

B.R1.2 This section could have been clarified by changing the wording "...shall define an Electronic Security Perimeter..." to "...shall define a separate Electronic Security Perimeter...".

B.R1.4 and B.R.1.5 These sections effectively define new categories of Cyber Assets that are required to meet a subset of the requirements of Critical Cyber Assets, yet the standard does not require that we keep a list of these types of assets, nor review them as defined in CIP-002. It appears that the "Measures" and "Compliance" sections of the standards do not apply to them. Some of the requirement subsets are incomplete. For example, can one comply with CIP-006 R2 and R3, as CIP-005 B.R1.5 requires, without also complying with CIP-006 R1? Does NERC agree with this interpretation?

B.R3.1 This section could have been clarified by changing the wording "...use non-routable protocols..." to read "...doesn't use routable protocols...".

The reason for suggesting this clarification is that a single computer may simultaneously use more than one communications protocol. Some of the protocols

may be routable and some may not be routable. This section should only apply if none of the protocols used are routable.

D. Compliance 2.3 Level 3 - 2.3.3 – Clarify that the access points are meant to be "access points to the Electronic Security Perimeter".

CIP-006 – Physical Security B.R1.8 This section effectively defines a new category of Cyber Asset that is required to meet a subset of the requirements of Critical Cyber Assets, yet the standard does not require that we keep a list of this type of asset nor review it as defined in CIP-002. Does NERC agree with this interpretation?

D. Compliance 2.1 Level 1 – 2.1.3 – Clarify that "Required documentation" is only for documentation required in CIP-006-1.

2.1 Level 1 - 2.1.6 – Clarify that the "One required document" is only for CIP-006-1.

CIP-007 – Systems Security Management B.R5.1 The references to CIP-003 R5, which describes access to information about a cyber asset, not access to the cyber asset itself, appear to be incorrect.

City of Tallahassee TAL
Electric Generators
Alan Gale

Comments:

While I applaud the SDT's efforts and numerous hours that have gone into these standards, these proposed standards are a quantum leap from what is being done to satisfy the Urgent Action Standard 1200. It will be difficult and costly to cover everything in a procedure of sufficient depth to satisfy all involved.

Based on the non-compliance levels, the emphasis has shifted from protecting Critical Cyber Assets to documenting our processes, and having a process to document it.

The administrative burdens imposed by the proposed standards are arbitrary and capricious. They will do little to improve the security of the Bulk Electric System (BES) and will be extraordinarily difficult to ensure they are in context for smaller entities. The creation of a new Cyber Security Department in a small utility is an undue burden but would be necessary to devote the necessary resources to become fully compliant with the myriad of documentation requirements put forth in these standards. These standards alone will create such a large "administrative overhead" that rate increases will be necessary without a significant increase in the reliability of the BES. Which portion of these proposed standards was violated and contributed to the last blackout or major disturbance?

A few examples of specific problems are:

CIP-003 – Security Management Controls R.4 is above and beyond what is necessary. I still need to post an evacuation route on a floor plan of the building. This would be in violation of R4.1, which requires "protection" of "floor plans of computing centers that contain Critical Cyber Assets". These floor plans are available via the county offices for building permits.

R.6 The process to document how I am going to control my process for controlling changes appears to be a large administrative burden without benefit to the security of the BES (whatever the BES really is this week).

CIP-004 – Personnel and Training R3.1 Seven year background checks will increase cost for utilities without additional benefit. A check prior to employment is performed

Response

Publicly available floor plans should not reveal information about the location of Critical Cyber Assets. A posted evacuation route would not require this level of detail.

R6 requires Responsible Entities to implement a change control process and document that process.

CIP-004 The periodicity of background checks reflects industry consensus. The Responsible Entity is expected to ensure that vendors will comply with the requirements of the Standards. A contract arrangement and evidence of compliance from the vendor will be sufficient to demonstrate compliance on the Responsible Entity's part.

CIP-005 The assets used to control access and monitor the Electronic Security Program are not Critical Cyber Assets and are only subjected to a subset of requirements.

CIP-006 CIP-008, R1.2 requires Responsible Entities to define response actions. The intent of the requirement in 006 is to implement these response actions immediately, upon receipt of a alarm or other means of discovery. Please see FAQ 6 for CIP-008.

CIP-007
The standard does not require a redundant system.

The requirement is to address testing so that updated signature files do not adversely affect the operation of the Critical Cyber Asset.

The requirement does not mandate manual review of all logs; automated processes are acceptable and encouraged.

and then performance is monitored during that employment. If an employee does something to jeopardize his employment it will be dealt with long before it will show up in his background check. How are vendors included? It looks like I am responsible for performing vendor background checks before I let them in?

CIP-005 – Electronic Security Perimeter(s) R1.6 requires treating the monitoring systems as a Critical Cyber Asset. This becomes problematic on many levels. How do you secure the card reader on the outside of the access point?

CIP-006 – Physical Security R3 requires "immediate" review of unauthorized access attempts. This would include all card swipes that did not allow access because they were at the wrong door, or the time window had closed for routine access. This immediate investigation of a properly working security system is unnecessary.

CIP-007 – Systems Security Management
R1 essentially requires a redundant system to adequately test new assets and patches in a "manner that reflects the production environment" but isn't the production environment.

R4.2 requires a procedure to test and install updated security signatures. What does "test" mean? Expose it to the virus?

R6.5 requires us to "review logs of system events related to cyber security and maintain records documenting reviews of logs". This is a huge workload. The scope of the requirement would require a line-by-line check of ALL security access attempts. Every card swipe is an event. Every 'Access not granted" is not necessarily an Incident, but there is no differentiation. If an automated process were utilized, why wouldn't the review of the automated process log be sufficient? CIP-008 – Incident Reporting and Response Planning
R1.1 requires a procedure to "characterize and classify events as reportable Cyber Security Incidents". Is this intended to be in addition to, the same as, or different from the reporting of actual attacks via the OE-417 form? Is the Vulnerability and Risk Assessment Security Guideline for the Electricity Sector expected to be the baseline? Even all those requirements are general in nature and "feel good" requirements.

Who is the "Third-party monitor without vested interest in the outcome for NERC"? Is this entity expected to perform NERC audits? How did they get the "responsibility" for Compliance Monitoring? (D1.1.3 of all standards.) Do I have to perform background

CIP-008 The standard provides flexibility for the Responsible Entity's to decide what constitutes a reportable Cyber Security Incident. The OE-417 and NERC's incident reporting guidelines can provide useful information for this purpose.

The third-party monitor is the entity that will audit NERC for compliance with these standards.

checks on them before I grant them access to do an audit? Can it be any "entity" or a non-governmental body, such as EPRI? This is the first I recall seeing this reference anywhere.

Drafting Team Responses to "No" Votes with Comments

Gainesville Regional Utilities GVL
Electric Generators
Mark Lee Bennett

Comments:

The 24 hour rule and the background checks for all personnel seems excessive

Response

This reflects industry consensus.

Drafting Team Responses to "No" Votes with Comments

Ontario Power Generation Inc OPG

Electric Generators

Barry Green

Comments:

Standards (CIP-002-1 through CIP-009-1) should apply only to Power System Control Centers at this time. The reliability of the power system will not be significantly increased by spending a large amount of time and funds to secure, from a cyber perspective, assets that do not have as great an overall impact on the power system, or where cyber attack is not the greatest risk.

Response

The scope for CIP-002 through CIP-009 includes Critical Cyber Assets outside the control center. Please see the Standard Authorization Request, dated March 8, 2004.

Drafting Team Responses to "No" Votes with Comments

Progress Energy - Carolinas
Electric Generators
Wayne Lewis

Comments:

General Comments:

Since these standards as drafted will introduce additional capital expenses and ongoing operating expenses, a cost impact analysis study should be completed prior to approval by the NERC Board of Trustees to determine the overall magnitude of these costs for the amount of increased security to the impacted systems. NERC and the drafting team have not demonstrated and documented the need for each of these standards or the unnecessarily burdensome and costly documentation trail that they require to provide the required audit capability.

In reviewing the FAQ's, it is recommended that the FAQ's be attached to the standards, since in some cases, they clarify some of the wording of the standards. The FAQ's will be helpful when it is necessary to interpret the meaning of the written standards. By providing FAQ's prior to balloting, they will indirectly, at a minimum, be relied upon for deciding whether or not to approve the standards.

CIP002 – no comments.
CIP003 – no comments.
CIP004 – no comments.
CIP005 – no comments.

CIP006 - R3 – Monitoring physical access - This standard is unworkable unless the wording is clarified that "Unauthorized access attempts shall be reviewed immediately "upon discovery" and handled in accordance with the procedures specified in Requirement CIP-008."

R6.1 – Testing of "all" physical security mechanisms. During formal audits, it is universally accepted to test a sample that should indicate problems rather than "all".

CIP007 – R8 requires a vulnerability assessment of "all" cyber assets within the ESP at least annually. During formal audits, it is universally accepted to assess a representative sample. Considering the "mission critical" nature and specialized characteristics of some of the legacy equipment involved in these environments, it is

Response

The need for Cyber Security Standards was brought to NERC from industry via a Standard Authorization Request (SAR). The SAR was developed into a scope document that was presented for public review and comment. A consensus of reviewers believed the need to move forward with developing cyber security standards per the scope of the SAR was appropriate. The Standards Development Process does not call for a cost/benefit analysis. The risk assessment process is left to the Responsible Entity, who should use reasonable business judgment when implementing these Requirements.

The FAQs will become a NERC reference document.

CIP006 - R3 CIP-008, R1.2 requires Responsible Entities to define response actions. The intent of the requirement in 006 is to implement these response actions immediately, upon receipt of a alarm or other means of discovery. Please see FAQ 6 for CIP-008. The Standards Development Process does not allow for changing Standard at this time.

R6.1 This requirement addresses maintenance and testing over a period of three years, not auditing.

CIP007 -- R8 A comprehensive assessment of all Cyber Assets within the Electronic Security Perimeter is necessary to ensure the security of the Critical Cyber Assets. A weakness in one device can put all Critical Cyber Assets at risk.

extremely labor-intensive and will unnecessarily increase the risk of outages on generating units, substations, and energy control systems to assess "all" assets within the ESP annually without impacting operations. This requirement was not worded this way in draft 3 (i.e., using the word "all"). We either need more time (3 years) to assess all assets within the ESP or we need to be able to assess a representative sample to satisfy this requirement.

CIP008 – no comments.
CIP009 – no comments.

Drafting Team Responses to "No" Votes with Comments

Seminole Electric Cooperative SEC
Electric Generators
Garl Zimmerman

Comments:

The determination of applicable Critical Cyber Facilities is ambiguous, particularly with regard to the interpretation of routable protocol use, as well as "critical assets" subject to the standard. In addition, the proposed standard imposes an unreasonable amount of documentation seemingly solely for the purpose of disproving non-compliance.

Response

CIP-002 R3 and its sub-requirements limit the definition of Critical Cyber Asset. CIP-002-1 FAQ 1 provides guidance on Critical Cyber Asset identification and CIP-002 FAQ 6 provides examples of routable protocols.

The drafting team made every attempt to reduce the amount of documentation necessary to demonstrate compliance. However, the compliance auditing process does rely on documentation to demonstrate compliance, the results of which is improved security for Critical Cyber Assets.

Drafting Team Responses to "No" Votes with Comments

Tampa Electric Company TEC
Electric Generators
John Currier

Comments:

TEC Comments Draft 4 (Draft) For information about my NO vote, please refer to Ron Donahey's comments. In addition, I have the following comments for which we would like clarification.

General Comments Sanctions and Penalties
It is difficult to approve standards without understanding the penalties for non-compliance. We feel that an understanding of potential sanctions and penalties are critical to determining the impact to our corporation.

Compliance Monitoring Process in all standards, Section 1.1.3 This section has been added since draft 3: We want to understand who can be a "third party monitor without vested interest in the outcome for NERC." This is unclear. Can anyone who wants to declare themselves an industry expert third party monitor and be allowed to come in and say they want to audit us or are these 3rd party monitors sent in by NERC on their behalf? Please explain the rationale for this section and perhaps add to the FAQ's

CIP-003 Security Management Requirements
R4 Information Protection -- This section is too vague and can be interpreted in many ways. At what level are you expecting access privileges to be documented? For instance, can we say all transmission personnel may have access to xxx, yyy, and zzz group of documents or do we have to get to the level of classifying each individual document? At a minimum, please clarify the expectations in the FAQ reference document.

CIP-004 Personnel and Training
R3 Personnel Risk Assessment -- Are we expected to do a criminal check in every state a person has lived in during the last 7 years? At minimum please address this question and the rationale for changing from 5-year to 7-years in the FAQ's.

CIP-007-001 Systems Security Management
R1.2 Testing -- Please clarify how to document that testing was performed in a manner that "reflects the production environment." The production environment usually cannot be replicated in a test environment. We are not sure what "reflects" means. For instance

Response

General
Per NERC's VP of Standards, as part of its ERO application, NERC is developing a guideline for the application of penalties. This guideline addresses most if not all of the considerations listed in this comment as suitable reasons for either increasing or decreasing the amount of a financial penalty. The compliance information in the standard itself addresses only the measures for determining whether an entity complied or not, and the levels of non-compliance that are used to determine how severely the entity failed to meet the standard. The remaining factors are general ones that are not specific to each standard, e.g. did the entity self-report, does the entity have a strong compliance program, etc. These factors, along with the financial penalty matrix will be provided in the penalty guidelines provided in the ERO application. The penalty guidelines will eventually become mandatory under approval of FERC and Canadian governmental agencies.

Compliance Monitoring Process - The third-party monitor is the entity that will audit NERC for compliance with these standards. RROs will audit Responsible Entities and NERC will audit RROs.

CIP-003 The Responsible Entity must define its information classification system as it sees fit in accordance with Critical Cyber Asset information protection program.

CIP-004 All states are required. The change from 5 to 7 reflects industry consensus and aligns with the requirements of the Fair Credit Reporting Act.

CIP-007 The Responsible Entity is not expected to control a spare generating unit or simulate the control of generation. CIP-007 FAQs 2 and 3 address this issue.

for systems that control plant generating units - to be like the production environment, we would need to control a "spare generating unit" (have none and this is not practical) or simulate the generation (cost prohibitive -- $2-5M for one simulator at one location, plus the manpower to set up the simulation and keep it current with plant changes). Currently we test logic using spare modules with no I/O that accesses generation units. We perform isolated changes to one area of the plant at a time to limit risks. Additionally we have redundant processes so that we can quickly backout changes if something is not working correctly. We feel these are sufficient testing processes for protecting our assets. Please clarify testing requirements in the FAQ's.

R2 Ports and Services -- For many systems that we have bought from vendors, there is no way to easily identify the ports and services used (or not used) other than through trial and error. While, we can ask vendors to supply us with information our experience has been that they are not certain of the need for various ports and services. Can you provide guidance on how to accomplish this in the FAQs?

R6.5 Security Status Monitoring -- Reviewing logs of all system events is impossible and cannot be done unless you sample the logs; we see little value in doing this. One system log may generate thousands of events daily and there may be hundreds of logs to review daily. Can you please provide some guidance in the FAQ about what level of review is expected?

FAQ's Comments
If this is to be a reference document (and we support that concept), all the items should be correctly worded so they apply to critical cyber assets not critical assets. Many good questions were asked during the January 31st webcast/ conference call, and it would be helpful if the answers to those were included in the final FAQ reference document.

R2 When an open port is discovered, the Responsible Entity should use reasonable business judgment to determine the appropriate state and usage of the port and document it.

R6.5 The requirement does not mandate manual review of all logs; automated processes are acceptable and encouraged.

FAQ's The Drafting Team intends to review the FAQs and correct errors as necessary before it is posted as a NERC reference document.

Drafting Team Responses to "No" Votes with Comments

Carolina Power & Light Company CPL
Brokers, Aggregators, and Marketers
James Eckelkamp

Comments:

General Comments:
Since these standards as drafted will introduce additional capital expenses and ongoing operating expenses, a cost impact analysis study should be completed prior to approval by the NERC Board of Trustees to determine the overall magnitude of these costs for the amount of increased security to the impacted systems. NERC and the drafting team have not demonstrated and documented the need for each of these standards or the unnecessarily burdensome and costly documentation trail that they require to provide the required audit capability.

In reviewing the FAQ's, it is recommended that the FAQ's be attached to the standards, since in some cases, they clarify some of the wording of the standards. The FAQ's will be helpful when it is necessary to interpret the meaning of the written standards. By providing FAQ's prior to balloting, they will indirectly, at a minimum, be relied upon for deciding whether or not to approve the standards.

CIP002 -- no comments.
CIP003 -- no comments.
CIP004 -- no comments. CIP005 -- no comments.

CIP006 - R3 -- Monitoring physical access - This standard is unworkable unless the wording is clarified that "Unauthorized access attempts shall be reviewed immediately "upon discovery" and handled in accordance with the procedures specified in Requirement CIP-008."

R6.1 -- Testing of "all" physical security mechanisms. During formal audits, it is universally accepted to test a sample that should indicate problems rather than "all".

CIP007 -- R8 requires a vulnerability assessment of "all" cyber assets within the ESP at least annually. During formal audits, it is universally accepted to assess a representative sample. Considering the "mission critical" nature and specialized characteristics of some of the legacy equipment involved in these environments, it is extremely labor-intensive and will unnecessarily increase the risk of outages on generating units, substations, and energy control systems to assess "all" assets within the ESP annually

Response

General:The need for Cyber Security Standards was brought to NERC from industry via a Standard Authorization Request (SAR). The SAR was developed into a scope document that was presented for public review and comment. A consensus of reviewers believed the need to move forward with developing cyber security standards per the scope of the SAR was appropriate. The Standards Development Process does not call for a cost/benefit analysis. The risk assessment process isleft to the Responsible Entity, who should use reasonable business judgment when implementing these Requirements.

The FAQs will become a NERC reference document.

CIP006 R3
CIP-008, R1.2 requires Responsible Entities to define response actions. The intent of the requirement in 006 is to implement these response actions immediately, upon receipt of a alarm or other means of discovery. Please see FAQ 6 for CIP-008. The Standards Development Process does not allow for changing Standard at this time.

R6.1 This requirement addresses maintenance and testing over a period of three years, not auditing.

CIP007 -- R8 A comprehensive assessment of all Cyber Assets within the Electronic Security Perimeter is necessary to ensure the security of the Critical Cyber Assets. A weakness in one device can put all Critical Cyber Assets at risk.

without impacting operations. This requirement was not worded this way in draft 3 (i.e., using the word "all"). We either need more time (3 years) to assess all assets within the ESP or we need to be able to assess a representative sample to satisfy this requirement.

CIP008 -- no comments.
CIP009 -- no comments.

Drafting Team Responses to "No" Votes with Comments

Cinergy Corporation CIN
Brokers, Aggregators, and Marketers
Walter L Yeager

Comments:

General Comment: Because so much information is contained in the FAQ's Cinergy suggests that the FAQ's be made part of the standard materials used for compliance guidance.

CIP 002 R1.1. Although NERC published a white paper describing various risk assessment methodologies, little guidance is provided in the standard or FAQ's as to specific expectations for the cyber security risk assessment. Further, sections of the standard seem to suggest physical security measures in response to cyber security threats, which might be identified in the assessment. Cinergy recommends adding a question to the FAQ's or language to the standard clarifying that participants should factor credible threat information the development of their risk assessment focusing on cyber security threats and electronic mitigating measures. It is not expected that participants should protect against all physical threats when implementing their cyber security program.

CIP 004 R4.2 The requirement states, "Responsible Entity shall revoke such access to Critical Cyber Assets within 24 hours for personnel terminated for cause and within seven (7) calendar days for personnel who no longer require such access". Cinergy interprets this requirement to mean that for personnel terminated NOT for cause, participants would have seven (7) calendar days to revoke access.

The levels of non-compliance (Section D.2.2.4) states that any one instance of personnel termination where access is not revoked in 24 hours creates a level 2 violation. The violation seems inconsistent with the requirement as stated, and we do not believe participant should be held to this. Please explain.

D2.3.1 This section prescribes a Level 3 violation if a training program exists but has not been updated annually. In other standards Level 3 and 4 violations are for serious events/omissions which jeopardize reliability. Parts of this standard still measure documentation completeness with no relevance to actual security. We believe a level 3 violation is too severe for the situation where a training program exists and has been implemented, but has not been updated in the last year.

Response

General: The FAQs will become a NERC reference document.

CIP 002
R1.1 Industry consensus does not support a prescriptive risk assessment methodology to identify Critical Assets. Responsible Entities may consider threats when performing its risk assessment.

CIP 004
R4.2 The Drafting Team agrees that the wording in D2.2.4 is an unintentional omission of the phrase “for cause” in the language of the standard. The Drafting Team has developed an errata item correcting this error and will present it to the Standards Authorization Committee for its consideration after approval of these standards for inclusion in the NERC ApprovedStandards Errata Sheet.

D2.3.1
Compliance with these standards will enhance the securityof Critical Assets through the protection of the Cyber Assets essential to their reliable operation, thereby contributing to the reliability of the bulk power systems. The Drafting Team made every attemptto provide tiered levels of non-compliance that reflect increasing severity to reliability. The Standards Development Process does not allow changes at this time.

CIP 006 R2, R3, R4 and R5.
Electronic measures alone are insufficient to meet the physical security Requirements of these standards. A completely enclosed (six-wall) boundary restricts access to Critical Cyber Assets, thereby limiting the number of personnel subject to the administrative requirements of CIP-004. Please refer to CIP-006 FAQ 1.

Drafting Team Responses to "No" Votes with Comments

CIP 006 R2. In each of the preceding drafts Cinergy has expressed operational concerns with implementing the expectation for a 6-wall physical security perimeter, access controls, monitoring, and logging of access, for critical cyber assets in substations that use a routable protocol to communicate outside of the electronic security perimeter. We believe the costs and operational impacts of these physical constraints are out of proportion to the probable risks and modes of cyber attack that might be used. Even though the critical cyber substation assets may represent only a small fraction of the substation assets, all employees who work in the substations would be covered under the administrative rules because it would be impossible to determine which substation employees may be required to work in the critical cyber asset substations. We ask that NERC consider adding language to the standard or to the FAQ's explaining that electronic measures may be sufficient to mitigate physical security requirements.

R3. See comments in R. 2 above.
R4 See comments in R. 2 above.
R5. See Comments in R. 2 above.

CIP 007 D.2.1. Level 1 Noncompliance: Parts of this standard still measure documentation completeness with no relevance to actual security. All levels of non-compliance in CIP 007 relate to documentation. Non-compliance should reflect "real" security issues rather than identifying whether papers have been updated or not. In this section, it is possible that the participant's systems could be fully secure but the participant would receive a non-compliance based solely on updating papers. While some documentation non-compliance may be relevant to prove compliance, this section of CIP 007 should include both actual systems security evaluation and documentation items.

D.2.2. Level 2 Noncompliance: Also, see D.2.1. Level 1 comments above.

D.2.3. Level 3 Noncompliance: In other standards, Level 3 and 4 violations are for serious events/omissions which jeopardize reliability. Also, see D.2.1. Level 1 comments above.

D.2.4 Level 4 Noncompliance: In other standards, Level 3 and 4 violations are for serious events/omissions which jeopardize reliability. Also, see D.2.1. Level 1 comments above.

CIP 007
D.2.1, D.2.2, D2.3, and D2.4
Compliance with these standards will enhance the security of Critical Assets through the protection of the Cyber Assets essential to their reliable operation, thereby contributing to the reliability of the bulk power systems. The Drafting Team made every attempt to provide tiered levels of non-compliance that reflect increasing severity to reliability.

Drafting Team Responses to "No" Votes with Comments

FirstEnergy Solutions FESC
Brokers, Aggregators, and Marketers
Edward C. Stein

Comments:

The following two recommendations are designed to provide the new standard with a "crisp" intent and to remove any ambiguity.

1) CIP-002-1 R3. Critical Cyber Asset Identification — Using the list of Critical Assets developed pursuant to Requirement R2, the Responsible Entity shall develop a list of associated Critical Cyber Assets essential to the operation of the Critical Asset. Examples at control centers and backup control centers include systems and facilities at master and remote sites that provide monitoring and control, automatic generation control, real-time power system modeling, and real-time interutility data exchange. The Responsible Entity shall review this list at least annually, and update it as necessary.

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

R3.1. The Cyber Asset uses a routable protocol to communicate outside the Electronic Security Perimeter; or,
R3.2. The Cyber Asset uses a routable protocol within a Control Center; or,
R3.3. The Cyber Asset is dial-up accessible.

FES Recommendation: FES does not agree with the use of "Control Center" in CIP-002 R3.2 and suggest that it be replaced with "Electronic Security Perimeter". The standard now reads "…Critical Cyber Assets are further qualified to be those having the following characteristics: The Cyber Asset uses a routable protocol within a Control Center …"

FES's interpretation is that as stated this would include any computer or device physically located at a Control Center that has a routable protocol, including both the EMS network and the corporate network. If Control Center in R3.2 were replaced with Electronic Security Perimeter, the intent of the Critical Cyber Asset definition is retained; Facilities, systems, and equipment which, if destroyed, degraded, or otherwise rendered unavailable, would affect the reliability or operability of the Bulk Electric System.

Response

1) CIP-002-1 R3.2 is meant to further qualify or limit the number of Critical Cyber Assets. Changing the verbiage as FE recommends would have the opposite effect.

2) 005-1 R1.2 Any reference to Critical Cyber Assets in CIP-005 refer to the list of Critical Cyber Assets identified in CIP-002. The FAQ has been corrected.

2) CIP-005-1 R1.2. For a dial-up accessible Critical Cyber Asset that uses a non-routable protocol, the Responsible Entity shall define an Electronic Security Perimeter for that single access point at the dial-up device.

FAQ #3 (CIP-005-1 Section) Page 13 of 30
Question: I have a single RTU that controls a critical bulk electric asset in a substation, connected through a modem to my EMS communication front-end. What is the Electronic Security Perimeter in this case? There is no LAN in the substation.
Answer: An Electronic Security Perimeter is required at the master station front-end but only required at the RTU if the RTU uses a routable protocol. RTUs that use a non-routable protocol with a master/slave synchronous polling method that cannot access anything on the EMS, and use SBO (select before operate) command to control devices at the RTU end, do not require an Electronic Security Perimeter. If a dialup modem on a critical bulk electric asset is used for configuration or polling it must be in an Electronic Security Perimeter that is just around the dialup access point (e.g., SCADA-controlled, dial-back, or other technologies that give proper access controls and logging).

FES Recommendation: The FAQ stated above appears to provide an exception to CIP-005 R1.2. It is our opinion that the standard should be clear in its requirements and we recommend that the drafting team consider revising CIP-005 R1.2 to address the ambiguity that exist by incorporating the FAQ response directly into the standard.

Drafting Team Responses to "No" Votes with Comments

Tampa Electric Company TEC
Brokers, Aggregators, and Marketers
Jose Benjamin Quintas

Comments:

For information about my NO vote, please refer to Ron Donahey's comments. In addition, I have the following comments for which we would like clarification.

General Comments
Sanctions and Penalties It is difficult to approve standards without understanding the penalties for non-compliance. We feel that an understanding of potential sanctions and penalties are critical to determining the impact to our corporation.

Compliance Monitoring Process in all standards, Section 1.1.3
This section has been added since draft 3: We want to understand who can be a "third party monitor without vested interest in the outcome for NERC." This is unclear. Can anyone who wants to declare themselves an industry expert third party monitor and be allowed to come in and say they want to audit us or are these 3rd party monitors sent in by NERC on their behalf? Please explain the rationale for this section and perhaps add to the FAQ's

CIP-003 Security Management Requirements
R4 Information Protection This section is too vague and can be interpreted in many ways. At what level are you expecting access privileges to be documented? For instance, can we say all transmission personnel may have access to xxx, yyy, and zzz group of documents or do we have to get to the level of classifying each individual document? At a minimum, please clarify the expectations in the FAQ reference document.

CIP-004 Personnel and Training
R3 Personnel Risk Assessment Are we expected to do a criminal check in every state a person has lived in during the last 7 years? At minimum please address this question and the rationale for changing from 5-year to 7-years in the FAQ's.

CIP-007-001 Systems Security Management
R1.2 Testing Please clarify how to document that testing was performed in a manner that "reflects the production environment." The production environment usually cannot be replicated in a test environment. We are not sure what "reflects" means. For instance

Response

General--Per NERC's VP of Standards, as part of its ERO application, NERC is developing a guideline for the application of penalties. This guideline addresses most if not all of the considerations listed in this comment as suitable reasons for either increasing or decreasing the amount of a financial penalty. The compliance information in the standard itself addresses only the measures for determining whether an entity complied or not, and the levels of non-compliance that are used to determine how severely the entity failed to meet the standard. The remaining factors are general ones that are not specific to each standard, e.g. did the entity self-report, does the entity have a strong compliance program, etc. These factors, along with the financial penalty matrix will be provided in the penalty guidelines provided in the ERO application. The penalty guidelines will eventually become mandatory under approval of FERC and Canadian governmental agencies.

Compliance Monitoring--The third-party monitor is the entity that will audit NERC for compliance with these standards. RROs will audit Responsible Entities and NERC will audit RROs.

CIP-003 The Responsible Entity must define its information classification system as it sees fit in accordance with Critical Cyber Asset information protection program.

CIP-004 Personnel and Training R3 Personnel Risk Assessment The Responsible Entity is expected to ensure that vendors will comply with the requirements of the Standards. A contract arrangement and evidence of compliance from the vendor will be sufficient to demonstrate compliance on the Responsible Entity's part.

The Responsible Entity must revoke authorized access within 24

for systems that control plant generating units - to be like the production environment, we would need to control a "spare generating unit" (have none and this is not practical) or simulate the generation (cost prohibitive -- $2-5M for one simulator at one location, plus the manpower to set up the simulation and keep it current with plant changes). Currently we test logic using spare modules with no I/O that accesses generation units. We perform isolated changes to one area of the plant at a time to limit risks. Additionally we have redundant processes so that we can quickly backout changes if something is not working correctly. We feel these are sufficient testing processes for protecting our assets. Please clarify testing requirements in the FAQ's.

R2 Ports and Services For many systems that we have bought from vendors, there is no way to easily identify the ports and services used (or not used) other than through trial and error. While, we can ask vendors to supply us with information our experience has been that they are not certain of the need for various ports and services. Can you provide guidance on how to accomplish this in the FAQs?

R6.5 Security Status Monitoring Reviewing logs of all system events is impossible and cannot be done unless you sample the logs; we see little value in doing this. One system log may generate thousands of events daily and there may be hundreds of logs to review daily. Can you please provide some guidance in the FAQ about what level of review is expected?

FAQ's Comments
If this is to be a reference document (and we support that concept), all the items should be correctly worded so they apply to critical cyber assets not critical assets. Many good questions were asked during the January 31st webcast/ conference call, and it would be helpful if the answers to those were included in the final FAQ reference document.

hours for cause. There will be occasions when the Responsible Entity makes best effort to recover its keys within 24 hours but is unsuccessful. It is not intended that this situation cause non-compliance; the requirement is to revoke authorized access.

The Responsible Entity is expected to ensure that vendors will comply with the requirements of the Standards. A contract arrangement and evidence of compliance from the vendor will be sufficient to demonstrate compliance on the Responsible Entity’s part.

CIP-005 Electronic Security Perimeters
The Drafting Team made every attempt to provide tiered levels of non-compliance that reflect increasing severity to reliability. The Standards Development Process does not allow for changes to the standards at this time.