Drafting Team Responses to "Yes" Votes with Comments

American Transmission Company LLC ATC

Transmission Owners

Peter Burke

Comments	Responses
Comments on CIP-002 thru -009: CIP-005-1 1. R1.4 requires non-critical cyber assets within the Electronic Security Perimeter to be identified and protected the same as critical cyber assets. This makes no sense and should be removed.	CIP-005 R1.4. addresses controls at access points to the Electronic Security Perimeter. The requirement ensures that those controls also apply to non-critical Cyber Assets that are within this perimeter. A weakness in the controls to any asset within the Electronic Security Perimeter may affect the operation of the Critical Cyber Assets within it. Please refer to the FAQs for CIP-005.
2. R1.5 requires that cyber assets that control access to the ESP be protected according to a list of a bunch of other standards and requirements. This is redundant to the extreme. Why not just include those assets in the definition of critical cyber assets? Then they will automatically be subject to those standards and requirements.	CIP-005 R1.5 While these systems themselves are not Critical Cyber Assets, they are essential to the protection of the Critical Cyber Assets and are therefore, subject to the specified subset of requirements.
CIP-006-1 1. R1.8 has the same problem as CIP-005-1 R1.5 above.	CIP-006-1 R1.8 While these systems themselves are not Critical Cyber Assets, they are essential to the protection of the Critical Cyber Assets and are, therefore, subject to the specified subset of requirements.
CIP-007-1 1. A.3 Purpose makes the standard apply to non-critical cyber assets within the ESP. This goes beyond reasonableness. The words "as well as the non-critical Cyber Assets" should be removed. 2. B Requirements applies the standard to other cyber assets within the ESP. The words "and other Cyber Assets" should be deleted. 3. The requirements say the "Responsible Entity shall comply with the following requirements of Standard CIP-007 for all Critical Cyber Assets ... within the ESP. This seems to imply that every individual device needs to have all the controls outlined in the standard. This needs to be clarified to make it clear that the standard requires control of the access points into the ESP, rather than to each device within the ESP. Change the wording to the "Responsible Entity shall comply with the following requirements of Standard CIP-007 for controlling access to all electronic paths into and out of the ESP."	CIP-007-1 1 and 2. A weakness in the controls to any Cyber Asset within the Electronic Security Perimter may affect the operation of the Critical Cyber Assets within it. Thus, the purpose and the requirements are appropriate.CIP- 005 addresses requirements for the perimeter and CIP-007 addresses requirements inside the perimeter.

Drafting Team Responses to "Yes" Votes with Comments

Boston Edison Company BECO

Transmission Owners

Charles Salamone

Comments

NSTAR Electric comments:

General Comment - The definition of Critical Assets in Draft 4 needs further clarification. The definition used for the CIP Standards should be consistent with the definition of citical assets that is used in the NERC Guidelines. The definition for a critical facility is outlined in the overview section of version 1.0 of the "Security Guidelines for the Electric Sector. It reads: "For purpose of these guidelines, a critical facility may be defined as any facility or combination of facilities, if severely damaged or destroyed, would have a significant impact on the ability to serve large quantities of customers for an extended period of time, would have a detrimental impact to the reliability or operability of the energy grid, or would cause risk to public health and safety."

CIP-004 - Personnel Risk Assessments should be required for all new individuals seeking access to critical locations. Waivers should be allowed for all current employees who have been in their current position/access to the Critical Location for 3 years, with no reported incidents.

CIP-006 - Sub Station Card Access - Due to implementation costs, this standard should be introduced as Guideline for 3 years, before being instituted as a standard.

Responses

General The definition in these standards reflects industry consensus, and once approved, will be added to NERC's Glossary of Reliability Terms.

CIP-004 Personnel risk assessments are required for all new individuals. Waivers are allowable only for personnel who have had a personnel risk assessments within the last 7 years.

CIP-006 Card access is only one of the acceptable means of meeting the requirements for physical access controls.

Drafting Team Responses to "Yes" Votes with Comments

Central Lincoln Peoples Utility District

Transmission Owners

Ronald Beck

Comments	Responses
This body of work has come along way since it's original draft and truly reflects the efforts of the drafting team to respond to and address feedback. While not perfect, it is worthy of approval.	

Drafting Team Responses to "Yes" Votes with Comments

Central Maine Power Company CMP

Transmission Owners

David Mark Conroy

Comments

I vote "Affirmative" based on the understanding that these standards apply to the control center, and do NOT apply to the realm outside the control center.

Responses

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

Drafting Team Responses to "Yes" Votes with Comments

Con Edison Company of New York CEPD

Transmission Owners

Edwin Thompson

Comments

The vote of "YES" is based on the assumption that there will not be substantial changes in the implementation plan which would shorten the published proposed schedule.

Responses

No changes have been made to Implementation Plan.

Drafting Team Responses to "Yes" Votes with Comments

Great River Energy GRE

Transmission Owners

Gordon Pietsch

Comments

CIP-007-R2: GRE does not believe mandating the management of ports and services of critical cyber assets is necessary if they reside with a secure electronic perimeter.

CIP-007-R5.3: GRE believes that strong authentication is critical to maintaining security of critical cyber assets instead of the use of passwords. If this is not possible, passwords should be greater than 8 characters and rotation should occur more frequently than annually regardless of risk.

Responses

CIP-007-R2:The standard as worded is supported by industry consensus built during three rounds of public review and comments.

CIP-007-R5.3 Responsible Entities may implement stronger controls than required by these standards; for example, they may choose to use 8 character passwords instead of the minimum 6 required by these standards.

Drafting Team Responses to "Yes" Votes with Comments

Hydro-Quebec HQT

Transmission Owners

Michel Armstrong

Comments

HQ TransEnergie recognizes the substantial effort made by the drafting team for the development of these standards.and HQ TransEnergie agrees with the standards but would like to submit the following comments: -standards must clear and at the same time provide entitites with sufficient flexibility to provide practical and effective means for implementation to assure the grid reliability.The publication of a document as a reference,like FAQ, would help to assure a consistent interpretation and application of the requirements.

CIP-007-1 requires annual port reviews of cyber critical assets inside the security perimeters.This annual port review is required for those micro-processor based relays that control critical assets.There are automated methods of performing this task.Depending on what type of communication protocol is being used at the device ports it may render this device a "non-critical cyber asset"Clarification should be published on which micro-processor relay inside security peimeters should be considered critical cyber assets. -

There should be for every requirements a corresponding level of non compliance for example CIP-003, R 3.2 Thank you for the opportunity to comment.

Responses

The FAQs will become a NERC reference document.

Responsible Entities will determine Critical Assets based upon their own risk assessment process, from which Critical Cyber Assets are then identified.

Industry consensus does not support the suggested detailed levels of non-compliance.

Drafting Team Responses to "Yes" Votes with Comments

International Transmission Company

Transmission Owners

Jim Cyrulewski

Comments

The term "six-wall" in CIP-006-1, Requirement R1.1 can be confusing and lead to suggest to some that extensive construction changes are necessary to meet the standard. Would suggest eliminating the term and just state the concept.

Responses

It is not the intent to require extensive construction, however, depending on the Responsible Entity's configuration and cost/benefit analysis, construction may be an option. Please refer to FAQs.

Drafting Team Responses to "Yes" Votes with Comments

LIPA LIPA

Transmission Owners

Richard Bolbrock

Comments

CIP-006-Physical Security R1. Physical Security Plan Section R1.8 essentially requires that Cyber Assets used in the access control and monitoring of the Physical Security Perimeter(s) be afforded the same protective measures as Critical Cyber Assets. By requiring this, they are effectively becoming part of the Critical Cyber asset inventory which is defined as assets "...essential to the reliable operation of critical assets." Is that the intent of this section?

R3. Monitoring Physical Asssets Section R3 states taht "Unauthorized access attempts shall be reviewed immediately and handled in accordance with the procedures specified in Requirement CIP-008." There are many occasions when unauthorized company personnel swipe their access badges at enttrances to the physical security perimeter not knowing that their access is restricted. Is the intent of this requirement to perform an immediate investigation each time this happens? This seems excessive if the unauthorized access has not been achieved. Please clarify.

CIP007 - Systems Security Management R5. Account Manaagement Section 5.1 refers to "individual and shared" system accounts whereas Section R5.1.2 simply refers to "individual user" accounts. What is the purpose of this distinction?

Responses

CIP-006, R1.8 contains the requirement for Cyber Assets used in the access control and monitoring of the Physical Security Perimeter(s), which are not as inclusive as the requirements for Critical Cyber Assets. Cyber Assets used in the access control and monitoring of the Physical Security Perimeter are not required to be on the list of Critical Cyber Assets, otherwise, they would be subject to all requirements of CIP-002 through CIP-009.

CIP-008, R1.2 requires Responsible Entities to define response actions. Please see FAQs for CIP-008.

CIP007 The intent in R5.1.2 is to track usage of each user account. The intent is further clarified in R5.2.3.

Drafting Team Responses to "Yes" Votes with Comments

Manitoba Hydro

Transmission Owners

Robert George Coish

Comments

In CIP-004-1, Requirement R2 to provide annual training for all personnel having authorized access to Critical Cyber Assets would be better stated as each responsible Entity has an annual plan for training which forms the basis for compliance audits. Consider such a comment if the standards open for revision, as this training can be provided in economical manner.

In general, CIP-002-1 through CIP-009-1 move the industry toward better security at a relatively consistent rate. But the FAQ indicates that manual discovery of access points could be used to meet Requirement 4.3 in CIP-005-1. This seems inordinately weak in comparison to the rest of the standards. Please explain how manual discovery (i.e. visual inspection as opposed to the use of IT tools) could reliably discover unauthorized, previously unknown, wired network access points within an existing network infrastructure?

Regarding CIP-007-1 Requirement R3, Security Patch Management, if a utility contended that they had adequate mitigations in place to justify very infrequent patching of some critical cyber assets (e.g. once a year or less), how would a NERC audit judge this?

Responses

Evidence of annual training for all personnel who have access to Critical Cyber Assets is required. The standard is not open for revision at this time.

Requirement 4.3 in CIP-005-1 The requirement allows for either manual or automated processes, which reflects industry consensus to address the potential danger of unintentional impacts to the operation of Critical Cyber Assets from the use of automated tools to discover access points.

CIP-007-1 Requirement R3 The requirement is to assess each patch and, in the case where a patch is not installed, the Responsible Entity must document compensating measures or acceptance of risk relative to that specific patch. A general plan that states patches will only be installed once a year would not meet the intent of the requirement.

Drafting Team Responses to "Yes" Votes with Comments

National Grid USA Transmission NEP

Transmission Owners

Peter Henry Lebro

Comments

National Grid is casting an affirmative vote in acknowledgement of the importance of Cyber Security, and this standard's important contribution to control room security. However, we have very serious concerns about this standard's usefulness with regard to substations. A one-size fits all approach to control rooms and substations is inappropriate. This standard should apply to control rooms only, and a separate standard should be developed for substations with substantial involvement of transmission owners and equipment manufacturers. For substations, the standard is process/compliance oriented, and not results driven. The cost to implement does not correspond to the benefits achieved. Annual training for a large percentage of field staff is excessive. The increased interaction with / inspection of relay and control schemes as specified by this standard could result in inadvertent trips, exposing the system to increased risk without corresponding benefit. The concept of ensuring communication circuit security only to the substation fence can result in a false sense of security. Collaboration with telecommunication circuit providers in the development of this standard should be considered. The NERC Glossary of Terms contains no definition of a control center. Our proposed definition is: "The central facility or facilities of a responsible entity where remote monitoring, operating, and/or controlling of elements of the bulk electric system are or can be performed in real time.

Responses

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.

These standards do rely on documentation to demonstrate compliance, the results of which is improved security for Critical Cyber Assets.

Training is only required for personnel with unescorted access to Critical Cyber Assets.

Invasive interaction is not required. The standard states that reasonable business judgment should be used when assessing these devices.

The SAR, based on industry input, also excluded telecommunications infrastructure between Electronic Security Perimeters.

The Standards Development Process does not allow the addition of new definitions to these Standards at this time.

Drafting Team Responses to "Yes" Votes with Comments

New York Power Authority NYPA

Transmission Owners

Ralph Rufrano

Comments

Regional Issues; â€¢ Some NPCC experts believe that 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. â€¢ CIP-007-1 requires annual port reviews of Cyber Critical Assets "inside" the security perimeter(s). These ports are basically potential electronic access points on the devices which should be at least documented and reviewed. These ports appear on microprocessor based relays that have been identified to control Critical Assets. There are a number of outstanding issues with annual port review with the most important being the process of generating the required annual information from the relay, which may have to be done locally at the device. Some have noted that in the past, procedures such has this have led to inadvertent trips and can degrade reliability from that which we have today. It was reported that presently we have Regional requirements to check these ports at least once every 6 years, not annually. Others noted that there are automated methods of performing this task that would not subject the system to any vulnerability while still others believe that many of these devices, depending on what type of communication protocol is being used at the device ports may render the device a "non-critical cyber asset". At the very least, all those commenting with their ballot should request clarification on which microprocessor relays that reside inside security perimeters should be considered Critical Cyber Assets. â€¢ Also concern was expressed over training required for people working in the substations that would need physical or cyber access. This will require that they receive background screening and specific training. Some indicated that a very large number of people have access to substations and installations outside of the Control Center. Specialized training for these people could prove to be prohibitively high in dollars and resources for little recognized benefit. â€¢ At a higher level, concern was also expressed by many about whether these standards will enhance or contribute to the reliability of the Bulk Power System in North America.

Responses

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.

Responsible Entities must determine which microprocessor relays are Critical Cyber Assets per CIP-002. The requirements addressing other Cyber Assets within the Electronic Security Perimeter are contained in CIP-005, R1.4.

Invasive interaction is not required. The standards state that reasonable business judgment should be used when assessing these devices.

Training is only required for personnel with unescorted access to Critical Cyber Assets.

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.

Drafting Team Responses to "Yes" Votes with Comments

New York State Electric and Gas Corporation NYET

Transmission Owners

Henry G Masti

Comments

We have two comments: 1) The Implementation Plan for Table 3. (Compliance Schedule for Standards CIP 002-1 through CIP 009-1. Interchange Authorities, Transmission Owners, Generator Owners, Generator Owners, Generator Operators, and Load- Serving Entities) identifies a first milestone date of December 31, 2006. For all the requirements except one this would be the milestone date for BW or Beginning Work. This date is 6 months earlier than any other group's first milestone date. Yet the remaining milestone dates are 6 months later. We would recommend that the first milestone date be moved out 6 months to be in line with the other tables. Since there is going to be significant discussions and training regarding the understanding and interpretation of the new standards, we believe that there will be insufficient time following the training and discussions to develop and approve a plan to address the requirements and begin implementation. This is especially true for this group since they have not been required to be self certified under UA Standard 1200. 2) There have been significant discussions and concerns expressed regarding the implementation of the Permanent Standards for remote sites such as substations. These discussions have focused on the cost, regarding administrative and training issues as well as patch management and testing requirements for remote sites versus the benefit as compared to a Control Center. We certainly would not object to NPCC's comments regarding setting up a separate Standard Authorization Request (SAR) to address the cyber security at these remote sites. However at a minimum we strongly recommend that these issues and concerns be further discussed and addressed to ensure that there is a clear understanding of what is required to achieve the level of Cyber Security required in a cost effective manner.

Responses

1) Responsible Entities affected by the latest functional model registration need more time to get from start to finish in implementing these standards. The Begin Work phase of the plan means that an entity has given thought to how it will approach implementing the standards and has documented that approach. The BW date as shown gives these entities time to begin estimating budgetary impacts of implementing the standards and to get those estimates into their budgetary process as soon as possible. Then, they have adequate time to complete their implementation and become auditably compliant with the standards. For these reasons, the drafting team believes this schedule is appropriate.

2) 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. Industry consensus does not suggest additional discussion at this time.

Drafting Team Responses to "Yes" Votes with Comments

Orange & Rockland NYOR

Transmission Owners

Edward Michael Olsen

Comments

The vote of "Yes" is based on the assumption that there will not be substantial changes in the implementation plan which would shorten the published proposed schedule.

Responses

No changes have been made to Implementation Plan.

Drafting Team Responses to "Yes" Votes with Comments

Potomac Electric Power Company PEPW

Transmission Owners

Richard Kafka

Comments

1. (Revised) Implementation Plan (Feb 3, 2006): The February 3 revisions corrected most of Table 3 registrant requirements from preceding Table 1 and Table 2 registrants required dates, The first column of Table 3 is still earlier than the first column of Table 1 and Table 2 (i.e. need to begin work on all requirements and be substantially compliant for CIP-003 R2 six months prior to Table 1 and 2). 2. CIP-002-1 R 1.1 and R1.2: While not the intent of the Drafting Team (per the January 31 web cast/conference call), it's possible that an entity could rule all of their assets out of scope depending on their risk based assessment methodology and the phrase "reliable operation of the Bulk Electric System" because the electric system is operated to withstand a single contingency. As discussed a cyber event has the potential of exceeding a single contingency. To ensure consistency across the electric industry, either the RROs or expand on CIP-002 FAQ 7 should address this issue. 3. CIP-002-1 R 1.2.3: Because of FERC Code of Conduct rules, GO or GOP can not easily make this assessment (i.e. should not have knowledge of reliable operation of the Bulk Electric System). Either ISO, RRO, TO, and/or TOP should make this assessment and communicate to GO or GOP. Recommend that RROs take lead in oversight for critical assets (generation, bulk transmission). 4. CIP-002-1 R 1.2.3: In the case where there is a different GO and GOP for a plant, who has responsibility for complying with the standards? Recommend that the GO has this responsibility. 5. We support the Drafting Team's recommendation to NERC that the FAQs be adopted as a reference document. It is important that the FAQs are kept as a reference document to understand the intent of the standards. This will assist in having consistency in performing the annual audits.

Responses

1. No changes have been made to Implementation Plan. Responsible Entities affected by the latest functional model registration need more time to get from start to finish in implementing these standards. The Begin Work phase of the plan means that an entity has given thought to how it will approach implementing the standards and has documented that approach. The BW date as shown gives these entities time to begin estimating budgetary impacts of implementing the standards and to get those estimates into their budgetary process as soon as possible. Then, they have adequate time to complete their implementation and become auditably compliant with the standards. For these reasons, the drafting team believes this schedule is appropriate.

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

3. Industry consensus does not support a prescriptive methodology to identify Critical Assets. However, these standards do not preclude coordination with other functional model entities with a shared interest.

4. As stated in the drafting team’s responses to comments on Draft 3, Responsible Entities are responsible for compliance with these standards. Responsibility for compliance should be determined by specific agreements and contracts between the parties. The FAQ CIP-002 Question 10 has been updated.

5. The drafting team will submit the FAQ for inclusion as a NERC reference document.

Drafting Team Responses to "Yes" Votes with Comments

Public Service Electric and Gas Company

Transmission Owners

Colin John Loxley

Comments	Responses
Support PJM comments	Please see responses to Bruce Balmat.

Drafting Team Responses to "Yes" Votes with Comments

SaskPower SPC

Transmission Owners

Wayne Guttormson

Comments

SaskPower RELUNCTANTLY votes yes on this standard. In general, SaskPower feels that this standard focuses too much on HOW to do things (codifying details) as opposed to WHAT is required for maintaining reliability (performance requirements). These standards also rely too heavily on documentation being required, instead of focusing on productive work being accomplished. As well, the compliance levels are excessively high. The levels of non-compliance do not fairly reflect the potential impact on the reliability of the grid; they are generally set too high. Comments on Definitions: Physical Security Perimeter: The definition of a Physical Security Perimeter should be changed. Phrase "other locations in which Critical Cyber Assets are housed and for which access is controlled". This statement is not clear. It is impractical to construct the six-walled boundary within substations, generation facilities and other locations. Comments on CIP-002 002_R1: R1.2.7 "Any additional assets" is not clear; it should be change to specific or third party critical assets or eliminate the term "additional critical assets" since they are outside the BES definition. Comments on CIP-004 004_R1: R1 Cyber Security Awareness reinforcement is required quarterly, in addition to the annual training requirements of R2. The quarterly awareness reinforcement is too much and excessive, it should be change to bi-annually or annually. "Contractors or service vendors" sometimes work less than 3 months, will they have to go for awareness reinforcement training? Awareness should be a part of training. 004_R2: R2.1. Eliminate R2.1 it is redundant to R2.2. R2.2 clearly mentions that training should be given to "appropriate to personnel roles and responsibilities". 004_R3: Suggest that the correct order from R1 to R4 is R3 (risk assessment), R2 (training), R1 (awareness), and R4 (access). Comments on CIP-005 005_R4: R4 - Why is this requirement separated from CIP-007-1- R8? Drawing a distinction between being on or within the perimeter is arbitrary for this requirement. Would these requests ever be implemented or review separately? It should be combined in one standard. Comments on CIP-007 General Comments: Note there is a reference made to the Cyber Vulnerability Assessment in both CIP-005 and CIP-007. CIP-005 relates to 'electronic access points', while CIP-007 relates to 'Cyber Assets within the Electronic Security Perimeter.' These points in both standards look the same. It should be combined in one standard.

Responses

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.

Definitions: It is not the intent to require construction, however, depending on the Responsible Entities configuration and cost/benefit analysis, construction may be an option. Please refer to FAQs.

CIP-002_R1: R1.2.7 The intent is to provide the Responsible Entity the opportunity to consider assets beyond those described in the standard when conducting a risk assessment.

CIP-004_R1: Awareness is not intended to be rigorous. Please see FAQs CIP-004, 4.

004_R2: R2.1.These are not duplicative, they provide more detail.

004_R3: The Standards Development Process does not allow changes at this time.

005_R4: R4 005 addresses requirements for the perimeter and 007 addresses requirements inside the perimeter.

CIP-007 General Comments: 005 addresses requirements for the perimeter and 007 addresses requirements inside the perimeter.

Drafting Team Responses to "Yes" Votes with Comments

Southern California Edison SCET

Transmission Owners

Dana Cabbell

Comments

As laid out in Standard CIP-002, each Responsible Entity is to evaluate and identify its own Critical Assets and there is no sharing of this role between the Generator Owner and the Reliability Coordinator and Balancing Authority. Requirement R1.2.3 is subjective and can lead to critical generating facilities being deemed a non-Critical Asset to the detriment of reliable transmission operations. Such a determination of whether certain generating facilities are needed to support the reliable operation of the Bulk Electric System should be made in consultation with the Reliability Coordinator and Balancing Authority. Reliability Coordinators, Balancing Authorities and Transmission Operators have been tasked with ensuring the reliable operation of the system through standards contained within the functional model and language in CIP-002 appears to be contrary to what is contained in these approved reliability standards.

Responses

Industry consensus does not support a prescriptive methodology to identify Critical Assets. However, these standards do not preclude coordination with other functional model entities with a shared interest.

Drafting Team Responses to "Yes" Votes with Comments

United Illuminating UICO

Transmission Owners

Robert James Pellegrini

Comments

Section CIP-005-1 Electronic Security Perimeter. UI Comment: The below section seems to add additional testing and exposure to BPS protective relays in which the relays will need to be accessed and evaluated annually. This would add significant resource requirements and also require the assets to be evaluated annually. UI feels that this requirement is un-necessary since it would add additional exposure and increase the possibility of an inadvertent trip of equipment thereby working against the spirit of the Cyber security standard which is to increase reliability of the BPS. UI asks for clarification with respect to BPS microproprocessor relays which are used for monitoring via Ethernet or dial up and not part of control via SCADA. UI feels that the added exposure of testing relays every year (as opposed to six year test cycle) is not in the spirit of the standard. Please clarify. R4. Cyber Vulnerability Assessment -- The Responsible Entity shall perform a cyber vulnerability assessment of the electronic access points to the Electronic Security Perimeter(s) at least annually. The vulnerability assessment shall include, at a minimum, the following: R4.1. A document identifying the vulnerability assessment process; R4.2. A review to verify that only ports and services required for operations at these access points are enabled; R4.3. The discovery of all access points to the Electronic Security Perimeter; R4.4. A review of controls for default accounts, passwords, and network management community strings; and, R4.5. Documentation of the results of the assessment, the action plan to remediate or mitigate vulnerabilities identified in the assessment, and the execution status of that action plan.

Responses

R4 requires assessment of the perimeter devices. Invasive interaction is not required. The standards state that reasonable business judgment should be used when assessing these devices.

Drafting Team Responses to "Yes" Votes with Comments

Xcel Energy

Transmission Owners

Gregory Pieper

Comments

D2.3.1 on CIP-005 should say "Critical CYBER Asset", instead of just "Critical Asset".

Responses

The Drafting Team agrees that this is an unintentional error in the language of the standard. The Drafting Team has developed an errata sheet correcting this error as suggested and will present the errata sheet to the Standards Authorization Committee for its consideration after approval of these standards.

Drafting Team Responses to "Yes" Votes with Comments

ISO New England Inc ISNE

RTOs, ISOs, and RROs

Kathleen Goodman

Comments

ISO New England strongly supports the initiative to provide industry controls for security of critical cyber assets. The existing Urgent Action (1200) Cyber Security Standard requirements represented a major first step for the industry to take in regard to providing cyber security for our critical assets. ISO New England supports the uniform application of the cyber standards represented in CIP-002-1 through CIP-009-1 on all entities that perform system reliability and dispatch functions related to the Reliability Coordinator, Balancing Authority, and Transmission Operator functions, that are typically found at a major dispatch control center facility. In the context of New England, that would apply to the ISO New England Control Center, and our five (5) Local Control Centers. By focusing the new standards on this discrete set of entities, ISO New England would also suggest that the vagaries introduced in these standards, which allow for "…reasonable business judgment…" to be applied regarding the applicability of these standards to a broad spectrum of entities, could be eliminated by focusing the uniform application of these standards on all control center entities noted above. Further, while ISO New England does support these standards, we feel that they remain unclear and open to vague interpretation in some requirements. Such key requirements are: 1.CIP002, R3 – The description leads us to believe that cyber assets within a stand-alone (electronically-islanded) network using a routable protocol for intra-communications only would not be considered critical cyber assets. However the WebEx teleconference implied that these could be critical cyber assets. We believe the wording of R3 should be clarified to ensure consistent interpretation. 2.CIP005, General – The purpose of this standard states that it is intended to identify and protect the cyber assets that comprise the electronic security perimeter, and the access points through the perimeter. However references to "device within the electronic security perimeter" could be construed to be referencing cyber assets bound by the perimeter, as opposed to just part of the perimeter. Such references (i.e. R1.1, etc) should be clarified to speak only of the perimeter devices. For the remaining entities identified in the Functional Model, we believe these standards, as written, are too broad and would introduce inefficiencies and unnecessary costs into the cyber security process. ISO New England recommends that the current Urgent Action (1200) Cyber Security Standard requirements be applicable to all other entities under the Functional Model by a date certain, and we suggest June 1, 2007 as a reasonable implementation date. These entities have been on notice of this existing set of standards and many of them have taken steps toward compliance or are already in compliance with the Urgent Action (1200) Cyber Security Standard. If it is found that more prescriptive Cyber Security standards are required by this subset of entities under the Functional Model,

Responses

Cyber assets within a stand-alone (electronically islanded) network using a routable protocol for intra-communications only would not be considered critical cyber assets unless they are in a control center.

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.

The Standards Development Process does not allow the addition of new definitions to these Standards at this time.

The Standards Development Process allows for this and ISO NE can submit a SAR at its discretion.

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.

new standards can be drafted that are directly applicable to their functions within the industry. To summarize, we suggest the following: 1) Standards (CIP-002-1 through CIP-009-1) should apply only to Control Centers performing the Reliability Coordinator (RC), Balancing Authority (BA) or Transmission Operator (TOP) functions. (2) The Definition of 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" concurrently be adopted into the Glossary of Terms to support implementation of this Standard(s). (3) Initiate a standards development process that would lead to the development of additional Cyber Security Standards, consistent with Urgent Action (1200) Cyber Security Standard requirements, to be applicable to all other entities under the Functional Model, with such standards to be established by a date certain in the reasonably near future. Securing the Control Centers (RC, BA, TOP) provides the best immediate Return On Investment for the security gain expected to be achieved by implementation of these Standards. ISO New England believes that 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.

Drafting Team Responses to "Yes" Votes with Comments

MAAC

RTOs, ISOs, and RROs

Bruce Balmat

Comments

CIP-002-01: The term "Control Center" in R3.2 needs to be taken out of the requirement in order to match the intention of the drafting team to not include corporate business LANs.

CIP-004-01: In the "Levels of non-compliance" section, items 2.1.5, 2.1.6, and 2.2.4 refer to a single instance of not performing a requirement which we regard as unrealistic and severe. We recommend that these items be made less prescriptive.

CIP-005-01: The following comment was provided by FirstElectric and is a good one, apparently there was some confusion about the FAQ actually being an exception to the Standard. Might be a good idea to Copy and Paste the text below when submitting your votes.

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.

Per question 3 of the FAQs on page 13 of 30 the answer to the FAQ appears to contradict this requirement. The FAQ response seems to indicate the dial-up device described in R1.2 would not be classified as a Critical Cyber Asset.

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).

Responses

CIP-002-01 R3 and its sub-requirements identify Cyber Assets that are essential to the operation of Critical Assets and were not intended to include business networks.

CIP-004-01: 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-005-01: The FAQ is an implementation guide, which will become a NERC reference document. The standard itself cannot contain examples.

No changes have been made to Implementation Plan.

Drafting Team Responses to "Yes" Votes with Comments

NERC Webcast (1/31) Comments: Response was that the FAQ document will be included as part of the approved standards, and the answer listed in the FAQ related to CIP-005-1, R1.2 would be considered an exception, even though the exception is not listed in the standard.

Recommendation: It is our opinion that the standard should stand on its own and not require an exception from a FAQ that will be forgotten about in years to come.

Implementation Plan: We are voting "Yes" on the Implementation Plan in good faith that the plan will not be adjusted at a later date to require earlier compliance with the Standards.

Drafting Team Responses to "Yes" Votes with Comments

Midwest Independent Transmission System Operator, Inc.

RTOs, ISOs, and RROs

Terry Bilke

Comments

Even though we are voting yes, we have significant concerns with this standard. This standard has nearly 100 items for which non-compliance can be assessed, a quarter of which are assigned level 4 (most severe). Most of the requirements in this standard are administrative and have no direct or immediate impact on reliability. While the cyber security process is very important, an entity should be graded in context of the whole rather than penalizing 100 different things. We raised these same concerns in comments to the standard. Our original comments to the drafting team were not given notice. We probably would have abstained, but the balloting process does not accept comments with abstentions. We're voting yes with the hope and expectation that there will be some reasonableness in the application of the standard.

Responses

The Drafting Team made every attempt to provide tiered levels of non-compliance that reflect increasing severity to reliability.

Drafting Team Responses to "Yes" Votes with Comments

Midwest Reliability Organization

RTOs, ISOs, and RROs

William J. Head

Comments

The compliance levels are excessively high. The levels of non-compliance do not fairly reflect the potential impact on the reliability of the grid; they are generally set too high. These standards rely too heavily on documentation being required, instead of focusing on productive work being accomplished. D2.3.1 on CIP-005 should say "Critical CYBER Asset", instead of just "Critical Asset".

Responses

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.

D2.3.1 on CIP-005 The Drafting Team agrees that this is an unintentional error in the language of the standard. The Drafting Team has developed an errata sheet correcting this error as suggested and will present the errata sheet to the Standards Authorization Committee for its consideration after approval of these standards.

Drafting Team Responses to "Yes" Votes with Comments

New York Independent System Operator NYIS

RTOs, ISOs, and RROs

Gregory Campoli

Comments

The NYISO supports these standards. However, we recognize that asset owners within the NYCA and NPCC believe that a separate SAR and standard(s) should be developed specific to assets outside of Control Centers and that the implementation plan for the balloted standard be updated to indicate that the CIP -- 002 -> 009 be assessed for control centers only. We respect and support those asset owners' perspectives.

Responses

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 "Yes" Votes with Comments

Ontario - Independent Electricity Market Operator IMO

RTOs, ISOs, and RROs

Don Tench

Comments

The IESO congratulates the Drafting Team for their work in the development of these standards.

IESO's Ballot Position on Standards CIP-002-1 to CIP-009-1: "Affirmative but with Comments"

While recognizing the substantial effort made by the drafting team in developing these standards, and recognizing that comments with an affirmative vote are not typically part of the ballot process, we nevertheless provide the following comments to record concerns with the Standards as written and further, recommend they be addressed at the first revision of the Standards subsequent to formal adoption.

Comments:

1. In some cases these Standards define requirements for which there is no corresponding compliance statement. This creates the possibility of confusion, as a Responsible Entity may not fulfill all requirements yet would be unable to determine which level of non-compliance to report.

For instance, in CIP-003, requirement R3.2 requires that, "documented exceptions to the cyber security policy must include an explanation as to why the exception is necessary and any compensating measures, or a statement accepting risk." However, there is no non-compliance level defined for the case where the Responsible Entity fails to fulfil this requirement. A Responsible Entity which does not comply with Requirement R3.2 should not claim full compliance, yet would be unable to find the appropriate level of non-compliance to report. The Standards should provide Responsible Entities with guidance on how to report such situations.

2. Requirement R3 CIP-004 should be revised to require a personnel risk assessment before personnel are granted authorized cyber access or permitted unescorted physical access to critical cyber assets or cyber assets on or within the electronic security perimeter.

3. As a general rule, the frequency at which entities are required to review and update documentation, and the permissible time between a system change and a documentation

Responses

1. Industry consensus does not support the suggested detailed levels of non-compliance. Furthermore, this specific example is covered under the levels on non-compliance, 2.1.2 as an incomplete exception would not be considered compliant.

2. 30 days reflects industry consensus. The Responsible Entity may implement stricter requirements.

3. The Standards Development Process does not allow the standards to be changed at this time.

4. No changes have been made to Implementation Plan.

revision, should not be arbitrarily prescribed in these standards. In most instances, a suitable documentation review frequency and update latency should be determined and documented by Responsible Entities based on risk management considerations. An appropriate Measure would be the presence or absence of a documented review frequency / update latency, with compliance being demonstrated by document review or update being performed within the defined time.

4. Our “Affirmative” vote is based on our understanding that the Implementation Plan will not be adjusted at a later date to require earlier compliance with the Standards.

In addition, in support of the standards, the IESO offers the following comments regarding concerns we understand may be expressed by some that application of the standards to Responsible Entities other than “control centers” is "excessively broad” and offers “minimal improvements to reliability":

It is a maxim in the security business that one’s physical and cyber security are only as strong as the weakest link. It is precisely for this reason that the CIP Standards need to apply to entities other than just “control centers”. We operate power systems, and as such, need to take a systems approach to protecting their functionality. There is no point in having a functioning control center if there is nothing to control. The application of the Standards to all entities with “Critical Assets” will supports the IESO’s Reliability Compliance Program (IRCP).

For entities with Critical Assets, the Standard requires protection for only those components that are either critical assets themselves, or which could, if they failed, affect critical assets. The standards include wording that provides entities with sufficient flexibility that they need not expend resources protecting physical or cyber assets which are not important for grid reliability. In particular, the following wording is used:

“These standards recognize the differing roles of each entity in the operation of the Bulk Electric System, the criticality and vulnerability of the assets needed to manage Bulk Electric System reliability, and the risks to which they are exposed. Responsible Entities should interpret and apply Standards CIP-002 through CIP-009 using reasonable business judgment. ” (emphasis added)

In addition, while Responsible Entities are expected to create a policy framework that is consistent with the requirements of the Standard, they can, in virtually all cases, grant themselves policy exceptions. The wording used in the standards is similar to the following: “Instances where the Responsible Entity cannot conform to its cyber security policy must be documented as exceptions and approved by the designated senior manager or delegate(s). . . . . Duly authorized exceptions will not result in non-compliance.

Drafting Team Responses to "Yes" Votes with Comments

In the IESO's view, these words provide Responsible Entities with considerable flexibility so that they can indeed allocate resources sensibly while still being in full compliance with the Standards as written.

We again thank the standards drafting team for their considerable efforts and commend the team for the many improvements incorporated in this most recent draft.

The IESO appreciates the opportunity to table these comments and looks forward to participating further in the standards development process.

Drafting Team Responses to "Yes" Votes with Comments

Southwest Power Pool SWPP

RTOs, ISOs, and RROs

Charles Yeung

Comments

SPP commends the standards drafting team with the completion of these 8 standards as presented, but would like to add the following comments:

General: A slight variation on the numbering scheme would be helpful, pointing a specific standard to the CIP in which it appears. For example: 3-R5.1 would be CIP 3, requirement 5.1. It would save time (and space) while navigating within each standard and when referencing the standards from other documents.

Standard CIP-002-1: Critical Cyber Asset Identification R3 and others: When a reliability function (e.g., Reserve Sharing) is outsourced to an entity such as OATI, how can or should the requirements of the standards be applied?

Standard CIP-003-1: Security Management Controls R5.1 / R5.1.1 It is better practice to assign approval authority by role or position rather than by name. This is a Social Engineering preventative control.

Standard CIP-004-1: Personnel and Training R3.3: What constitutes adequate documentation for vendors and contractors? If a Responsible Entity considers a statement from the vendor/contractor company as sufficient, will (or can) that decision be overridden?

Standard CIP - 005-1: Electronic Security Perimeter(s) R3.2 This requirement will be interpreted to mean that attempts at unauthorized accesses mean focused efforts, not general "noise" that is common on the Internet.

Standard CIP - 006-1: Cyber Security - Physical Security R3: The requirement to perform immediate reviews of "unauthorized access attempts" will be interpreted to apply in a commercially reasonable way-insofar as occupying leased space and resource limitations make strict compliance extremely difficult and/or expensive.

Standard CIP - 007-1: Systems Security Management
R4.2: Since anti-virus signature updates are automatic and monitored, this requirement would actually reduce, not increase, security. Testing signatures is not feasible; systems remain unprotected during the testing phase, and there is no viable "back out" procedure.

Responses

General: The numbering is part of the standards template and cannot be changed by the drafting team.

Standard CIP-002-1
As stated in the drafting team's responses to comments on Draft 3, Responsible Entities are responsible for compliance with these standards. Responsibility for compliance should be determined by specific agreements and contracts between the parties. The FAQ CIP-002 Question 10 has been updated.

Standard CIP-003-1
Named approval authority may be considered protected information and handled appropriately.

Standard CIP-004-1:
The Responsible Entity must use reasonable business judgment to determine what is adequate to meet the requirements and demonstrate compliance. Compliance audit processes are outside the scope of these requirements.

Standard CIP - 005-1:
The Responsible Entity should consider this when developing its processes in R3.

Standard CIP - 006-1
The Responsible Entity should use reasonable business judgment when developing its processes in R3.

Standard CIP - 007-1
The requirement does not mandate testing before updating anti-virus signatures.

The Standards Development Process does not allow the

Drafting Team Responses to "Yes" Votes with Comments

R5.3.1: While it is understood that policies can be stricter than what the standard requires, an 8 character password should be the minimum acceptable, with exceptions needed in instances when fewer characters are permitted.

R5.3.3: Annual password changes might be acceptable in automated applications where no individual has access to the account, but that is excessive for individual accounts. It would be better to have separate requirements for automated and individual accounts, with a maximum of 90 day passwords for individual users.

Standard CIP - 008-1: Incident Reporting and Response Planning No comments

Standard CIP - 009-1: Recovery Plans For Critical Cyber Assets R1.2 We take this to mean we can assign the roles and responsibilities of responders by job title, not by name.

standards to be changed at this time.

The Standards Development Process does not allow the standards to be changed at this time.

Standard CIP - 009-1
This is a reasonable interpretation.

Drafting Team Responses to "Yes" Votes with Comments

Manitoba Hydro MHEB

Load-Serving Entities

Ronald Dacombe

Comments	Responses
In CIP-004-1, Requirement R2 to provide annual training for all personnel having authorized access to Critical Cyber Assets would be better stated as each responsible Entity has an annual plan for training which forms the basis for compliance audits. Consider such a comment if the standards open for revision, as this training can be provided in economical manner.	Evidence of annual training for all personnel who have access to Critical Cyber Assets is required. The standard is not open for revision at this time.
In general, CIP-002-1 through CIP-009-1 move the industry toward better security at a relatively consistent rate. But the FAQ indicates that manual discovery of access points could be used to meet Requirement 4.3 in CIP-005-1. This seems inordinately weak in comparison to the rest of the standards. Please explain how manual discovery (i.e. visual inspection as opposed to the use of IT tools) could reliably discover unauthorized, previously unknown, wired network access points within an existing network infrastructure?	The requirement allows for either manual or automated processes reflecting industry consensus to address the potential danger of unintentional impacts to the operation of Critical Cyber Assets from the use of automated tools to discover access points.
Regarding CIP-007-1 Requirement R3, Security Patch Management, if a utility contended that they had adequate mitigations in place to justify very infrequent patching of some critical cyber assets (e.g. once a year or less), how would a NERC audit judge this?	The requirement is to assess each patch and, in the case where a patch is not installed, the Responsible Entity must document compensating measures or acceptance of risk relative to that specific patch. A general plan that states patches will only be installed once a year would not meet the intent of the requirement.

Drafting Team Responses to "Yes" Votes with Comments

MidAmerican Energy Company MEC

Load-Serving Entities

Thomas C. Mielnik

Comments

On behalf of MidAmerican Energy, I vote yes for the Cyber Security Standards with the following comments:

1. The compliance levels are excessively high. The levels of non-compliance do not fairly reflect the potential impact on the reliability of the grid; they are generally set too high.

2. These standards rely too heavily on documentation being required, instead of focusing on productive work being accomplished.

In spite of these concerns, I vote yes for the Cyber Security Standards.

Responses

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 "Yes" Votes with Comments

Niagara Mohawk NMPC

Load-Serving Entities

Michael Schiavone

Comments

1. The Standards as written are "one size fits all" and are not appropriate for the disparity of assets that exist at the Control Center and substation.

2. NMPC believes that there is a greater return on investment and potential benefit to confine these standards to the Control Center.

3. NMPC believes that there is a greater chance of inadvertent trips related to the increased human interaction with Critical Cyber Assets at the substation level that these Standards require, thereby potentially reducing or degrading the level of reliability that would be experienced otherwise.

4. Annual training seems overly excessive. One time training and periodic awareness training would be more appropriate.

5. NMPC believes that there is a higher level of risk that a cyber incident at a Control Center could have more wide spread impact to the Bulk Electric System (BES) than a cyber incident at a remote BES facility. The standards as written don not reflect this.

6. 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.

NMPC recommends the following to address the above comments.

1. Standards CIP-002-1 through CIP-009-1 should only be applied to a Responsible Entities Control Center(s). Therefore modify the Implementation Plan so that the Standards apply to Control Centers only.

2. The existing Standard CIP-002-1 through CIP-009-1 should be modified to focus on Control Centers Only.

3. A new Standard should be developed for a Responsible Entities Critical Cyber Assets beyond the Control Center.

Responses

1.The standards were written to accommodate a diverse industry.

2.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.

3.Invasive interaction is not required. The standard states that reasonable business judgment should be used when assessing these devices.

4.Annual training is necessary to reinforce sound security practices. Awareness complements training.

5.These standards are intended to protect Critical Cyber Assets regardless of location. A Responsible Entity's risk assessment will determine where these assets reside.

6.Continued development of tools for these purposes is expected over time.

Response to Recommendations:
1.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.

2.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.

3.The Standards Development Process allows for this and Niagara Mohawk can submit a SAR at its discretion.

Drafting Team Responses to "Yes" Votes with Comments

4. There is currently no definition in the NERC Glossary of Terms for Control Center. NMPC Proposes the following definition: Control Center definition: 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.	4.The Standards Development Process does not allow the addition of new definitions to these Standards at this time.

Drafting Team Responses to "Yes" Votes with Comments

Public Service Electric and Gas Company

Load-Serving Entities

Jeff Mueller

Comments

PSE&G supports the comments submitted by PJM.

Responses

Please see response to Bruce Balmat.

Drafting Team Responses to "Yes" Votes with Comments

Salt River Project SRP

Load-Serving Entities

John Underhill

Comments **Responses**

No comments.

Drafting Team Responses to "Yes" Votes with Comments

Wisconsin Public Service Corporation WPS

Load-Serving Entities

James Maenner

Comments

The compliance levels are excessively high. The levels of non-compliance do not fairly reflect the potential impact on the reliability of the grid; they are generally set too high. These standards rely too heavily on documentation being required, instead of focusing on productive work being accomplished.

Responses

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 "Yes" Votes with Comments

Grant County PUD No.2 GCPD

Transmission Dependent Utilities

Kevin John Conway

Comments

GCPD casts an affirmative vote for this issue. GCPD understands the needs for these standards, however due to the many cyber systems, both from a business and reliability perspective, the fact that different organizational business units manange them sometimes to other standards. The fact is that there are more standards organizations other than NERC that regulate these other business units, there is an increasing disconnect in how to meet all the needs since cyber systems are interconnected, and/or housed in common locations. Several times policies have been implimented in our organization only to discover they violate or do not fully meet other standards from other standards orgainzations. GCPD feels that NERC should only focus on those standards that deal directly with reliability, and work through the other standards organizations when it feels standards in cyber and physical security of cyber assets are needed.

Responses

Cyber security is a fundamental component of bulk power system reliability. These standards are intended to protect Critical Cyber Assets that are essential to the reliable operation of Critical Assets associated with the Bulk Electric System.

Drafting Team Responses to "Yes" Votes with Comments

Constellation Generation Group

Electric Generators

Michael Gildea

Comments

If compliance costs (cyber in this case) become significant, competitive generation must find a new vehicle to capture these additional costs.

Responses

We thank you for your observation.

Drafting Team Responses to "Yes" Votes with Comments

Lincoln Electric System LES

Electric Generators

Dennis Florom

Comments

LES agrees with the standards in principle, however, we believe that the required measures are too detailed in nature, and predispose even entities with prudent and complete security programs to call out exceptions.

Responses

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 "Yes" Votes with Comments

Manitoba Hydro Marketing MHEM

Electric Generators

Gerald Koroscil

Comments	Responses
In CIP-004-1, Requirement R2 to provide annual training for all personnel having authorized access to Critical Cyber Assets would be better stated as each responsible Entity has an annual plan for training which forms the basis for compliance audits. Consider such a comment if the standards open for revision, as this training can be provided in economical manner.	Evidence of annual training for all personnel who have access to Critical Cyber Assets is required. The standard is not open for revision at this time.
In general, CIP-002-1 through CIP-009-1 move the industry toward better security at a relatively consistent rate. But the FAQ indicates that manual discovery of access points could be used to meet Requirement 4.3 in CIP-005-1. This seems inordinately weak in comparison to the rest of the standards. Please explain how manual discovery (i.e. visual inspection as opposed to the use of IT tools) could reliably discover unauthorized, previously unknown, wired network access points within an existing network infrastructure?	The requirement allows for either manual or automated processes reflecting industry consensus to address the potential danger of unintentional impacts to the operation of Critical Cyber Assets from the use of automated tools to discover access points.
Regarding CIP-007-1 Requirement R3, Security Patch Management, if a utility contended that they had adequate mitigations in place to justify very infrequent patching of some critical cyber assets (e.g. once a year or less), how would a NERC audit judge this?	The requirement is to assess each patch and, in the case where a patch is not installed, the Responsible Entity must document compensating measures or acceptance of risk relative to that specific patch. A general plan that states patches will only be installed once a year would not meet the intent of the requirement.
In reference to Table 3 of the Revised Implementation Plan, completion of the "Begin Work" phase should be changed from December 31, 2006 to "end of 2nd Qtr 2007". As Table 3 entities will just be registering this spring, an extra 6 months would allow a more reasonable timeframe to plan budgets and resources to meet the "Begin Work" requirements. This change would also provide a better time alignment with the Begin Work phase for Other Facilities of Table 1. Table 1 entities have been registered for some time and would be more prepared for compliance.	No changes have been made to Implementation Plan.

Drafting Team Responses to "Yes" Votes with Comments

United States Bureau of Reclamation

Electric Generators

Deborah M. Linke

Comments

CIP-002-1 Cyber Security -- Critical Cyber Asset Identification
We would suggest that Regional Councils work with their members to identify critical assets to the bulk power system. They are in the best position; based on overall knowledge of the power system, contingencies, flow studies, etc., to make such an assessment. Expecting the individual entities to consistently and appropriately identify critical assets is an unreasonable expectation. Once the Councils have acted to identify critical bulk power assets, the identification of the associated critical cyber assets should be simplified and more effective.

CIP-004-1 Cyber Security -- Personnel and Training The risk assessment period was extended to 7 years in the recent draft. Government entities subject to this requirement, such as Reclamation, will need to work with Office of Personnel Management to extend the normal investigation timeframe beyond the 5 years normally employed. We would suggest going to a 5 year investigation period for both initial and re-review periods for consistency with normal federal background check periods.

CIP-007-1 Cyber Security -- Systems Security Management Requirement R8 addresses cyber security vulnerability assessment in some detail. It is unclear, however, whether such testing needs to be conducted on the actual operational system or whether a test system (configured and managed like the operational system) can be employed to meet the assessment requirements. We would suggest that testing of "backup" or equivalently configured systems be acceptable in meeting this requirement for safety and continuity of operations reasons. Although this same argument could be made for the perimeter assessment discussed in CIP-005-1 (R4), the threats and risks at these entry points should be expected and a more robust posture could be expected to be present. For this reason, live testing may be a more appropriate approach.

Responses

CIP-002 Industry consensus does not support a prescriptive methodology to identify Critical Assets. However, these standards do not preclude coordination with the RROs.

CIP-004 This version of the standards was changed to 7 years in response to industry comments. A 5-year assessment period is more restrictive and will not violate the standard's requirement as long as the Responsible Entity can demonstrate there are no gaps in the periodic personnel risk assessments.

CIP-007 The requirement (R8) addresses vulnerability assessments (not testing) of the production environment.

Drafting Team Responses to "Yes" Votes with Comments

US Army Corp of Engineers Northwestern Division

Electric Generators

Karl Bryan

Comments

The Cyber Security Standard needs to recognize that the US Army Corps of Engineers (as well as other Dept. of Defense generation sites) may not be able to fully disclose compliance with the standard. Disclosure may be prohibited due to National Security laws or military regulations. So this needs to be recognized when these facilities are audited. karl

Responses

The Drafting Team encourages US Army Corp of Engineers to work with the Compliance Monitor to address this issue.

Drafting Team Responses to "Yes" Votes with Comments

Con Edison Company of New York CEPD

Brokers, Aggregators, and Marketers

Rebecca Adrienne Craft

Comments

The vote of "YES" is based on the assumption that there will not be substantial changes in the implementation plan which would shorten the published proposed schedule.

Responses

No changes have been made to Implementation Plan.

Drafting Team Responses to "Yes" Votes with Comments

Manitoba Hydro Electric Board MHEB

Brokers, Aggregators, and Marketers

Daniel C Prowse

Comments

In CIP-004-1, Requirement R2 to provide annual training for all personnel having authorized access to Critical Cyber Assets would be better stated as each responsible Entity has an annual plan for training which forms the basis for compliance audits. Consider such a comment if the standards open for revision, as this training can be provided in economical manner.

In general, CIP-002-1 through CIP-009-1 move the industry toward better security at a relatively consistent rate. But the FAQ indicates that manual discovery of access points could be used to meet Requirement 4.3 in CIP-005-1. This seems inordinately weak in comparison to the rest of the standards. Please explain how manual discovery (i.e. visual inspection as opposed to the use of IT tools) could reliably discover unauthorized, previously unknown, wired network access points within an existing network infrastructure?

Regarding CIP-007-1 Requirement R3, Security Patch Management, if a utility contended that they had adequate mitigations in place to justify very infrequent patching of some critical cyber assets (e.g. once a year or less), how would a NERC audit judge this?

Responses

Evidence of annual training for all personnel who have access to Critical Cyber Assets is required. The standard is not open for revision at this time.

Requirement 4.3 in CIP-005-1 The requirement allows for either manual or automated processes reflecting industry consensus to address the potential danger of unintentional impacts to the operation of Critical Cyber Assets from the use of automated tools to discover access points.

CIP-007-1 Requirement R3 The requirement is to assess each patch and, in the case where a patch is not installed, the Responsible Entity must document compensating measures or acceptance of risk relative to that specific patch. A general plan that states patches will only be installed once a year would not meet the intent of the requirement.

Drafting Team Responses to "Yes" Votes with Comments

PSEG Energy Resources & Trade LLC PS

Brokers, Aggregators, and Marketers

James Hebson

Comments

PSEG concurs with the comments submitted by PJM.

Responses

Please see responses to Bruce Balmat.

Drafting Team Responses to "Yes" Votes with Comments

Sacramento Municipal Utility District SMUD

Brokers, Aggregators, and Marketers

E. Nick Henery

Comments

Great Job!!

Responses

Drafting Team Responses to "Yes" Votes with Comments

Corporate Risk Solutions, Inc.

Small End-Use Customers

Philip Scott Sobol

Comments

Tremendous effort by the team. Good work.

Responses