Drafting Team Responses to General Comments

Commentor Bob Wallace

Entity Ontario Power Generation

Comments

We have some General Comments. This form has no place for General Comments. In the future, all such forms should have a place for General Comments.

- Some of the following standards require approval or signature by "senior management" or "executive management." OPG often has need or reason to delegate that task. Those requirements should be amended so that a designee may approve or sign. The first example is CIP-002 Requirement R4. The corresponding Measures should be modified to stay in synchronization with their Requirements.

- The second version of these standards were posted without notification. This impeded our review significantly. In the future only one version should be posted. We commented on the January 24 document.

Responses

Noted.

References to designated delegate have been added.

Noted.

Commentor Bryan L Singer

Entity Rockwell Automation, Chairman ISA SP-99

Comments

I do not believe the majority of NERC's Cyber Security Standards CIP--002--1 through CIP--009--1 are ready to ballot at this time, because they do not adequately address a key segment of our country's critical power infrastructure - generation control systems.

I have examined the draft standards as part of my role in developing technical reports, recommended practices and standards for manufacturing and control systems security, as a part of the Instrumentation, Systems, and Automation Society's SP99, "Manufacturing and Control System Security" standards committee.

I am the chairman of this effort, and a representative of many other areas within the industry. As part of Rockwell Automation, I am also the leader in security services and am active in developing and implementing consistent approaches to improve the reliability and cyber-security of the process controls environment. As a long time professional in security of electronic and computer based systems, I am very active in this community as we come to a new realm of understanding about the issues that face process control systems. ISA is interested in consistency with other standards, where appropriate, to avoid end user confusion and an impossible challenge for manufacturers of control systems equipment. To that end, we are working with Tom Flowers of your CSSWG to establish a liaison process that would allow such considerations to be addressed earlier in the process. However, you have asked for comments at this time, and we believe these issues need to be addressed now, before issue, for the standard to be effective.

In addition to the direct impact on generation, generation control systems, if not adequately addressed, become additional "back door" electronic avenues that can compromise the bulk grid that the NERC standard/s appear to be focused on protecting. The standard/s should either acknowledge they do not cover the generation aspects of our

Responses

Generator Operators are included in the list of applicable entities and Generation control systems are addressed by these standards. Please see the drafting team's responses to Joe Weiss. The drafting team will forward your interest in a closer relationship to NERC. Please recognize that NERC has open meetings and encourages participation from all interested parties.

critical power infrastructure, or add information on how to treat it.

Wholesale application of typical business systems security approaches to control systems is not appropriate. The ISA SP-99 committee was founded and continues to proceed largely upon this basis. We have assembled over 200 companies across many faces of the industry, representing over 250 individual members. We have all united with the common purpose of developing a singular standard which will contribute to the industry as a whole by providing a consistent and thorough approach to control systems security. SP99 was created to provide guidance on how to apply security to control systems. Substantial guidance has been published by the SP99 committee, and has been available since April of 2004. It should be referenced in the NERC standard.

Additionally, given that we have many members from across the industry, including members from other areas of the electrical and power generation community, we recommend a closer relationship between ISA SP-99 and the NERC. A closer relationship is essential to ensure that no competing standards or conflicting information is released that will degrade the goals of the industry as a whole.

Joe Weiss, a member of ISA's SP99 , and NERC 's CSSWG, has provided specific comments and recommended revisions which address these concerns. Those comments should be responsibly addressed.

Commentor Carol L. Krysevig

Entity Allegheny Energy Supply Company

Comments

1. Why was the reference to penalties/sanctions removed from the Standards without being mentioned as a change from the Urgent Action Standard 1200?

2. There are still a significant number of items in this draft that don't take into account the environment, physical and electronic, of a power station. If someone accesses the "physical perimeter" of a power station, they would be able to cause an outage, through "non-cyber" means, if sufficiently motivated regardless of the kinds of cyber precautions undertaken.

This standard should concentrate on preventing "cyber" attacks from locations outside the "physical perimeter" and "electronic perimeter".

Therefore, in order to not create non-uniform requirements between cyber and non-cyber security requirements, the exact means of accomplishing this should be determined by the responsible entity.

Prescriptive requirements as defined in the sections of this standard should not be mandated, but rather moved to separate document of "potential safeguards" or "frequently asked questions".

Responses

NERC changed the Standard template, which was pointed out in the Development Highlights.

These standards are for protection from cyber attacks. Physical security of Critical Cyber Assets is addressed as this is part of a good cyber security program. However, the larger issue of physical security of assets such as a power station are not within the scope of these standards.

Cyber attacks can be perpetrated by insiders within the physical and/or the electronic perimeters. These standards address that risk without prescribing the processes, procedures, or technologies that Responsible Entities implement to accomplish the goal of mitigating that risk.

Drafting Team Responses to General Comments

Commentor Dennis Kalma

Entity AESO

Comments

Should be a reference that these standards should be read as a group e.g.: See also CIP002-009

Responses

Reference has been added.

Commentor Edwin C. Goff III

Entity Progress Energy

Comments

Add a definition of routable protocol. FAQ 7 refers to OSI layer 3, as the definition. This could be construed to include field bus devices such as smart transmitters, and other field input devices, located through out a typical power plant or sub station. Field bus protocols such as Foundation Fieldbus, Profibus, and Device Net, which are used for communication between field instruments and Control processors should be excluded. These field devices pose no greater security threat than conventional hard wired field devices connected to a control processor or RTU.

GENERAL COMMENT FOR CIP-002-1 THROUGH CIP-009-1:
Comment 1 -- Consider using the following in all standards: The guidance included in the CIP Cyber Security Standards are applicable to Critical Cyber Assets where technically feasible and when supported by the operating system and software applications unless implementation of these controls cause system performance degradation to a level that causes adverse impact to reliable operation of Critical Assets.

Comment 2 -- Overall there appears to be significant administrative burden attributed to record keeping, largely for auditing purposes rather than enhancement of cyber security. This burden becomes significant largely due to newly defined processes and mandated frequency of reviews.

Comment 3 -- This version has introduced new processes that are far beyond those of the 1200 standards such that even entities which were substantially compliant under 1200 will find it very difficult to be compliant with the new standards given the implementation plan of these standards becoming effective October 2005 and then certifying compliance in 1st Qtr 2006.

Responses

The FAQ has been updated to address common protocols such as Profibus and Modbus. Refer to FAQ, page 4.

Technical feasibility has been added where appropriate.

The drafting team believes documentation and auditing are important aspects of cyber security.

Please see Draft 2 of the Implementation Plan. Auditable compliance differs by Applicable Entity, by Standard and Requirement.

Commentor Francis J. Flynn, Jr., PE

Entity National Grid USA

Comments

National Grid has some General Comments. This form has no place for General Comments. In the future, all such forms should have a place for General Comments.

Responses

Noted.

Drafting Team Responses to General Comments

- Some of the following standards require approval or signature by "senior management" or "executive management." Some Responsible Entities delegate that task. Those requirements should be amended so that a designee may approve or sign. The first example is CIP-002 Requirement R4. The corresponding Measures should be modified to stay in synchronization with their Requirements.	References to designated delegate have been added
- The second version of these standards were posted without notification. This impeded our review significantly. In the future only one version should be posted. We commented on the January 24 document.	Noted.
Review of all Requirements and Measures must be performed by the drafting team. Throughout the document there are inconsistancies between requirements and measures. The drafting team must resolve all these inconsistancies. They are to numerous to mention. The drafting team must look at them all. We find that the defined measures are requirements and should be detailed as requirements.	Requirements and Measurements have been aligned

Commentor Guy Zito

Entity NPCC CP9

Comments	*Responses*
NPCC Participating Members have some General Comments. This form has no place for General Comments. In the future, all such forms should have a place for General Comments.	Noted.
- Some of the following standards require approval or signature by "senior management" or "executive management." Some Responsible Entities delegate that task. Those requirements should be amended so that a designee may approve or sign. The first example is CIP-002 Requirement R4. The corresponding Measures should be modified to stay in synchronization with their Requirements.	References to designated delegate have been added.
- The second version of these standards were posted without notification. This impeded our review significantly. In the future only one version should be posted. We commented on the January 24 document.	Noted.
A general statement that applies to all the Cyber Security Standards is that the Measures, Requirements and Levels of non-Compliance need to be reviewed/revisited to ensure there is consistency. The drafting tem should ensure that with ALL these standards, additional requirements aren't being introduced in the compliance section. A requirement should have a measure and associated levels of non-compliance associated with not meeting it. These levels must be carefully reviewed to identify and prioritize which are really critical to Cyber Security, i.e. documentation in some instances is not as critical to the reliability of the Bulk Power System as evaluating incidents. The corresponding levels of non-compliance should individually be reviewed and reflect this.	Requirements, Measurements, and Levels of Non-compliance have been aligned.

Drafting Team Responses to General Comments

Commentor James W. Sample

Entity California ISO

Comments

1)The group of standards still looks inconsistent in a number of areas:
a) There are a number of instances where a requirement is established in one standard which covers the same ground as requirements in another standard, and where contradictory requirements result;
b)The numbering of sections remains inconsistent;
c) The time periods prescribed for activities such as document review and document revision are still inconsistent across the CIP 002 to 009 group of standards.
d) It is clear that a professional technical writer has not looked at these standards to make it clear and homogenous.

These inconsistencies have caused much time to be wasted by review teams which is regrettable considering it could have been easily solved.

2) If an entity is found not to have properly identified its critical infrastructure in 002, will this, ipso facto, mean being assessed as non-compliant in the other remaining standards (since all other standards are built on the assumption that the entities' lists of critical cyber assets are definitive?

3)The set of standards does not clearly require a security and governance program if it is determined that there are no critical assets. The standards must require that a program exist regardless of whether critical assets exist. The standard should state that the entity must perform an annual review to reconfirm its position on cyber assets. As such, the order of 002 and 003 should be reversed.

4) Most references to unattended facilities do not seem to bear relevance on security measures to critical cyber assets. The requirement for making a distinction between attended and unattended assets should be reviewed.

Furthermore, if this distinction is deemed necessary, definitions should be provided for the term unattended. It is not clear whether a facility that is continuously monitored, or a facility that is manned frequently, but not continuously, is unattended.

5) Throughout these standards there are numerous instances where requirements are effectively first established in the Measures and/or Levels of Non-Compliance sections of the text. This is inappropriate. If a condition needs to be met to be fully compliant, that condition should be identified in the Requirements section. In particular, it should not be necessary to read descriptions of non-compliance to infer the requirements for full compliance.

6) In several of the draft standards, there are instances where levels of non-compliance are described in such a way that entities could simultaneously satisfy the conditions of more than one level of non-compliance. Levels of non-compliance should be described as a set of mutually exclusive conditions in order to avoid confusion and inappropriate certification.

7) Requirements related to authorizing, controlling, monitoring, and auditing electronic and physical access to critical cyber assets are specified in several different standards. This is confusing at best, and has resulted in both duplication and contradiction. All requirements pertaining to access control should be specified in one standard for better consistency and clarity.

Responses

1. The drafting team has addressed inconsistencies between and within standards, and aligned Requirements and Measures. Draft 3 was reviewed by technical editors.

2. If a Responsible Entity does not properly document its findings that it has no Critical Cyber Assets, and further does not comply with the other standards in the suite (CIP-003 through CIP-009), it will be found out of compliance with those standards.

3. The drafting team has received comments from many entities that do not believe they must institute a formal security program if they do not own Critical Cyber Assets. Per the requirements of CIP- 002, all Applicable Entities must affirm their list of critical cyber assets annually.

4. References to unattended facilities have been removed.

5. The drafting team has addressed inconsistencies between and within standards, and aligned Requirements and Measures. Draft 3 was reviewed by technical editors.

6. Levels of Non-compliance have been reviewed and better aligned with Requirements and Measures.

7. Requirements are identified in the standard pertaining to each facet of cyber security. This can result in the appearance of duplication, but is not actually the case.

8. Time frames have been standardized.

9. The standards do contain some prescriptive requirements based on the drafting team's experience in the industry. Prescriptive requirements have been kept to a minimum and the use of risk-based assessments is provided for, in fact required, wherever possible.

10. Data retention has been standardized in most cases to one full calendar year.

Drafting Team Responses to General Comments

8) As a general rule, the frequency at which entities are required to review and update documentation should not be arbitrarily prescribed in these standards. Rather, the review frequency should be determined and documented by those entities based on risk management considerations. An appropriate Measure for such a requirement would be the presence or absence of a documented review frequency, with compliance being demonstrated by document review/update being performed at that defined frequency.

9) In a number of places, these standards are very prescriptive and appear to be inconsistent with, or at least appear not to contemplate, the application of a risk based approach to meeting an overall goal. Because of the high degree of specificity, some requirements may not be applicable to all Responsible Entities, and the intent of other requirements may be fully satisfied without meeting the requirement as worded. In situations where the intent of the requirement (or the purpose of the standard) can be satisfied without meeting the specific wording of one or more requirements, entities should be permitted to claim full compliance provided they document their rationale for doing so.

10) In a number of Standards, the text of the Data Retention portion of the Standard (under Compliance) contradicts the text in the subsequent Additional Compliance Information Section of the same Standard.

Commentor Jim Hansen

Entity Seattle City Light

Comments	***Responses***
The term 'Authorized Access' is used in CIP-004,005, and 006 but not defined here. Please add a definition for this term, and specifically describe whether it is intended to mean authorized electronic access, physical access, or both. This would help us understand the intent of these sections. It may be appropriate to spell out physical or electronic (or both) where appropriate in the standard. Training requirements for staff granted authorized physical access but not electronic access would be different than staff granted both for example. If this term means physical access, it would be helpful if exemptions (such as escorted visitors) or any special circumstances were identified.	Authorized Access is a commonly used term in the Information Technology arena. It is understood to mean access that has been approved, whether for physical or electronic access. Authorized access is used in the standards and deals both with physical access and with electronic access. The requirements pertaining to authorized access are identified separately in CIP-005 (Electronic Security) and CIP-006 (Physical Security). The Responsible Entity's training program should address the different needs of physical versus electronic access authorization.
CIP-002 to 009: Please tie measures to the pertinent requirements. This will assist us in insuring our compliance with these standards.	
CIP-002 to 009: Please match compliance levels to specific measures. This will assist us in insuring we are aware of our current level of compliance.	Requirements, Measurements, and Levels of Non-compliance have been realigned in each standard.
CIP-002 to 009: There are overlaps and inconsistencies in some cases since different groups within the drafting team wrote these standards. For example in CIP-005 M5.1 Organizational controls are part of the measurement in this section but are already specified and measured in CIP-003. We recommend that a professional technical writer who can correct these problems in order to avoid causing confusion and unnecessary expense review these standards in total.	Technical writers have reviewed the Draft 3 standards.

Drafting Team Responses to General Comments

Commentor	Jim Hiebert
Entity	California ISO

Comments	***Responses***
Please tie measures to the pertinent requirements. This will assist us in insuring our compliance with these standards.	This comment has been addressed.
Please match compliance levels to specific measures. This will assist us in insuring we are aware of our current level of compliance.	This comment has been addressed.
There are overlaps and inconsistencies in some cases since different groups within the drafting team wrote these standards. For example in CIP-005 M5.1 Organizational controls are part of the measurement in this section but are already specified and measured in CIP-003. We recommend that a professional technical writer who can correct these problems in order to avoid causing confusion and unnecessary expense review these standards in total.	The drafting team has addressed inconsistencies between and within standards, and aligned Requirements and Measures. Draft 3 was reviewed by technical editors.
The term 'Authorized Access' is used in CIP-004,005, and 006 but not defined here. Please add a definition for this term, and specifically describe whether it is intended to mean authorized electronic access, physical access, or both. This would help us understand the intent of these sections. It may be appropriate to spell out physical or electronic (or both) where appropriate in the standard. Training requirements for staff granted authorized physical access but not electronic access would be different than staff granted both for example. If this term means physical access, it would be helpful if exemptions (such as escorted visitors) or any special circumstances were identified. Suggested definition would be: Access that is granted according to an established scheme of governance.	Authorized Access is a commonly used term in the Information Technology arena. It is understood to mean access that has been approved, whether for physical or electronic access. The type of access being discussed is inferred by the standards in which the term is used.
Should clearly correlate 'Requirements' to 'Measures' and 'Measures' to 'Compliance'. This way there is a clear relationship all the way from requirements to compliance. Currently it is hard to correlate this and it appears that in several cases they don't correspond with each other.	This comment has been addressed.
The term 'shall' is used in both the 'Requirements' and 'Measures' sections. The term 'shall' should only be used in the 'Requirements' section and the 'Measures' section shouldn't use 'shall' but rather performance language.	This comment has been addressed.
This standard should be broken up into two distingue standards. One with specific requirements for Control Systems and one with specific requirements for plants and sub-stations. This standard seems to be more focused on Control Systems where the requirements seem to fit very well, however, due to the technology, etc. at plants and sub-stations, these requirements don't fit as well. Also, there is a different risk model for Control Systems versus plants and sub-stations. Due to the risk difference there are should be distingue requirements for each.	The standards will remain as one set addressing both control systems and plants/substations. The implementation plan has been revised to better recognize the time required to comply for plants/substations. The risk model used by a Responsible Entity for identifying Critical Assets and Critical Cyber Assets is to be chosen by the Responsible Entity and can be different for different types of facilities.
Technical feasibility – along the lines of the comments above in 3, if this standard isn't separated between Control Centers, plants, and sub-stations it should take into consideration the technical feasibility of the requirements and annotate it so that the 'exception to standard' overhead doesn't get out of hand. We don't want to make this counter productive by creating a massive about of paperwork administration not allowing us to focus on the spirit of the standard.	References to technical feasibility have been added.

Drafting Team Responses to General Comments

Commentor Joe Weiss

Entity Kema

Comments

NERC identifies this as the Permanent Cyber Security Standard. However, the Drafting Team and other NERC CIPC members agree that this is simply a minimum starting point. Many utilities and others that are not part of the NERC process will read the NERC Website and assume this is the final document since it is named the Permanent Standard. Consequently, NERC needs to either change the title to something such as Interim Cyber Security Standard or this Standard needs to address significantly more items in much more detail.

From an equipment perspective, there has been a blurring of the distinction between transmission and distribution, particularly above 15- 69KV. There are distribution applications above the classic definition of bulk being 35KV or above. Consequently, the term bulk could result in precluding the review of critical equipment that could have a potential impact on the bulk electric grid. Additionally, communications is a critical path for cyber vulnerabilities of Critical Cyber Assets. There have been actual cases where cyber impacts on communications have resulted in cyber impacts on bulk critical assets. Therefore, I would make the following suggestion under Applicability in each section:

Applicability
Include a risk-based approach to determine the applicability of all electronic assets that are interconnected to the bulk electric grid including those explicitly excluded if the risk warrants.

Responses

The word "Permanent" was used to differentiate the CIP-002 through 009 standards from the Urgent Action Standard 1200. The urgent action provision requires the standard to expire after 24 months. Conversely, the "permanent" standard is one that does not have a finite expiration date and will remain in effect until it is replaced.

Noted.

Commentor John Lim

Entity Con Edison

Comments

Since there is no place for overall/general comments, the following applies to all standards:

The high level numbering of requirements and measures must match. This is true in some standards, but in others, the numbering in the measures do not match requirements.

While the changes in the standards are highlighted in a separate document, they will be easier to follow in a change section at the beginning of each standard as a preamble to the standard itself.

The standards expressly exclude nuclear facilities. In the absence of cyber security standards for nuclear facilities, does this exclusion not introduce a considerable vulnerability in the overall reliable operation of the bulk electric system? It is generally understood that any Federal requirement which are more stringent overrides these standards.

Responses

The Requirements, Measurements and Levels of Non-compliance have been aligned.

The NERC template for standards formatting does not present the changes between drafts of a given version of a standard in the standard, but in a separate standard developments highlights document as noted. Changes between versions, for instance if CIP-002-1 were approved and later revised to become CIP-002-2, those changes would be captured in a separate table within the standard document.

Nuclear facilities are the purview of the NRC or Canadian Nuclear Safety Commission as appropriate.

Drafting Team Responses to General Comments

Commentor Karl Tammar

Entity ISO/RTO Council

Comments	*Responses*
The standard still looks inconsistent in a number of areas: a) Some of the measures and requirements language seems to be similar both in the same section of the standards and across the standards. b) The numbering is still inconsistent. c) It is clear that a professional technical writer has not looked at these standards to make it clear and homogenous. These inconsistencies have caused much time to be wasted by review teams which is regrettable considering it could have been easily solved.	The drafting team has addressed inconsistencies between and within standards, and aligned Requirements and Measures. Draft 3 was reviewed by technical editors.
The time periods prescribed throughout are still inconsistent across the CIP 002 to 009 standards.	Time periods have been standardized.
If an entity is found not to have properly identified its critical infrastructure in 002, will this mean being scored as non-compliant in the other remaining standards?	No.
The standard does not clearly require a security and governance program if it is determined that there are no critical assets. The standards must require that a program exists regardless of whether critical assets exist. The standard should state that the entity must perform an annual review to reconfirm its position on cyber assets. As such, the order of 002 and 003 should be reversed.	The drafting team has received comments from many entities that do not believe they must institute a formal security program if they do not own Critical Cyber Assets. Per the requirements of CIP- 002, all Applicable Entities must affirm their list of critical assets annually.
Most references to unattended facilities do not seem to bear relevance on security measures to critical cyber assets and should be reviewed.	References to unattended facilities have been removed.
NERC needs to ensure that the level of non-compliance is commensurate to the violation's impact to reliability rather than merely being an administrative violation.	Levels of Non-compliance have been reviewed and better aligned with Requirements and Measures.

Drafting Team Responses to General Comments

Commentor Kathleen M. Goodman

Entity ISO New England Inc.

Comments	*Responses*
This form has no place for General Comments. In the future, all such forms should have a place for General Comments.	Noted.
Some of the following standards require approval or signature by "senior management" or "executive management." Some Responsible Entities delegate that task. Those requirements should be amended so that a designee may approve or sign. The first example is CIP-002 Requirement R4. The corresponding Measures should be modified to stay in synchronization with their Requirements.	References to designated delegate have been added.
The second version of these standards were posted without notification. This impeded our review significantly. In the future only one version should be posted. We commented on the January 24 document.	Noted.
Need to define document vs. record and use them consistently. Typically, a document provides the process or procedural requirements of fulfilling an activity. A record provides proof of what the organization actually did and cannot be altered. Another term that is used interchangeably with the two is "data," which is not a document and not always a "business record".	Terminology has been made consistent throughout the standards.
Inadequately stated timeframe requirements for retention and documentation updates. Several instances of inconsistent timeframe requirements. Under Compliance, <<other audit records>> should read <<other auditable records>>. It seems the window for such audits is very tight (90 days).	Timeframes have been realigned.
The terms <<compliance monitor>> and <<performance-reset period>> are unclear.	Compliance monitor and performance-reset period are terms related to the NERC Compliance Enforcement program and are defined there.
The standards CIP002-CIP009 still looks inconsistent in a number of areas: a) Some of the measures and requirements language seems to be similar both in the same section of the standards and across the standards; b) The numbering is still inconsistent; c) It is clear that a professional technical writer has not looked at these standards to make it clear and homogenous. These inconsistencies have caused much time to be wasted by review teams which is regrettable considering it could have been easily solved.	Requirements, Measurements, and Levels of Non-compliance have been aligned.
The time periods prescribed throughout are still inconsistent across the CIP 002 to 009 standards. If an entity is found not to have properly identified its critical infrastructure in 002, will this mean being scored as non-compliant in the other remaining standards?	Timeframes have been addressed.

Drafting Team Responses to General Comments

Commentor Keith Fowler

Entity LG&E Energy Corp.

Comments

We are in agreement with the comments submitted by the ECAR CIPP group.

Responses

Please see responses to comments submitted by the ECAR CIPP group.

Commentor Ken Fell

Entity New York Independent System Operator

Comments

There is no formal means to communicate general comments, and the review process should be revised to accommodate such comments.

The timeframe for review and comments was particularly brief. In the future, a 45 day minimum review period should be implemented.

A second document (with the same version number) was published on NERC's website for consideration without notice, which had significant changes in format and numbering, which made an organized effort to review and comment that much more difficult.

The amount of both redundancy as well as contradictions across CIP's show a need for some consolidation and review of all CIP's prior to submission to the public. A technical writer may be needed to assure consistency.

Performance Reset Period, referred to often in various CIP's, needs to be defined.

Levels of non-compliance should be better defined, to eliminate the need for "dangling or's." Clearly state that any finding of non-compliance constitutes's a non-compliance rating consistent with the ranking system. Assure consistency and separation of non-compliance definitions to eliminate overlap.

Standardize on timelines across CIP's.

Modify requirement for approval or signature from "senior management" to allow for senior management designee.

Responses

Noted.

Noted.

Noted.

The drafting team has addressed inconsistencies between and within standards, and aligned Requirements and Measures. Draft 3 was reviewed by technical editors.

Performance Reset Period comes from the NERC Compliance Enforcement program and is defined there.

Levels of Non-compliance have been reviewed and better aligned with Requirements and Measures.

Time frames have been standardized.

References to designated delegate have been added.

Drafting Team Responses to General Comments

Commentor L.W. Brown

Entity Edison Electric Institute

Comments

One overarching point of great importance: If not within this standard, NERC standards in general (or at least the official, published criteria for auditing and enforcement) must have an appropriate "exceptions" policy. There will always be situations when "strict compliance" is in fact not the optimal approach for a utility or other responsible entity to follow.

The NERC cyber security standards should apply to all entities affecting the bulk market, as well as all entities participating in the bulk market. In particular, this includes NERC itself, as NERC is increasing its cyber links both to that market and to market participants, and will have access to, as well as possession of, information sensitive to that market.

Compliance measurement factors must be much more directly, specifically, and obviously linked to each specific Requirement of the standards, in order to facilitate both compliance and auditing. At the very least, this means that each measurement factor should have the same number as its related Requirement, as well as wording similar enough to prevent confusion. It would help to have each factor listed on the same page as, and in conjunction with, its respective Requirement.

It must be more clearly specified that these standards do not apply to facilities subject to regulation by the Nuclear Regulatory Commission (NRC), including any non-nuclear facilities that may happen to be within physical perimeters subject to such regulation. Facilities subject to NRC regulation will soon have their own NRC cyber security standards to comply with. Since the NRC standards are still in development, while NERC's cannot be postponed, the industry must be assured that facilities subject to the NRC standards will not have to comply with potentially inconsistent NERC standards.

The references to telecommunications equipment remain unclear in that they still give the impression that these standards apply to all of an entity's interconnected telecommunication system. It was the understanding of many that the standards were actually intended only to apply to specific pieces of telecommunication equipment that was located within a secure perimeter or otherwise "directly" connected to critical cyber assets.

The document previously referred to as an "FAQ" (frequently asked questions) should be adopted along with the standard, in order to facilitate proper understanding and compliance, and to ensure that such material always remains consistent with the standards. If the FAQ is not adopted, then some of the material previously appearing therein – such as examples of risk assessment or business continuity methodologies, as well as illustrative diagrams – ought to be placed into the standards in order to make the standards more intelligible to those who have not been intimately involved in the extensive explanatory discussions taking place during the drafting process.

CIP-007-1 Includes much material that also appears elsewhere. Such duplication should be eliminated. The approach taken in these comments is to suggest that material in other sections be removed if it is duplicative of CIP-007.

As a result of adopting new cyber security standards, NERC must also update and revise its Indications, Analysis and Warning program to bring it into conformity with those standards.

Responses

Responsible Entities may not write exceptions to NERC standards. CIP-003 R3 addresses exceptions to an Responsible Entity's Cyber security policy. Duly authorized exceptions, where permitted, will not result in non-compliance.

The offices of NERC and the Regional Reliability Organizations have been added to the Applicability section of these standards.

The drafting team has addressed inconsistencies between and within standards, and aligned Requirements and Measures. Draft 3 was reviewed by technical editors.

The Applicability section (Section 3) of each of these standards clearly states, "3.2 the following entities are exempt from this standards: 3.2.1 Facilities regulated by the U.S. Nuclear Regulatory Commission or the Canadian Nuclear Safety Commission."

References to telecommunications have been modified to clarify only telecommunications equipment on the electronic security perimeter are addressed by these standards.

The FAQ will continue to be available as a reference document associated with these standards.

The drafting team has addressed duplication among and within these standards. Draft 3 was reviewed by technical editors.

The IAW program is under review.

Sanctions are a function of the NERC Compliance Enforcement program. As such, the establishing of sanctions have been removed from the content of a NERC Standard.

For consistent application of these standards and associated compliance monitoring, terms used in the standards must be defined, either as already existing definitions in the NERC Glossary of Terms or as part of the standard development process. Allowing each Responsible Entity to interpret terms on their own could lead to inconsistent application of the standards.

Terminology has been standardized.

Drafting Team Responses to General Comments

There should at least be an explanation of why sanctions were removed from the standards. Some commenters would have preferred to have retained them as part of the standards.

perhaps each entire definition section as a whole, were to be clarified by adding language to the effect that interpretations of terms (especially those, like the three here, unable to be further clarified) will be acceptable for compliance purposes, even if they may differ from those of other Responsible Entities or of auditors, as long as they are reasonable or justifiable under normal standards of business decision-making.

Despite being stated here regarding each Definition section ...[include] general language endorsing interpretation made as a result of reasonable business decisions bears repeating at several locations throughout the Standards in regard to terms that are not given a specific definition.

What are the differences, if any, between a "member of senior management" and a "senior management officer" (see CIP-002-1 Measure M5, and CIP-003-1 Requirement R3) or a "senior management official" (see CIP-003-1 Compliance 1.3.2)? One term should be used consistently throughout all of the cyber security standards.

Commentor Larry Conrad

Entity ECAR Critical Infrastructure Protection Panel

Comments

Standardize the periodicity for review so that most requirements have either an annual or a quarterly review period. At present there are varying times for review, which make it difficult to maintain all of the documentation

Measures should point back to the appropriate requirement. At present it is sometimes difficult to understand which measure points back to which requirement.

Change the data retention from 3 years to 2 years throughout the document

Responses

Time frames have been standardized.

Requirements and Measures have been realigned.

Data retention has been standardized in most cases to one full calendar year.

Commentor Larry Conrad

Entity CINERGY

Comments

Cinergy supports all of the comments developed by the ECAR CIPP Group, which are being submitted to the Drafting Team under separate cover. Cinergy has these comments in addition to those submitted by the ECAR CIPP Group.

Timing for the reviews of the documentation need to be standardized both in the presentation in the document and also in the time frames prescribed for the reviews. Sometimes the timing requirements appear in the requirements section, sometimes in the measures section, and sometimes they are only referenced in the non-compliance section.

Responses

Please see responses to comments from ECAR CIPP Group.

Timeframes have been standardized.

Requirements and Measurements have been realigned.

Drafting Team Responses to General Comments

(See example in section CIP-004-1 & CIP-005-1 below.) Due to these inconsistencies, there are instances where the timing requirements contradict one another within the individual CIP standard. A table needs to be developed showing all of various timing/review requirements so that periodicity for reviews and updates are clear. For many of the requirements, annual reviews should be sufficient.	Please see Draft 2 of the Implementation Plan. Auditable compliance differs by Applicable type as well as by Standard and Requirement.
Measures should point back to the appropriate requirement. At present it is sometimes difficult to understand which measures point back to which requirements.	
Implementation Plan for Other Facilities (not Control Centers): Some weeks ago, participants had been asked to provide an estimate of how long it would take them to implement the proposed permanent standards. Cinergy estimated that approximately four (4) years would be required. The implementation plan states that all entities must be audibly compliant with all sections by 1st quarter of 2007. We once again state that it will take one year for the planning and three (3) additional years to implement all requirements of the permanent standards. We ask that the implementation plan be adjusted to reflect the input of the participants. If the implementation plan is not adjusted for all CIP sections, then at least the sections dealing with Physical Security, Security Management Controls, Systems Security Management, and Electronic Security need to be moved back to reflect the input from the utilities that will have to implement compliance.	
Implementation Plan for Control Areas: In most cases the Control Areas are expected to be "auditably compliant" with almost all requirements by 1st quarter of 2006. The logic, provided by an ECAR representative, for this is that these requirements are ‘direct descendents" from Standard 1200. However, the scope of CIPP 002 through CIPP 009 has been extended so much that there are very few ‘direct descendents’ from Standard 1200. While we realize that Control Areas were covered by Standard 1200, Control Areas should have until 1st quarter of 2007 to comply with the requirements which have changed substantially from Standard 1200 to the current proposed permanent standards. Additional detail is provided at the end of these comments indicating specific examples.	
Define "Integrity Software."	Integrity software was changed to Anti-Virus Software.

Drafting Team Responses to General Comments

Commentor Laurent Webber

Entity Western Area Power Administration

Comments

It seems that the requirements defined in the NERC Permanent Cyber Security Standard have been drafted individually with no attempt to synchronize the requirements, measures, and compliance between individual CIPs and even within single CIPs. The overall effect of the "Critical Asset" definitions and the cascading requirements in following CIPs must be carefully considered in terms of the onerous burden in cost, personnel, resource allocation, and how these will affect overall reliability. As utilities are required to allocate resources to these onerous Permanent Cyber Security Standards, attention to other critical reliability functions will likely be reduced.

Responses

The drafting team has addressed inconsistencies between and within standards, and aligned Requirements and Measures. Draft 3 was reviewed by technical editors.

Commentor Lawrence R Larson, PE

Entity Midwest Reliability Organization

Comments

Please clarify what is meant by Authorized Access; the term is used several times in the document.

Responses

Authorized Access is access that has been granted to a person in order to perform their job. This is a commonly used term in the Information Technology arena.

Drafting Team Responses to General Comments

Commentor Linda Campbell

Entity FRCC

Comments

Nowhere in any of the standards does NERC detail the policies and procedures involved with removing confidential information or configuration information when equipment or other type of media are decommissioned.

"Exemptions" is still a term used in CIP-002-1 Measures (C.M3, C.M4 (used twice) and Compliance (D.1.3.3). This term is used no where else and is not defined.

Exceptions and deviations are used throughout the standards, and while described as different in the answer to our previous comments (deviations are where you meet part but not all of standard; exception is where you meet no parts of the standard), neither the standard nor the FAQ differentiates the terms. Question 4 in the FAQ describes documenting both in the same manner.

Inconsistency remains between levels of non-compliance across standards.... For example, level one non-compliance for maintenance of log data is different between CIP-005 and CIP-006.

The standards drafting team should consider better aligning the measures sections with the requirements sections. In some cases the alignment is strong, where in others it is difficult to determine which requirement a specific measure is intended for. For example, CIP-003 has 8 requirements but 18 measures. Additionally, the non-compliance levels should be more closely aligned with the measures, which needs work in all standards.

If an organization makes a conscious decision, due to technical feasibility or practicality, not to implement a requirement as defined by this standard, can the organization document an exception or deviation (as defined above) to the standard without having to report non-compliance?

Responses

Disposal and redeployment are now addressed CIP-007.

References to exemptions have been removed.

References to deviations have been removed and the FAQ updated.

The drafting team has updated Levels of Non-compliance in each standard.

Requirements, Measures, and Levels of Non-compliance have been realigned.

Responsible Entities may not write exceptions to NERC standards. CIP-003 R3 addresses exceptions to a Responsible Entity's Cyber security policy. Duly authorized exceptions, where permitted, will not result in non-compliance.

Drafting Team Responses to General Comments

Commentor Lyman Shaffer

Entity Pacific Gas and Electric Company

Comments	*Responses*
1. Should clearly correlate "Requirements" to "Measures" and "Measures" to "Compliance". This way there is a clear relationship all the way from requirements to compliance. Currently it is hard to correlate this and it appears that in several cases they don't correspond with each other.	1. This comment has been addressed.
2. The term "shall" is used in both the "Requirements" and "Measures" sections. The term "shall" should only be used in the "Requirements" section and the "Measures" section shouldn't use "shall" but rather performance language.	2. This comment has been addressed.
3. This standard should be broken up into two distinct standards. One with specific requirements for centralized Control Systems and one with specific requirements for plants and sub-stations. This standard seems to be more focused on Control Systems where the requirements seem to fit very well, however, due to the technology, etc. at plants and sub-stations, these requirements don't fit as well. Also, there is a different risk model for Control Systems versus plants and sub-stations. Due to the risk difference there are should be distinct requirements for each.	3. The standards will remain as one set addressing both control systems and plants/substations. The implementation plan has been revised to better recognize the time required to comply for plants/substations. The risk model used by a Responsible Entity for identifying Critical Assets and Critical Cyber Assets is to be chosen by the Responsible Entity and can be different for different types of facilities.
4. Technical feasibility -- along the lines of the comments above in 3, if this standard isn't separated between Control Centers, plants, and sub-stations it should take into consideration the technical feasibility of the requirements and annotate it so that the "exception to standard" overhead doesn't get out of hand. We don't want to make this counter productive by creating a massive about of paperwork administration not allowing us to focus on the spirit of the standard.	4. References to technical feasibility have been added.

Drafting Team Responses to General Comments

Commentor Marc Butts

Entity Southern Company, Transmission, Operations, Planning and EMS Divisions

Comments

The standards seem to be written to reflect a perspective that all Critical Cyber Assets are under the direct control of the Responsible Entity. In some cases, the actual asset involved may be provided by a vendor that fully operates and maintains the asset under an application services agreement or merely provides bug-fix and enhancements services. Although the Responsible Entity using the asset would be responsible for the standard requirements, there are practical limitations to this in a customer vendor relationship (e.g., vendors with multiple customers have variations on procedures and minimum expectations to accommodate these standards). At a minimum, the standard does not clearly, explicitly recognize these situations and how they should be addressed.

These standards rely based on the Definitions on the direct relationship of a Cyber Asset to an identified Critical Asset when identifying a Critical Cyber Asset. It is recognized that most cyber systems that are associated with a critical asset will also be associated with non-critical assets (and thus become classified as Critical Cyber Assets. The definition of Critical Cyber Asset should not, however, ignore the fact that a cyber asset associated with only non-critical assets may effectively become a critical asset if its security compromise results in sufficient non-critical asset problems that, taken in total or cumulatively, result in Critical Asset problems or general grid reliability risk. As an analogy, if a toll-road freeway in a city was deemed a critical asset and the "Easy Pass" system was deemed the critical cyber system associated with it, the freeway would still be impacted by the compromise of the surface-road street light system as many more vehicles entered (and perhaps overloaded) the freeway to avoid malfunctioning street lights and the resulting congestion (and possible resulting accidents).

Although NERC is the sponsor and provider of the IDC, SDX and RCIS which many in the industry consider Critical Cyber Assets due to their direct and indirect influence on grid controls and decisions, it is not listed in the Applicability section of the Standards. Why is NERC not listed as having the standards apply to them? Even if NERC intends to comply, should they not be explicitly listed due to their role in the Cyber Assets just mentioned? If NERC is not held responsible for these applications' security then who should be? The same would be true for a Regional Reliability Council that operates similar systems for their Interconnection.

Responses

It is up to the Responsible Entity to ensure that the requirements of the standards are met. This may require contract language with a third-party vendor, to ensure the services they provide as Critical Cyber Assets comply with the standards.

The scenario described effectively results in an N-2 or greater contingency, which these standards do not attempt to address. Any Responsible Entity can add additional cyber assets to the list of Critical Cyber Assets as it deems necessary to protect the grid.

The offices of NERC and the Regional Reliability Organizations have been added to the Applicability section of these standards.

Drafting Team Responses to General Comments

Commentor Patrick Miller

Entity PacifiCorp

Comments	*Responses*
Throughout the standards, the requirements do not map directly to the measures (1:1 ratio). It would be much easier to adhere to -- and enforce -- the measures if they directly represented the requirements. Without the 1:1 relationship, there will be requirements that will go unaddressed to a certain degree.	The requirements and measures have been aligned.
There is no clear language around the framework or minimum requirements for a "risk based assessment." Without some form of directional statements, models or representations, there will be much confusion and [often only] minimal effort put forth which may not meet the spirit of the standard.	Risk assessment methodologies are the subject of a NERC Critical Infrastructure protection Committee white paper being developed. The Responsible entity must choose the appropriate risk assessment methodology or methodologies suited to their individual environment.
There is a significant amount of redundant information at the beginning of each standard. This can introduce an element of complacency for the reader by presenting the same (or only slightly different) information multiple times. It would create efficiency and clarity if there were a single section for definitions, purpose, applicability, etc...	Each of these standards is a separate standard and must conform to the NERC format for standards.
The current naming convention is very hard to reference, in both type and speech. Since the name has changed from "1300" to "CIP-002-01 through CIP-009-01", it is easier (which will ultimately mean a defacto usage) to revert to "1300" or "CIP." Please consider using a single standard name again, and breaking out the individual standards -- something similar to what was used for the 1300 nomenclature but still meets NERC intentions.	The naming convention is consistent with the convention chosen for all NERC standards, as established during the development of the Version 0 standards.
The information provided in these reports could, by inference, indicate areas where organizations are weak, or may have insufficient controls/security in place. As such, the information should be protected accordingly. NERC should provide an encryption mechanism so that when this information is submitted it will be appropriately protected.	Any policies or other materials that are part of or protected by a Responsible Entity's Cyber Security policies is not intended for public release. Identification of areas of non-compliance, and subsequent posting are mandated by the NERC Board of Trustees.

Drafting Team Responses to General Comments

Commentor Paul McClay

Entity Tampa Electric

Comments

The preface to the Definitions section should reference the NERC Glossary of Terms. There does not appear to be a Reliability Standards Glossary of Terms.

"Exceptions" and "deviations" are used throughout the standards, and while described as different in the answer to Tampa Electric's previous comments (deviations are where you meet part but not all of standard; exception is where you meet no parts of the standard), neither the standard nor the FAQ differentiates the terms. Question 4 in the FAQ describes documenting both in the same manner.

Inconsistency remains between levels of non-compliance across standards.... For example, level one non-compliance for maintenance of log data is different between CIP-005 and CIP-006.

The standards drafting team should consider better aligning the measures sections with the requirements sections. In some cases the alignment is strong, where in others it is difficult to determine which requirement a specific measure is intended for. For example, CIP-003 has 8 requirements but 18 measures. Additionally, the non-compliance levels should be more closely aligned with the measures, which needs work in all standards.

If an organization makes a conscious decision, due to technical feasibility or practicality, not to implement a requirement as defined by this standard, can the organization document an exception or deviation (as defined above) to the standard without having to report non-compliance? If you have a documented deviation to a standard, can you report being in compliance?

Responses

The NERC Glossary of Terms can be found on the NERC web site.

References to deviations have been removed.

Requirements, Measures, and Levels of Non-compliance have been aligned.

Responsible Entities may not write exceptions to NERC standards. CIP-003 R3 addresses exceptions to an Responsible Entity's cyber security policy. Duly authorized exceptions, where permitted, will not result in non-compliance.

Drafting Team Responses to General Comments

Commentor Pete Henderson

Entity Independent Electricity System Operator

Comments

General Comments:
1)The group of standards still looks inconsistent in a number of areas:
a)-There are a number of instances where a requirement is established in one standard which covers the same ground as requirements in another standard, and where contradictory requirements result;
b)The numbering of sections remains inconsistent;
c)-The time periods prescribed for activities such as document review and document revision are still inconsistent across the CIP 002 to 009 group of standards.
d)-It is clear that a professional technical writer has not looked at these standards to make it clear and homogenous.

These inconsistencies have caused much time to be wasted by review teams which is regrettable considering it could have been easily solved.

2)-If an entity is found not to have properly identified its critical infrastructure in 002, will this, ipso facto, mean being assessed as non-compliant in the other remaining standards (since all other standards are built on the assumption that the entities' lists of critical cyber assets are definitive?

3)The set of standards does not clearly require a security and governance program if it is determined that there are no critical assets. The standards must require that a program exist regardless of whether critical assets exist. The standard should state that the entity must perform an annual review to reconfirm its position on cyber assets. As such, the order of 002 and 003 should be reversed.

4)-Most references to unattended facilities do not seem to bear relevance on security measures to critical cyber assets. The requirement for making a distinction between attended and unattended assets should be reviewed.

Furthermore, if this distinction is deemed necessary, definitions should be provided for the term unattended. It is not clear whether a facility that is continuously monitored, or a facility that is manned frequently, but not continuously, is unattended.

5)-Throughout these standards there are numerous instances where requirements are effectively first established in the Measures and/or Levels of Non-Compliance sections of the text. This is inappropriate. If a condition needs to be met to be fully compliant, that condition should be identified in the Requirements section. In particular, it should not be necessary to read descriptions of non-compliance to infer the requirements for full compliance.

6)-In several of the draft standards, there are instances where levels of non-compliance are described in such a way that entities could simultaneously satisfy the conditions of more than one level of non-compliance. Levels of non-compliance should be described as a set of mutually exclusive conditions in order to avoid confusion and inappropriate certification.

7)-Requirements related to authorizing, controlling, monitoring, and auditing electronic and physical access to critical cyber assets are specified in several different standards. This is confusing at best, and has resulted in both duplication and contradiction. All requirements pertaining to access control should be specified in one standard for

Responses

1. The drafting team has addressed inconsistencies between and within standards, and aligned Requirements and Measures. Draft 3 was reviewed by technical editors.

2. If a Responsible Entity does not properly document its findings that it has no Critical Cyber Assets, and further does not comply with the other standards in the suite (CIP-003 through CIP-009), it will be found out of compliance with those standards.

3. The drafting team has received comments from many entities that do not believe they must institute a formal security program if they do not own Critical Cyber Assets. Per the requirements of CIP- 002, all Applicable Entities must affirm their list of critical assets annually.

4. References to unattended facilities have been removed.

5. The drafting team has addressed inconsistencies between and within standards, and aligned Requirements and Measures. Draft 3 was reviewed by technical editors.

6. Levels of Non-compliance have been reviewed and better aligned with Requirements and Measures.

7. Requirements are identified in the standard pertaining to each facet of cyber security. This can result in the appearance of duplication, but is not actually the case.

8. Time frames have been standardized.

9. The standards do contain some prescriptive requirements based on the drafting teams experience in the industry. Prescriptive requirements have been kept to a minimum and the use of risk-based assessments is provided for, in fact required, wherever possible.

10. Data retention has been standardized in most cases to one full calendar year.

better consistency and clarity.

8)-As a general rule, the frequency at which entities are required to review and update documentation should not be arbitrarily prescribed in these standards. Rather, the review frequency should be determined and documented by those entities based on risk management considerations. An appropriate Measure for such a requirement would be the presence or absence of a documented review frequency, with compliance being demonstrated by document review/update being performed at that defined frequency.

9)-In a number of places, these standards are very prescriptive and appear to be inconsistent with, or at least appear not to contemplate, the application of a risk based approach to meeting an overall goal. Because of the high degree of specificity, some requirements may not be applicable to all Responsible Entities, and the intent of other requirements may be fully satisfied without meeting the requirement as worded. In situations where the intent of the requirement (or the purpose of the standard) can be satisfied without meeting the specific wording of one or more requirements, entities should be permitted to claim full compliance provided they document their rationale for doing so.

10)-In a number of Standards, the text of the Data Retention portion of the Standard (under Compliance) contradicts the text in the subsequent Additional Compliance Information Section of the same Standard.

Commentor Philip D. Riley

Entity Public Service Commission of South Carolina

Comments

The PSCSC reiterates its view that the approach in all the standards being reviewed appears to be compliance-based rather than performance-based. Is the objective having a plan and procedures on hand, or a reliable system? The PSCSC maintains that the real objective is reliability, and not readily available plans and procedures. The real measure of success is effective implementation of the plans and procedures such that reliability is not compromised.

Responses

The drafting team believes both performance and compliance are important and have drafted Measures and Levels of Non-compliance reflecting that position.

Drafting Team Responses to General Comments

Commentor Randy Schimka

Entity San Diego Gas and Electric Co

Comments	*Responses*
We ... suggest including a revised definition for the term 'authorized access' that includes both physical and electric access.	Noted.
Many of the questions we've heard discussed about this standard revolve around the issue of identifying Critical Cyber Assets. Some clean examples of what qualify as Critical Cyber Assets, perhaps in the FAQ document, would go a long way towards clarifying some of the questions with respect to this definition.	The FAQ has been updated.
- Requirements should be clearly correlated with Measures and Compliance in the various sections. Some of the sections seem to have been drafted with this in mind, while others have not. For consistency's sake, we believe there should be a one-for-one correspondence between Requirements and Measures.	The drafting team has addressed inconsistencies between and within standards, and aligned Requirements and Measures.
- Since the sections of the standard have been drafted by separate teams, there are some inconsistencies between the sections. We recommend that NERC have a professional technical writer review and edit future drafts of these documents to bring a high level of consistency to the process and to help clarify terminology before balloting.	Draft 3 was reviewed by technical editors.
There are several occasions in the documents where a reader can interpret the standard one way if thinking in terms of control centers and then another way if thinking in terms of substations, power plants, etc. Is there any way to expand on the language and organization in the documents to make the differentiation clearer between the different types of facilities? We'd all like to see a final product that is concise and brief, but sometimes we struggle with the application or definition of some of these materials.	
We'd also be interested in learning the drafting team's perspective about the inclusion or exclusion of Distribution Control or other utility SCADA systems as they relate to this standard. Has Distribution or other control systems been left out of the requirements due to prioritization, costs for implementation, or will there perhaps be a phased-in approach where they will be added in later? Is the thought to eventually include Distribution control systems in the NERC standards? It seems impractical to spend this much time, money, and effort on Bulk Power-related assets such as EMS control systems and perhaps substation and power plant assets when a similar amount of damage or havoc can be accomplished from a power system perspective if Distribution SCADA systems were compromised.	NERC Standards are directed to the reliable operation of the Bulk Electric System. As such, Distribution systems are outside the purview of a NERC standard.

Drafting Team Responses to General Comments

Commentor Raymond A'Brial

Entity Central Hudson Gas & Electric Corporation (CHGE)

Comments	***Responses***
We have some General Comments. This form has no place for General Comments. In the future, all such forms should have a place for General Comments.	Noted.
- Some of the following standards require approval or signature by "senior management" or "executive management." Some Responsible Entities delegate that task. Those requirements should be amended so that a designee may approve or sign. The first example is CIP-002 Requirement R4. The corresponding Measures should be modified to stay in synchronization with their Requirements.	References to designated delegate have been added.
- The second version of these standards were posted without notification. This impeded our review significantly. In the future only one version should be posted. We commented on the January 24 document.	Noted.

Commentor Richard Engelbrecht

Entity Rochester Gas and Electric

Comments	***Responses***
We have some General Comments. This form has no place for General Comments. In the future, all such forms should have a place for General Comments.	Noted.
- Some of the following standards require approval or signature by "senior management" or "executive management." Some Responsible Entities delegate that task. Those requirements should be amended so that a designee may approve or sign. The first example is CIP-002 Requirement R4. The corresponding Measures should be modified to stay in synchronization with their Requirements.	References to designated delegate have been added.
- The second version of these standards were posted without notification. This impeded our review significantly. In the future only one version should be posted. We commented on the January 24 document.	Noted.

Drafting Team Responses to General Comments

Commentor Richard Kafka

Entity Pepco Holdings, Inc. - Affiliates

Comments	*Responses*
Improvements have been made in definitions. Access to the glossary being developed would assist in our review and understanding. Additional definitions are required for terminology utilized in the standards which are not presently defined under the definitions (e.g. Under Control of a Common System, Routable Protocol, differentiation between Special Protection Scheme and a standard Protection System,).	The Glossary is available from NERC's web site.
What are the differences, if any, between a "member of senior management" and a "senior management officer" (CIP-002-1 M5 and CIP-003-1 R3) or a "senior management official" (CIP-003-1 Compliance 1.3.2)? If no difference is meant, then one term should be used consistently throughout the permanent cyber security standards. If there are differences, then each term should be further defined.	Terminology has been standardized.
Why was the comment period for this version of the standards shortened from 45 to 30 days? The shorten period, the small differences in posted final versions, and the significant format changes from the previous draft, have made meeting the deadline to provide comments challenging at best. As a result our comments may not be complete. As a result comments that may have been raised during this draft may not be raised until the next draft.	The comment period for draft 2 was shortened to accelerate the development process of these standards. Draft 3 is posted for the customary 45 days.
Compliance measurement factors must be much more directly, specifically, and obviously linked to each specific Requirement of the standards, in order to facilitate both compliance and auditing. At the very least, this means that each measurement factor should have the same number as its related Requirement, as well as wording similar enough to prevent confusion. It would help to have each factor listed on the same page as, and in conjunction with, its respective Requirement.	Requirements and measures have been aligned.
The document previously referred to as an "FAQ" (frequently asked questions) should be adopted along with the standard, in order to facilitate proper understanding and compliance, and to ensure that such material always remains consistent with the standards. If the FAQ is not adopted, then some of the material previously appearing therein -- especially the illustrative diagrams -- must be placed into the standards in order to make the standards more intelligible to those who have not been intimately involved in the extensive explanatory discussions taking place during the drafting process.	The FAQ will continue to be available as a reference document associated with these standards.
As a result of adopting new cyber security standards, NERC must also update and revise its Indications, Analysis and Warning program to bring it into conformity with those standards.	The IAW program is under review.
Why were sanctions removed from the standards? Is there no sanction now for various levels of compliance?	Sanctions are a function of the NERC Compliance Enforcement program.
As part of the NERC conference call, it was communicated that Urgent Action 1200 expires in mid August and that under the by-laws that it can not be extended further. It was hoped that passage of the permanent standards (or a least some) could be achieved so that there would only be a 2 week gap (i.e. become effective the beginning of September). Each draft permanent standard lists a Proposed Effective Date of October 1, 2005 which would mean there would be a 6 week gap not a 2 week gap. Should the Proposed Effective Date be September 1 in each Standard? As a contingency can a second urgent action identical to 1200 be implemented to cover any gap in cyber security standards (i.e. effective from the expiration of 1200 until the passage of the permanent standards)? Note that if a portion of the permanent standards are passed you may not have an effective cyber security policy (e.g.	The potential gap between the expiration of UA Standard 1200 and the adoption of CIP-002 through CIP-009 is being addressed. Please see the proposed changes to the NERC Standards Development process.

Drafting Team Responses to General Comments

CIP-002-1 does not immediately pass but others do - How would you know what Critical Cyber Security Assets to apply the other standards that may have passed?).

Commentor Robert C. Webb

Entity

Comments

I do not believe the majority of NERC's Cyber Security Standards CIP–002–1 through CIP–009–1 are ready to ballot at this time, because they do not adequately address the special considerations necessary when applying the standards to a key segment of our country's critical power infrastructure - generation control systems.

I have examined the draft standards as part of my role in developing technical reports, recommended practices, and standards for manufacturing and control systems security, as a part of the Instrumentation, Systems, and Automation Society's SP99, "Manufacturing and Control System Security" standards committee.

I am the Managing Director of that committee, and a professional engineer with considerable experience in power plant automation. ISA is interested in consistency with other standards, where appropriate, to preclude end user confusion and an impossible challenge for manufactures of control systems equipment. To that end, we are working with Tom Flowers of your CSSWG to establish a liaison process that would allow such considerations to be addressed earlier in the process. However, you have asked for comments at this time, and we believe these issues need to be addressed now, before approval, for the standard to be effective.

In general, CIP-002-1 through CIP-009-1 do a good job of addressing the key elements of a good security program; the drafting team should be congratulated. However, without specific guidance on how to apply some of the recommendations to legacy generation control systems, the standards could be counter productive. This guidance need not be exhaustive, but can be provided at a high level, with references to additional detailed information. In other words, wholesale application of typical business systems security practices to control systems is not appropriate. SP99 was created to provide guidance on how to apply security to control systems, without adversely affecting their primary function. Substantial guidance has been published by the SP99 committee, and has been available since April of 2004. It should be referenced in the NERC standard.

In addition to the direct impact on generation, generation control systems, if not adequately addressed, become additional "back door" electronic avenues that can compromise the bulk grid that the NERC standards appear to be focused on protecting. The standards should cover such systems, regardless of generator size.

Joe Weiss, a member of ISA's SP99 , and NERC 's CSSWG, has provided specific comments and recommended revisions which address these concerns. Those comments should be responsibly addressed.

Responses

Please see responses to Bryan Singer, Rockwell Automation.

Drafting Team Responses to General Comments

Commentor Robert Strauss

Entity New York State Electric & Gas Corporation

Comments	Responses
We have some General Comments. This form has no place for General Comments. In the future, all such forms should have a place for General Comments.	Noted.
- Some of the following standards require approval or signature by "senior management" or "executive management." Some Responsible Entities delegate that task. Those requirements should be amended so that a designee may approve or sign. The first example is CIP-002 Requirement R4. The corresponding Measures should be modified to stay in synchronization with their Requirements.	References to designated delegate have been added.
- The second version of these standards were posted without notification. This impeded our review significantly. In the future only one version should be posted. We commented on the January 24 document.	Noted.

Commentor Roman Carter

Entity Southern Company Generation

Comments	Responses
The standards seem to be written to reflect a perspective that all Critical Cyber Assets are under the direct control of the Responsible Entity. In some cases, the actual asset involved may be provided by a vendor that fully operates and maintains the asset under an application services agreement or merely provides bug-fix and enhancements services. Although the Responsible Entity using the asset would be responsible for the standard requirements, there are practical limitations to this in a customer vendor relationship (e.g., vendors with multiple customers have variations on procedures and minimum expectations to accommodate these standards). At a minimum, the standard does not clearly, explicitly recognize these situations and how they should be addressed.	It is up to the Responsible Entity to ensure that the requirements of the standards are met. This may require contract language with a third-party vendor, to ensure the services they provide as Critical Cyber Assets comply with the standards.
These standards rely based on the Definitions on the direct relationship of a Cyber Asset to an identified Critical Asset when identifying a Critical Cyber Asset. It is recognized that most cyber systems that are associated with a critical asset will also be associated with non-critical assets (and thus become classified as Critical Cyber Assets. The definition of Critical Cyber Asset should not, however, ignore the fact that a cyber asset associated with only non-critical assets may effectively become a critical asset if its security compromise results in sufficient non-critical asset problems that, taken in total or cumulatively, result in Critical Asset problems or general grid reliability risk. As an analogy, if a toll-road freeway in a city was deemed a critical asset and the "Easy Pass" system was deemed the critical cyber system associated with it, the freeway would still be impacted by the compromise of the surface-road street light system as many more vehicles entered (and perhaps overloaded) the freeway to avoid malfunctioning street lights and the resulting congestion (and possible resulting accidents).	The scenario described effectively results in an N-2 or greater contingency, which these standards do not attempt to address. Any Responsible Entity can add additional cyber assets to the list of Critical Cyber Assets as they deem necessary to protect the grid.
Although NERC is the sponsor and provider of the IDC, SDX and RCIS which many in the industry consider Critical Cyber Assets due to their direct and indirect influence on grid controls and decisions, it is not listed in the Applicability section of the Standards. Why is NERC not listed as having the standards apply to them? Even if	The offices of NERC and the Regional Reliability Organizations have been added to the Applicability section of these standards.

Drafting Team Responses to General Comments

NERC intends to comply, should they not be explicitly listed due to their role in the Cyber Assets just mentioned? If NERC is not held responsible for these applications' security then who should be? The same would be true for a Regional Reliability Council that operates similar systems for their Interconnection.

Commentor Steven L Townsend

Entity Consumers Energy

Comments

Consumers Energy has also submitted comments via the ECAR CIPP.

Responses

Please see responses to comments submitted by the ECAR CIPP group.

Commentor Terry Doern

Entity Bonneville Power Administration, Department of Energy

Comments

GENERAL COMMENTS:
1- Address the situation where dial-up relays a Single Relay

3) Assessment of Assets is a lot of work and will take 6-12 months to complete before follow-up work can begin. This should delay the implementation schedule.

4) Documentation must be manageable not burdensome. A few control center sites versus hundreds of field sites. For example BPA has an estimated 5,000 intelligent electronic devices that could be considered critical. Just listing them all, let alone changing all the passwords if someone retires - - as only one of many change tasks, is burdensome. We would have to visit each and every site within 7 days. Impossible!

5) It is unclear if our risk assessment should address just a single contingency (N-1), a double contingency (N-2) or multiple contingencies (N-K). From the power system engineering point of view N-1 is achievable, N-2 is difficult, N-K is impossible

6) GENERAL Issue: Requirements are not consistently titled. The requirements in CIP-002 and CIP-003 don't use titles. CIP-004 titles each requirement with a hyphen prior to the actual requirement. Some requirements are titled followed by a colon. Recommendation: Title all requirements and use a hyphen or a colon consistently for CIP-002 thru 009. A Technical writer needs to edit this material - - not an engineer or cyber security professional.

7) GENERAL Issue: It's difficult to correlate requirements to the associated measures, compliance data retention, and the levels of non-compliance in the standard. Recommendation: Use the requirement title, a numbering scheme or a table that shows the correlation to the requirements. (e.g., R1.1 M1.1). CIP-003 is number poorly.

Responses

1. Requirements pertaining to dial-up devices have been revised.

3. The implementation plan has been revised.

4. The drafting team believes documentation and auditing are important aspects of cyber security.

5. The level of risk assessment is to be determined and documented by the Responsible Entity.

6. Noted.

7. Alignment of requirements to measures and to levels of non-compliance has been addressed.

8. Noted.

9. Noted.

10. Any Responsible Entity can add additional cyber assets to the list of Critical Cyber Assets as they deem necessary to protect the grid.

11. FISMA was reviewed during the initial drafting of these

8) GENERAL Issue: The procedure to exempt items in these standards should be clearly defined at the start of each standard.

9) GENERAL Issue: The words 'entity and responsible entity' are used in various ways throughout CIP standards. Clarify if possible.

10) GENERAL Issue: Non-routable protocols may be cyber security risk in some cases and should not be excluded where there is a risk to the power system. Recommend adding text where needed stating - 'if high risk to the power system safety or reliability then non-routable protocols shall be considered, using these standards.'

11) GENERAL DOUBLE-CHECK: FISMA may take precedence over NERC. ???? Did this get resolved? If so where?

12) GENERAL: It may be nearly impossible to be compliant with CIP002-009 due to the large scope, number of sites, thousands of critical cyber assets and detailed documentation requirements. A better approach towards compliance would be for the utility to identify its most critical issues using a risk based assessment and then devote staff and money to resolving the most critical items. Striving to be compliant for low value work when it could impact reliability is not prudent utility practice. Compliance with burdensome documentation or low probability risks shall not take resources away from our key missions -- to be safe and to keep the lights on.

13) The exemption process must be a tool for management to reach compliance for these standards.

14) Control centers compliance reporting should be separate from unattended facilities such as substations.

15) The implementation plan should be prioritized to fix the most critical cyber assets first.

standards.

12. The Responsible Entity is required to use risk assessment to identify the assets critical to reliable operation of the grid, then protect only those cyber assets critical to the reliable operation of the Critical Assets.

13. The exemption process has been clarified.

14. Compliance reporting will be defined by the NERC and Regional Compliance Monitoring and Enforcement Programs.

15. The implementation plan has been revised.

Commentor Todd Thompson

Entity SPP

Comments

The standard still looks inconsistent in a number of areas:
a)--Some of the measures and requirements language seems to be similar both in the same section of the standards and across the standards.
b)--The numbering is still inconsistent.
c)--It is clear that a professional technical writer has not looked at these standards to make it clear and homogenous.
These inconsistencies have caused much time to be wasted by review teams which is regrettable considering it could have been easily solved.

The time periods prescribed throughout are still inconsistent across the CIP 002 to 009 standards.

If an entity is found not to have properly identified its critical infrastructure in 002, will this mean being scored as non-compliant in the other remaining standards?

Responses

The drafting team has addressed inconsistencies between and within standards, and aligned Requirements and Measures. Draft 3 was reviewed by technical editors.

Time frames have been standardized.

If a Responsible Entity does not properly document its findings that it has no Critical Cyber Assets, and further does not comply with the other standards in the suite (CIP-003 through CIP-009), it will be found out of compliance with those standards.

The drafting team has received comments from many entities that do not believe they must institute a formal security program if they do

Drafting Team Responses to General Comments

The standard does not clearly require a security and governance program if it is determined that there are no critical assets. The standards must require that a program exists regardless of whether critical assets exist. The standard should state that the entity must perform an annual review to reconfirm its position on cyber assets. As such, the order of 002 and 003 should be reversed.	not own Critical Cyber Assets. Per the requirements of CIP- 002, all Applicable Entities must affirm their list of critical assets annually.
Most references to unattended facilities do not seem to bear relevance on security measures to critical cyber assets and should be reviewed.	References to unattended facilities have been removed.

Commentor Tom Pruitt

Entity Duke Power Company

Comments	*Responses*
--General formatting is still problematic and creates problems following references. The numbering scheme is confusing and not consistent. Why use R's, M's, then switch to numbers?	Formatting of the standards was established during the development of the Version 0 standards. These standards follow the prescribed convention.
--While this purports to provide flexibility in determining which assets are in scope, the words used in defining Critical Assets/Critical Cyber Assets are very broad and include expectations that scope is very broad.	The use of risk-based assessments, as required in the standards, allows a Responsible Entity to limit the impact of these standards to those facilities/assets critical to the reliability of the electric grid.
--What excludes a unit or station from being in the plan? --Clarification on controlling access to transmission control houses is needed.	Requirements for physical access control have been refined.