Drafting Team Responses to General Comments

Name Terry Bilke

Entity Midwest ISO

Comments

Thanks for the opportunity to comment. It’s apparent that a great deal of hard work and thought has gone into the development of the standard.

These comments are not from a cyber expert, but as someone who must administer a compliance program.

My primary concern with this standard (and it's not unique to this standard) is that there seems to be a desire to have an even distribution of the different levels of non-compliance. In general, we would expect something of a pyramid distribution of compliance violations, with few (if any) level 4 types of events. Level 3 and level 4 non-compliance should be for serious events/omissions that jeopardize reliability.

There are 25 different things in this standard that cause a level 4 non-compliance (some for a missing piece of paper or having an outdated piece of paper with the wrong name on it). There area well over 100 different opportunities for assessing compliance violations.

While it may be that all the items in the cyber standard are important, the administration of this standard should be simplified. As an analogy, if I were to take a 100 question exam, it’s possible I could miss 5 or 6 items, but my score would still be an A. I could probably miss 20 and still pass. Wouldn’t this type of approach work?

Again, level 3 and level 4 non-compliance should be for serious events/omissions that jeopardize reliability.

Thanks for your consideration.

Response:

The Drafting Team has rewritten the levels of noncompliance. The rewritten levesl have been reviewed by NERC's Compliance Enforcmeent Program personnel and found to be saisfactory. The Drafting Team has passed along your comments to NERC.

Drafting Team Responses to General Comments

Name Pat Bourassa

Entity Wisconsin Public Service Corporation

Comments 1-7 (Most Sections)
Due to the nature of a plant's Distributed Control System (DCS) component placement it will be very costly to physically secure all system devices on multiple DCS networks if they employ routable protocol.

Response: Instances where a Responsible Entity is unable to meet the requirement to place equipment in an enclosure as required, it can write an exception to its own security policies (see CIP-003). A Responsible Entity's duly authorized exception will not result in non-compliance, as noted in the Additional Compliance sections of these standards

Drafting Team Responses to General Comments

Name Laurence W. Brown

Entity Edison Electric Institute

Comments

This version, Draft 3, of the proposed NERC Cybersecurity Standards reflects a dramatic improvement over the previous two drafts. However, the improved clarity in the language now permits a more focused assessment of the potential impact of the Standards. Therefore, rather than decreasing in size and scope as compared to EEI's comments on the last set of comments, the breadth and complexity of EEI's comments on this draft have dramatically increased. These comments are the product of three teleconferences of at least two hours each, as well as the additional written and oral input of numerous EEI member-company personnel. We emphasize this point in order to indicate the serious, thoughtful manner in which these comments were developed, and the critical nature of the need to address them fully in order to ensure a positive outcome when final proposed Cybersecurity Standards are put to a vote. EEI recognizes and supports the need for such a positive outcome, as recently affirmed by its Board of Directors at the Annual Meeting this June.

1. As expressed in previous comments by EEI, there needs to be a consistent waiver or exceptions policy implemented by NERC. For example, it may not be possible or prudent to enforce all aspects of normal access control procedures during emergencies such as resulting from natural disasters or events involving law enforcement personnel. Moreover, CIP-003-R3, -3.2 and -M3, and CIP-004-C1.4, for example, specifically refer to "exceptions." Thus, it is unclear whether (a) exceptions in an of themselves will result in noncompliance, (b) exceptions can exist for other Standards even where not mentioned, (c) or exceptions can or must be "built in" to policies (for example, whether a policy can avoid a possible future noncompliance situation by mentioning in advance how and under what circumstance some or all aspects of it can be approriately or properly disregarded).

2. The industry needs to be extremely careful to avoid the creation of purely documentation-based non-compliances. With increasing legal requirements for compliance, and the associated penalties for noncompliance, noncompliance should be reserved for "real" security issues. It is simply too easy to make a mistake in documentation in light of the constantly evolving cyber environment. In the Version 0 Operating Standards, for instance, non-compliance is reserved for operating the grid in an unstable manner, not for failing to keep the phone number of a senior management official updated. Compliance will tend to be seen by the public and by regulators as purely binary, YES or NO — they will not be likey to understand, or forgive, a purely documentary failure. This could be addressed by making the levels of non-compliance much more generic or general.

Also, a comparison of measures to levels of compliance can yield scenarios that the levels of compliance don't anticipate. This is not due to any shortcoming or error by the drafting committee, but rather because anticipating every possible scenario of non-compliance is impossible. For instance, how would an auditor determine compliance with a requirement to modify records within any particular time period?

One simple way to make the standard less prescriptive but still accomplish all the security

Response:

1. Emergency situations are address in CIP-003. Responsible Entities may not take exceptions to NERC Standards, however, they may write exceptions to their own policies and procedures that implement the requirements of these standards.

2. The Drafting Team has removed prescription where possible. The prescriptiveness that remains is necessary to provide the clarity requested by a majority of commenters.

The documentation required by these standards allow Responsible Entities to demonstrate during an audit that the policies, processes, and procedures that they have implemented consistently comply with the requirements of these standards.

Measures have been reworded throughout to ensure they do not conflict with the requirements.

3. These comments were passed along to NERC's Compliance Enforcement Program personnel.

4. The Risk Assessment Whitepaper is now available on the ESISAC website at www.esisac.com/library.html.

5.The Levels of Noncompliance are part of NERC's current Standard template.

6. These standards include minimum requirements. Responsible Entities may go beyond the minimum as they deem appropriate.

7. FAQs were posted for review and comment along with each draft of these standards. The Drafting Team has reviewed and modified the FAQS as necessary to address comments it received during the third round of public review and comment on these standards. The FAQs are an aid to understanding the requirements of these standards; however, they are not part of the standards.

CIP-002
The verbal explanation of Area G appended to the diagram indicates that the relationship concerned is network

and auditing goals would be to remove all documentation requirements from the requirement sections. Move documentation to the measures section, and have general measures that would require adequate and reasonable documentation of compliance to the requirements. This would help shift the focus from paper auditing to cyber security auditing. In addition, it would also reduce the potential for inflexible interpretations of the standards by third party auditors (see, e.g., the above discussion of "all ports and services").

3. NERC and or the Regions need to create clear audit procedures to permit Responsible Entities to know exactly how, and against what, compliance will be measured. Not only will this assist compliance, but it will be invaluable for the education of non-industry outside auditors that may be brought in from time to time to conduct audits apart from or in preparation for the NERC audit process. One important issue to address in such procedures is the protection of sensitive information, both regarding auditors themselves and regarding litigation "discovery" and use. SEE comment above on CIP-007-M9.

Additionally, audit process workshops would be invaluable in helping the industry prepare both for compliance and for eventual audit.

4. The Risk Assessment Whitepaper still has not been published on either the NERC-CIPC or the ES-ISAC site. That must be done as soon as possible, even in the absence of a final set of cybersecurity standards, to permit Responsible Entities to begin to improve their security posture voluntarily, and prepare for the most rapid possible implementation of standards.

5. It is unclear why CIP-002 through CIP-009 need different levels of noncompliance, when other standards, such as CIP-001, do not have such levels.

6. Controlling ports may not be enough — individual addresses should also be covered by the Standards.

7 The FAQ must be included for comment along with the Standards. Specific FAQ Comments:

For CIP-002

Circle "G" in the diagram at No. 1 does not give a clear enough indication of the relationship of "covered" non-critical cyber assets to facilities such as generation units and substations. Perhaps an addtional diagram would clarify how to identify such assets. SEE ALSO above comments to CIP-005-R1.4 and CIP-007-R1.

No. 7 Fails to clarify that, while redundancy does not change criticality, it may indeed change reasonably appropriate measures that are needed for such a facility.

No. 12 appears to suggest cyber assets associated with a person who has only verbal dispatch control must be treated as critical. Is that the intent, given that such assets do not have direct generation control? If that was the intent, we suggest that is excessive, given that the asset itself cannot have any direct impact.

connectivity to Critical Cyber Assets.

FAQ #7 has been renumbered to #6 and indicates that the minimum level of security required by these standards is applicable to all Critical Cyber Assets.

Yes, if that person is performing a critical function.

CIP-006
That is correct.

Drafting Team Responses to General Comments

For CIP-006

No. 14 appears to imply that raised floors and dopped ceilings are inherently insecure.

Drafting Team Responses to General Comments

Name	Peter Burke		
Entity	American Transmission Company		
Comments	American Transmission Company concurs with the comments submitted separately by the Edison Electric Institute and by the Midwest Reliability Organization.	**Response:**	Please see responses to Laurence W. Brown, Edison Electric Institute.

Drafting Team Responses to General Comments

Name Marc Butts

Entity Southern Company

Comments

Comment 1 - Emergency Waiver Provisions - The standard needs to provide a way to have emergency waivers. Even nuclear regulations allow for such waivers of standards in the event of emergencies. During storm restoration or other natural disasters when we invoke our mutual aid agreements and start bringing in outside crews to restore service, we need some clause where we can grant physical access to our assets without having to track background screening, training requirements, etc. We shouldn't be in violation of a cyber security standard during these emergency times of 'getting the lights back on'. Another example is if you had a 'security incident' at a critical facility then are you non-compliant because the law enforcement officers have crossed some physical perimeter without our training or our having a record of their background check? There needs to be provision for an exception process in cases of "formally declared" critical situations where it's in the interest of reliability that we temporarily suspend the requirements. No entity should be found non-compliant with this standard because of required actions in the name of reliability.

Comment 2 - Excessive reporting Requirements:
The standards are overly prescriptive in describing how to implement and how to document compliance. All such prescriptive details should be omitted. Also, there are excessive requirements for documentation, even though the documentation itself adds no value from a security perspective. For example: CIP-007 Systems Security Management requires the documentation of the status and configuration of all ports and services available on all Cyber Assets (not just the critical cyber assets) inside the Electronic Security Perimeter(s). Consider a network consisting of 100 nodes. With 64,000 possible ports per node, you then have 6,400,000 data points. And this is even before you add services which seems to be excessive documentation.

Comment 3 - Onerous background checks:
CIP-004 Personnel and Training requires that all personnel have a personnel risk assessment performed and take specific NERC Cyber security Training prior to having access to a critical cyber asset. This could potentially delay emergency system restoration when mutual aid resources are being used. An exemption for emergencies should be included. Normal fitness for duty and supervisory observation should be adequate in addressing continual personnel risk assessments.

Comment 4 - This standard is drafted with the implied conditions that the Critical Cyber Assets identified are in the possession of and controlled by the responsible entity. In most cases this is true but in some cases this might not be. Current examples are OASIS and tagging services and in some cases certain tasks may be expanded to EMS services in the future. For instance, in the arrangement where a vendor is providing an "application service" arrangement, the physical cyber asset (such as the servers) might be located away from the responsible entity's facility that contains the client hardware. In this case, the vendor's site would most likely become a physical and cyber security perimeter. Since the vendor is not ultimately responsible for compliance with this standard (i.e., the responsible

Response:

1. Emergency situations are address in CIP-003. Responsible Entities may not take exceptions to NERC Standards, however, they may write exceptions totheir own policies and procedures that implement the requirements of these standards.

2. The Drafting Team has removed prescription where possible. The prescriptiveness that remains is necessary to provide the clarity requested by a majority of commenters.

The documentation required by these standards allows Responsible Entities to demonstrate that the policies, processes, and procedures that they have implemented consistently comply with the requirements of these standards.

3. See response to 1, above.

4. The Critical Cyber Asset owners are responsible for compliance with these standards. Actions taken in compliance with these standards may be delegated as determined by specific agreements and contracts between the parties

entity is always responsible), this places additional liabilities and obligations on the vendor-customer relationship that would have to be worked out most likely from a contractual standpoint. This may become impractical as each responsible entity using a vendor's product tries to obtain terms with a vendor that fits its expectations and requirements compliant with its local physical and cyber policies. Practically speaking, how are the responsible entities suppose to comply with tracking and measurement documentation

Drafting Team Responses to General Comments

Name Linda Campbell

Entity FRCC

Comments

Overall this standard is a vast improvement over the previous drafts and we appreciate the time and effort the committee took in improving the consistency and understandability of the standard.

We will vote on whether this standard is ready to be distributed for balloting after all comments are completed.

This standard does not provide a minimum baseline for compliance. For example, it should state that at the Cyber Security perimeter, at a minimum, firewalls or devices that perform firewall functions should be install at all ingress/egress points. These devices should restrict traffic as required by the standard.

GENERAL COMMENTS ON THE NERC ONLINE COMMENTING FORMAT:

1. The online entry tool is not user friendly.
2. There is no way of getting a receipt that our comments were accepted into the database
3. There is no ability to get a copy of the comments entered into the online forms.
4. The idea of submitting comments separated out by the R#, M# and C# is a very good idea and helped commenter the ability to link requirements to measurements and to the compliance levels.

Response:

CIP-003 through CIP-009 provide the minimum set of requirements that Responsible Entities must meet to protect Critical Cyber Assets. Because of the diverse nature of the industry and the diversity of available solutions, the standards do not mandate specific technologies or methods of meeting these requirements.

Comments on the commenting form have been passed along to NERC.

Drafting Team Responses to General Comments

Name Roger Champagne

Entity Hydro-Québec TransÉnergie

Comments	We believe there is an unnecessary complexity that exists in the levels of non-compliance. The Standard seems to be more process oriented as opposed to goal oriented.	**Response:**	The levels of noncompliance have been rewritten. The documentation required by these standards allows Responsible Entities to demonstrate during an audit that the policies, processes, and procedures that they have implemented consistently comply with the requirements of these standards.

Drafting Team Responses to General Comments

Name Theodore Creedon, P.E.

Entity Creedon Engineering

Comments Federal matching funds should be made available for implementation.

Response: This issue is beyond the scope of these standards

Drafting Team Responses to General Comments

Name Joel De Granda

Entity Florida Power and Light

Comments This standard does not provide a minimum baseline for compliance. For example, it should state that at the Cyber Security perimeter, at a minimum, firewalls or devices that perform firewall functions should be install at all ingress/egress points. These devices should restrict traffic as required by the standard.

Response: Please see responses to Linda Campbell, FRCC.

Drafting Team Responses to General Comments

Name Richard Engelbrecht

Entity RGE

Comments NPCC Participating members believe there is an unnecessary complexity that exists in the levels of non-compliance.

The Standard seems to be more process oriented as opposed to goal oriented.

Response: Please see responses to Roger Champagne, Hydro-Québec TransÉnergie.

Drafting Team Responses to General Comments

Name Ken Fell

Entity New York ISO

Comments We believe there is an unnecessary complexity that exists in the levels of non-compliance.

The Standard seems to be more process oriented as opposed to goal oriented.

Response: Please see responses to Roger Champagne, Hydro-Québec TransÉnergie.

Drafting Team Responses to General Comments

Name	Francis Flynn		
Entity	National Grid USA		
Comments	National Grid believes that there is unnecessary complexity that exists in the levels of non-compliance. The Standard seems to be more process oriented as opposed to goal oriented.	**Response:**	Please see responses to Roger Champagne, Hydro-Québec TransÉnergie.

Drafting Team Responses to General Comments

Name Jerry Freese

Entity American Electric Power

Comments

NERC should perform a risk-based business case as to the cost of implementing these standards industry-wide before approving and implementing such standards.

There is concern with regard to the Responsible Entity's ability to protect and maintain confidentiality of the information required to adhere to these standards when the Responsible Entity will be audited by the Regional Reliability Organization. It could become challenging for the Responsible Entity to keep Critical Infrastructure Protection information out of the public when information needs to be shared with outside organizations for auditing purposes.

The term "roundtable protocol" is used in the document several times. The definition is in the FAQs and should also be included in the standards definition preceding each each section.

There are few if any references to inspections (planned or unannounced) in these standards. Maybe they're addressed somewherre else, but I'd like to know a little about how these standards are enforced, not just descriptions of the various levels of non-compliance.

Each section starts with development steps. The intended audience may know who SAC and SARs are, but not everyone is familiar with those terms and I did not see them defined.

Response:

The need for Cyber Security Standards was brought to NERC from industry via a Standards Authorization Request (SAR). The SAR was developed into a scope document that was presented for public review and comment. A consensus of reviewers believed the need to move forward with developing cyber security standards per the scope of the SAR was appropriate. The risk assessment process is left to the Responsible Entity.

Data Confidentiality Agreements are in place and all auditors are required to sign them and handle sensitive information appropriately.

The concept of routable protocols are well understood in the IT industry and re-defining the terms for inclusion in NERC's Glossary NERC's "Glossary of Terms Used in Reliability Standards" could create unnecessary confusion.

Please see NERC's web site for a description of the Compliance Enforcement Program.

The terms Standards Authorization Committee (SAC) and Standard Authorization Request (SAR) are defined in NERC's Standards Process Manual, which is available for review and download from NERC's web site.

Drafting Team Responses to General Comments

Name Edwin C. Goff III

Entity Progress Energy

Comments

If a single entity is registered with multiple functional areas (Balancing Authority, Transmission Owner, Generator Owner), will the single entity submit separate compliance certifications for each separate functional area?

With UA1200 standards, the forms which were created by & submitted to Regional bodies only allowed for entries as 100% Compliant or as Non-compliant; there was no "Substantially Compliant" entry permissible. Will the new compliance forms allow entities to file as "BW", "SC", or "AC" ?

Response:

These are NERC Compliance Enforcement Program issues and beyond the scope of these standards.

Drafting Team Responses to General Comments

Name Kathleen Goodman

Entity ISO New England Inc

Comments

In general, the non-compliance sections of all these CIP standards appear to be complex and, in most instances, focused on maintaining processes instead of accomplishing goals. We would encourage the drafting team to look at each of the non-compliance sections to not only streamline the non-compliance measures and levels but to also acheive the fundamental goals of each of the standards (it appears as though, the way the non-compliance sections are written, that there was just a one-to-one correlation of requirements to compliance).

The CIP002-009 draft standards appear to use the terms "documents," "records," and "data" interchangeably. This is very confusing to personnel with ISO9000 experience and who have responsibilities for corporate record management programs. A set of definitions for documents, records, and data is being provided. It is recommended that the drafting team further review CIP002-009 to provide greater clarity for all requirements, measures, and compliance levels. This is key to better understanding how these items are to be handled and retained for compliance purposes.

Documents explain what an organization plans to do and instruct its employees how they should perform their tasks. Documents include but are not limited to policies, processes and procedures, blank forms, specifications, drawings, maps, etc. Documents must be reviewed and approved and can be revised.

Records are evidence that an activity has been conducted. Records provide a snapshot of past actions, events, and outcomes, demonstrate compliance with policies and procedures, demonstrate accomplishments, and can only be modified or revised in compliance with proper and auditable trails.

Data is information in a raw form that can be used as a reference or to extract information via analysis that is collected for examination and consideration and used to help decision-making, or information in an electronic form that can be stored and processed by a computer.

Response:

The levels of noncompliance have been rewritten.

The documentation required by these standards allows Responsible Entities to demonstrate during an audit that the policies, processes, and procedures that they have implemented consistently comply with the requirements of these standards.

The Drafting Team has revised the standards for consistency. Please see the FAQs.

Drafting Team Responses to General Comments

Name	Jerry Heeren
Entity	MEAG Power

Comments

Certain items in the FAQ need to be addressed further as shown below:

1) Question #9 of the FAQ for CIP-002 needs to be clarified further with regard to the section beginning "Frame relay, without....". Clarification of the "additional protocols" in this section would be helpful. In general, the term "on top of" is confusing when dealing with multiple protocols. Frame relay may encapsulate IP protocol which would make the IP protocol data and would require the frame relay equipment (generally a router) to remove the data from the frame packet and reconstruct it as IP protocol. This effectively makes the IP protocal a tunnel that would require an attacker to obtain a connection into frame cloud, guess the DLCI of the target device and guess the IP addresses of the equipment connected to the frame relay device at the target site. In addition, when the frame relay data is encrypted, is it really IP protocol any more? It seems as if wrapping the IP protocol in an encrypted frame packet would be due diligence".

2) Question #13 in the FAQ for CIP-002 needs to be clarified further - i.e., Is the answer to question #13 in the FAQ saying that all of the entities in a jointly owned asset are responsible for all of the personnel, or if one entity is out of compliance would all the entities be out of compliance?

Response:

1) The FAQ has been updated to provide additional sources of information regarding telecommunications or networking protocols.

2)

Drafting Team Responses to General Comments

Name Peter Henderson

Entity Independent Electricity System Operator (IESO)

Comments

1. The IESO believes there is an unnecessary complexity that exists in the levels of non-compliance.

2. The Standard seems to be more process oriented as opposed to goal oriented.

Response: Please see response to Roger Champagne, Hydro-Québec TransÉnergie.

Drafting Team Responses to General Comments

Name	E. Nick Henery		
Entity	SMUD		
Comments	The Drafting Team will need to go through the Standard and assign responsibility to each function from the functional model like the Version 0 STD. For this Standard to enforceable the generic use of Responsible Entity is the same as the generic use of Control Area. Even if the Standard lists the different functions it leaves open the possibility of misinterpretation as to which function is truly responsible.	**Response:**	The Responsible Entities are clearly enumerated in the each standard, Section A, item 4.

Drafting Team Responses to General Comments

Name Richard Kafka

Entity Pepco Holdings, Inc.

Comments

Draft 3, of the proposed NERC Cybersecurity Standards reflects a dramatic improvement over the previous two drafts. However there still are a number of critical items that need to be addressed (e.g. scope - required versus required for risk based assessmsnet, exception process for emergencies, audit quidelines or standards).

There needs to be a consistent waiver or exceptions policy implemented by NERC. For example, it may not be possible or prudent to enforce all aspects of normal access control procedures during emergencies such as resulting from natural disasters or events involving law enforcement personnel. Moreover, CIP-003-R3, -3.2 and -M3, and CIP-004-C1.4, for example, specifically refer to "exceptions." Thus, it is unclear whether (a) exceptions in an of themselves will result in noncompliance, (b) exceptions can exist for other Standards even where not mentioned, (c) or exceptions can or must be "built in" to policies (for example, whether a policy can avoid a possible future noncompliance situation by mentioning in advance how and under what circumstance some or all aspects of it can be approriately or properly disregarded).

The Risk Assessment Whitepaper still has not been published on either the NERC-CIPC or the ES-ISAC site. That is needed before the next draft in order to have a better understanding of CIP-002.

Why do standards CIP-002 through CIP-009 have different levels of noncompliance, when other standards, such as CIP-001, do not have such levels? Is there a need for consistnecy across all NERC standards?

For CIP-002 through CIP-009, the Regional Reliability Organization is listed as having the Compliance Monitoring Responsibility. Who is responsible for auditing the Regional Reliability Organizations? If there is a need to audit the RROs, should this be listed in the standard?

Add C in front of each compliance section (CIP-002 through CIP-009) to be consistent with comment form. (e.g. instead of 1.1 use C1.1 in each standard). This would be consitent with reguirements and measurement sections which use a R or a M.

The document 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. This is important from an audit stand point. Consideration should at least be given to the FAQ becoming a NERC Reference Document.

Response:

Emergency situations are addressed in CIP-003. Responsible Entities may not take exceptions to NERC Standards, however, they may write exceptions totheir own policies and procedures that implement the requirements of these standards.

The Risk Assessment Whitepaper is now available on the ESISAC website at www.esisac.com/library.html.

The Drafting Team has rewritten the levels of noncompliance. The rewritten levesl have been reviewed by NERC's Compliance Enforcmeent Program personnel and found to be saisfactory.

The standards have been modified to show that NERC will monitor the RROs and a third party without vested interest in the outcome will monitor NERC.

The Drafting Team may not change the NERC-approved standards format.

The Drafting Team has recommended to NERC that the FAQs be adopted as a Reference document.

The Drafting Team has reviewed and modified the FAQS as necessary to address comments it received during the third round of public review and comment on these standards.

Drafting Team Responses to General Comments

FAQ pg 4, Q12: This suggests that a generation dispatcher located within a marketing group is considered a Generation Control Center and a critical asset, even when the only control of generation they have is through verbal communication. Since most generation instruction is based on guidance from the market operator (PJM in our case), we do not appreciate how the failure or compromise of a cyber asset related to the dispatcher can significantly impact the ability to operate generation and/or have any significant impact on the reliability of the power grid. Please clarify.

FAQ pg 5, Q14: Is this consistent with CIP-005? CIP-005 implies communication within the electronic security perimeter is in scope.

FAQ on 009 secure storage - Is same level of secuirty of cyber and physical required for data storage?

Drafting Team Responses to General Comments

Name John Lim

Entity Con Edison

Comments

1. Compliance levels are unnecessarily complex.

2. The standards should focus on objective oriented requirements with minimal reference to specific implementations or technologies.

Response: Please see response to Roger Champagne, Hydro-Québec TransÉnergie.

Drafting Team Responses to General Comments

Name Deborah Linke

Entity Bureau of Reclamation

Comments

The categorization of Critical Cyber Assets and the subsequent requirements are still very broad and allow very little room for applying a risk assessment process that directs resources to those areas that pose the most risk. If implemented as written, Reclamation is concerned that the Cyber Security Standard could well dilute the focus of our efforts to protect critical equipment since it also requires, absent risk assessment, that a utility also protect equipment that poses little risk, leaving fewer resources to protect high-risk equipment.

The standards as written are somewhat technology dependent. The nature of data communications is rapidly changing and a risk-based assessment process allows progression as those changes occur.

Response:

CIP-002 Requirement R1 has been re-written and the list of "Required Critical Assets" removed. Responsible Entities are now required to use a risk assessment to identify a Critical Assets will now be determined by risk assessment. Please see responses to comments on CIP-002.

Drafting Team Responses to General Comments

Name Paul McClay

Entity Tampa Electric

Comments	Response:
Overall this standard is a vast improvement over the previous drafts and we appreciate the time and effort the committee took in improving the consistency and understandability of the standard.	
Numbering -- you’ve numbered requirements R1, R2 etc. and Measures M1, M2, etc. but compliance (section D) is numbered 1, 2.1, 2.2, etc. It would be more consistent to use C1, C1.1, C2, etc.	The numbering is part ofhte Standard template, which the Drafting Team cannot change.
Where it makes sense and for consistency, the Requirements should be in the form "The Responsible Entity shall..." Not all are.	The requirements statements have been revised as suggested.
FAQ’s Certain items in the FAQ’s do more than clarify the intent of the standard; they add criteria or requirements that should be in the standard. We believe that where this is true, this additional information belongs in the standard, not the FAQ as "the standard" is that to which entities must comply, not the FAQ. Examples of this include:	The drafting team has attempted to remove all language in the FAQs that could be misinterpreted as additional requirements.
CIP-002 question 11 CIP-003 question 8 (separation of duties, not in the standard so if that is important it should be in the standard) CIP-004 question 7 CIO-006 question 3 CIP-006 question 8 CIP-006 question 13.	

Drafting Team Responses to General Comments

Name David McCoy

Entity Great Plains Energy/Kansas City Power & Light

Comments	Overall, no provison has been made for emergencies such as hurricanes, tornados and ice storms. In these events these requirements need to be relaxed to the extent deemed necessary by the responsible party.	**Response:**	CIP-003 R1.1 addresses the issue of emergency waivers.

Drafting Team Responses to General Comments

Name	Jeff Mitchell
Entity	ECAR

Comments No other comments from ECAR TSPP or CIPP related to IROL. ECAR CIPP submitted comments separately.

Response: Please see responses to Larry Conrad, ECAR CIPP.

Drafting Team Responses to General Comments

Name	Scott Mix
Entity	KEMA, Inc

Comments When a technical feasibility clause is included in any of the requirements, there should be some form of record indicating that the action is technically infeasible, and why (e.g., IED model xxx does not support individual user accounts). As written now, it's almost to easy to opt out of a requirement by stating it's technically infeasible.

Response: A FAQ has been added to address this concern.

Drafting Team Responses to General Comments

Name	Darrick Moe		
Entity	WAPA		
Comments	It would add clarity and reduce confusion, if under Levels of Non-Compliance where there are multiple items which constitute a given level of non-compliance; to add text that indicates that any of the items listed constitutes the given level of non-compliance.	**Response:**	The levels of noncompliance are written as "or" statements meaning that any one constitutes the given level of non-compliance.

Drafting Team Responses to General Comments

Name Kurt Muehlbauer

Entity Exelon

Comments

Exelon fully supports the protection of critical cyber assets that impact the reliability of the bulk electric system operations. Exelon respectfully submits the following comments to seek clarification on the standard and for consideration in the next draft of the permanent standard. Exelon is ready and willing to support NERC in creating an effective cyber security standard for the industry.

1. As currently written, Exelon will vote "no" on CIP-002 through CIP-009 because these standards do not assess cyber security. They are administratively prescriptive and the compliance measures have no relationship to measuring levels of security.

Compliance levels are flawed in that they measure documentation completeness with no relevance to actual cyber security. This trivializes the meaning of the compliance levels. An entity could fail many of the standards due to lack of completed documentation, while their computer and network systems meet and even exceed the security requirements.

To this point we re-iterate comments on draft 3 developed by EEI:

"The industry needs to be extremely careful to avoid the creation of purely documentation-based non-compliances. With increasing legal requirements for compliance, and the associated penalties for noncompliance, noncompliance should be reserved for "real" security issues. It is simply too easy to make a mistake in documentation in light of the constantly evolving cyber environment. In the Version 0 Operating Standards, for instance, non-compliance is reserved for operating the grid in an unstable manner, not for failing to keep the phone number of a senior management official updated. Compliance will tend to be seen by the public and by regulators as purely binary, YES or NO — they will not be likely to understand, or forgive, a purely documentary failure. This could be addressed by making the levels of non-compliance much more generic or general....

One simple way to make the standard less prescriptive but still accomplish all the security and auditing goals would be to remove all documentation requirements from the requirement sections. Move documentation to the measures section, and have general measures that would require adequate and reasonable documentation of compliance to the requirements. This would help shift the focus from paper auditing to cyber security auditing. In addition, it would also reduce the potential for inflexible interpretations of the standards by third party auditors..."

Other regulatory entities are using these standards to establish regulatory law. Therefore it is critical that these standards accomplish what they are intended to accomplish.

2. We recommend modifying CIP-002 to make the risk based analysis the primary criteria for determining which assets are critical. R1 should require that control rooms are required critical assets, but all other critical assets should be identified through a risk-based analysis. An asset’s true impact to the system should determine whether it is critical. We also

Response:

1. The Drafting Team has reviewed the standards and removed prescription where possible. The prescriptiveness that remains is necessary to provide the clarity requested by majority of commenters.

The documentation required by these standards allow Responsible Entities to demonstrate that the policies, processes, and procedures that they have implemented consistently comply with the requirements of these standards.

2. The list of "Required Critical Assets" in CIP-002 R1 has been removed. The identification of Critical Assets is to be done using a risk-based assessment. Please see the revised CIP-002 and responses to comments for CIP-002.

3. The use of "reasonable business judgement" when interpreting and implementing these standards is included in the purpose statement of each standard. A FAQ also address this concept.

4. The standards do not dictate how Responsible Entities must implement the requirements of these standards; rather, it leaves those decisions up to each entity using "reasonable business judgment." See response above.

5. Measures and levels of noncompliance have been reviewed and modified as necessary. Please see response to comments for each standard.

believe that determination of criticality must be done by each entity with input from the entity’s RTO and regional reliability organization.

For example, a variety of criteria must be considered when determining whether or not a generation asset is critical. These include base load and peaking, the size of the region, the capacity factor and the geographical location.

3. There should be a definition for "reasonable" and the drafting team should develop an adequate definition and include this term where applicable in the requirements and measures. We recommend the drafting team consider the following definition drafted by EEI:

"Reasonable: The quality of measures such as controls, methodologies, plans, safeguards, or otherwise, that permit implementation of this Standard as appropriate to each individual Responsible Entity implementing this Standard under its own reasonable business judgments, in consideration of such factors as the size of the entity, the nature of its activities, the nature of the risks it faces, administrative and financial burdens, and the potential impact on the public, the electric grid, and its own business of harm to its critical cyber, and associated physical, assets."

4. It is imperative that each responsible entity has the latitude to develop consistent enterprise programs that meet all applicable reporting and regulatory requirements. Responsible entities are also required to be compliant to SOX, NRC, FERC, and other regulatory bodies.

The current detailed explanations in the measures and compliance levels as to how compliance should be demonstrated, documented, and the prescriptions for review processes and frequency, do not provide the latitude necessary for entities to develop robust policies and procedures that can, where practical, meet various regulatory body requirements.

Drafting Team Responses to General Comments

Name Jeffrey Mueller

Entity PSEG Companies

Comments The PSEG Companies have reviewed and share the concerns expressed in the Comments of PJM and EEI. Accordingly, the PSEG Companies support the comments of PJM and EEI, and request that the concerns expressed in those comments be properly addressed in the next version of the draft standard.

Response: Please see responses to Laurence W. Brown, Edison Electric Institute.

Drafting Team Responses to General Comments

Name	Mitchell Needham
Entity	Tennessee Valley Authority

Comments TVA would also recommend a change in the criteria for critical assets from specific values of load and generation to system analysis based on single point failure to verify system stability.

Response: Please refer to response to comments submitted to CIP-002.

Drafting Team Responses to General Comments

Name Dave Norton

Entity Entergy Transmission

Comments General Comment on Use of Dates:

There are references to dates by when compliance is required and others about when compliance is reported. Largely, the labeling inconsistency exists between the Standards and the Implementation Plan. Suggestion: In both the Standards and the Implementation Plan consistently only refer to the time/date by which compliance is required -- not when it is reported. For purposes of the Implementation Plan, perhaps the Tables should be labeled "end of [yr]" to denote when Standards compliance is required. Compliance reporting and timetables is the aegis of the RRO.

Response:

The Implementation Plan has been modified to reflect changes to the standards. Reportability is not discussed

The following comments apply for all of the CIP standards, 002-009 individually:

Applicability

The Applicability sections are stilted. Note, for example, that in CIP-002-1 there are dog-chasing-tail references between section 3.1 and R.1.1.1. Applicable entities are listed in 3.1, but functions are not (see the whole list which includes parties rather than functions such as "NERC". This flaw exists despite "Functional Model" entities). R1.1.1. refers back to 3.1 as though it describes functions. It doesn't. This is a consistent flaw throughout the standards.

The list of entities in the Applicability section comes from NERC's Functional Model.

Measures

None of the measures are written as measures. They are all incomplete sentences with few verbs and no direction on how to measure those sentence fragments. Almost all appear intended to be measured as Pass or Fail. These all need to be rewritten to indicate what the measure is. For example, in many cases just adding, "The Entity has or does not have...documentation (or whatever)" would cure this problem. From a legal and grammar perspective the current format is unenforceable and does not make sense in the English language.

The measures have been rewritten to refer back to requirements. The measure statements are complete when read in context with the opening clause.

Levels of Non-Compliance

These levels are written in complete sentences and are understandable as the Measure should be. After the Measures are rewritten, the Levels of Non-Compliance should be examined and reworked as well. Some of the measures have no non-compliance associated with a failure to achieve the intent of the measure. This may have been intentional, but it is one of the things to check for. Additionally, the Levels of Non-Compliance should be written in parallel with the measure that they refer to. In other words the non-compliances for Measure 1 should appear as the first few items in the non-compliance list, the non-compliances for Measure 2 should follow, etc. It is clear that some Measures may not be included in all of the levels of Non-Compliances, but nonetheless, the order should be easier to follow than it is now.

The levels of noncompliance have been rewritten.

Penalties

No Penalties or Consequences are listed for anything.

The Penalties section was removed from the Standard template. It is a Compliance Enforcement Program issue.

Drafting Team Responses to General Comments

Name Kevin Perry

Entity Southwest Power Pool

Comments	Southwest Power Pool concurs with the comments submitted by the ISO-RTO Council (IRC). The comments contained in this response are in addition to the IRC submission. The following general comments are also offered:	**Response:**	Please see responses to Karl Tammar, IRC.
	Many of the standards requirements are significantly changed from the Urgent Action standard currently in place. There should be no expectation that entities compliant with the 1200 standard will be able to easily come into compliance with the replacement standards.		The Implementation Plan proposed by the Drafting Team is intended to address issues associated with implementing the requirements of the CIP-002 through CIP-009.
	Many of the new requirements are onerous, requiring signififcant expenditures of dollars and addition of staff with no cost-benefit evaluation. With the cost pressures the industry faces today, each entity is having to carefully husband their resources and justify each expenditure. In that light, there needs to be a threat assessment performed to verify that the requirements of these standards are justified and not just requirements tossed onto the table because they sound good. The entities facing the costs of these standards must be assured that the threat is significant enough that their limited resources need to be devoted to these protections and not somewhere else where the threat is greater. To what extent has any credible threat information been factored into the development of these standards? What other credible threats exist that demand immediate mitigation and pose greater risk than what these standards address?		The need for Cyber Security Standards was brought to NERC from industry via a Standards Authorization Request (SAR). The SAR was developed into a scope document that was presented for public review and comment. A consensus of reviewers believed the need to move forward with developing cyber security standards per the scope of the SAR was appropriate. The risk assessment process is left to the Responsible Entity.

Drafting Team Responses to General Comments

Name	Tom Pruitt	
Entity	Duke Power Company	
Comments	We would like to thank the SDT for their efforts. It is clear that much work has gone into getting them to this point. Even though we do not think any of these are ready for ballot, the improvements made in each draft are very encouraging. The standards really look good from a cyber-security perspective; overall they are pretty clear and make sense. There is going to be quite a bit of expense in complying with this, but with that compliance there is quite a bit of risk reduction.	**Response:**

Drafting Team Responses to General Comments

Name Howard Rulf

Entity We Energies

Comments	Overall comments to the standard: Since this standard addresses both cyber and physical security, re-title the standard accordingly. Develop consistent risk management criteria matrices and other standard worksheet guidelines and check lists to strive for security consistency between complying organizations.	**Response:**	CIP-006 addresses physical security of Critical Cyber Assets. The standards allow each Responsible Entity to determine how it will implement the requirements.

Drafting Team Responses to General Comments

Name Lyman Shaffer

Entity PG&E

Comments

We believe that there needs to be regional clarity around which generation facilites are covered under this standard. The reference to the 80% single largest contingency means one thing while the references to black start systems could take us down to very small hydro generation facilities which should be outside the scope of this standard.

We also believe very strongly that the FAQ document should reflect the fact that each entity has some flexibility in the implementation of these standards based on their assessment of the risks and vulnerabilities identified in the process. They are ulltimately accountable for their performance.

Response:

The list of "Required Critical Assets" in CIP-002 R1 has been removed. The identification of Critical Assets is to be done using a risk-based assessment. Please see the revised CIP-002 and responses to comments for CIP-002.

The standards allow each Responsible Entity to determine how it will implement the requirements.

Drafting Team Responses to General Comments

Name Robert Strauss

Entity NYSEG

Comments

We believe there is an unnecessary complexity that exists in the levels of non-compliance.

The Standard seems to be more process oriented as opposed to goal oriented.

Response:

Please see responses to Roger Champagne, Hydro-Québec TransÉnergie.

Drafting Team Responses to General Comments

Name Karl Tammar

Entity IRC

Comments The following requirements are either new or substantially greater in scope than those appearing in NERC 1200:

Standard--Requirement Number
CIP-002--R1
CIP-003--R4
--R5
--R6
CIP-005--R1.1
--R1.2
--R1.3
--R1.4
--R1.5
--R2.3
--R2.4
--R2.5
--R3.1
--R3.3
CIP-006--R1
--R1.4
--R7
CIP-007--R1
--R6.1
--R6.2
--R6.3
--R7
--R8
CIP-008--R1.1
--R1.2
--R1.5
CIP-009--R4

Response: The scope of CIP-002 through CIP-009 (originally numbered 1300) is documented in the SAR and has been further developed via multiple rounds of industry review and comment.

Drafting Team Responses to General Comments

Name Robert C. Webb

Entity Instrumentation, Systems and Automation Society

Comments 1. Who is ISA and Why is ISA commenting on CIP-002 through CIP-009?

These comments were developed by members of the Instrumentation, Systems and Automation Society, (ISA), SP99, "Manufacturing and Control Systems Security" committee’s leadership team. The overall committee is composed of over 200 members including many users, government representatives, academics, control systems manufactures, and engineers with expertise in automation and control systems. ISA’s SP99 is working to develop control systems security standards that provide sufficient guidance to the control systems and IT domain stakeholders to assure that security risks can be appropriately reduced without adversely affecting the intended functionality of those systems. ISA has published over 150 pages of guidance specific to the application of cyber security to control systems, in the form of two technical reports: ISA’s ANSI/ISA-TR99.00.01-2004, "Security Technologies for Manufacturing and Control Systems", and ANSI/ISA-TR99.00.02-2004, "Integrating Electronic Security into the Manufacturing and Control Systems Environment." Both highlight the unique aspects of control systems which must be considered when applying security procedures and technology to control systems. ISA’s constituency includes both fossil and nuclear power plant automation practitioners, and ISA has active standards committees in both of these areas (SP77, Fossil Power Plant Standards, and SP67, Nuclear Power Plant Standards).

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 have been working with NERC to establish a liaison process that would allow such considerations to be addressed earlier in the process. The development of that liaison process is nearly complete. However, comments are due at this time, and we believe these issues need to be addressed now, before approval of these standards, for the standards to be effective, without damaging the systems they are intended to protect. Thus members of the SP99 committee leadership team, with domain expertise in power generation and associated control systems have put together summary comments in several areas that should be addressed before issue of these standards.

2. Overview and Summary of Essential Changes

In general, we found these documents to be excellent examples of how an industry group can (and should) provide coherent and well structured guidance on cybersecurity. We commend NERC’s drafting team and review process; it has resulted in a quality set of documents that should be widely used.

At the same time, and in fact because of the expected wide application of these documents, we believe that three general areas should be addressed before approval of these documents.

a)--Broader scope - to address a larger % of generation resources and key distribution

Response: Regarding comment #2a, the exclusionary language concerning generation assets has been removed with the exception of nuclear generation which is excluded by the SAR. Because distribution assets are not considered part of the Bulk Electric System, these resources remain excluded as well.

Regarding comment #2b, much of the prescriptive language on how certain security measures should be applied has been removed. For example, the requirement for port scans in CIP 005, R4.2 has been replaced by a requirement to review and verify only ports and services required for normal and emergency operations are enabled. In addition, the Drafting Team has removed most references to "how" security measures should be applied throughout the Standards unless it is required for compliance purposes.

Regarding comment #2c, language has been added to reflect the fact that some security solutions that are available today were not available when some legacy systems were designed and put into service. CIP-003, CIP- 004, CIP-005, and CIP-006 contain language addressing exceptions to their policies that may be required to deal with legacy systems and facilities where modern security solutions are not technically possible. In these cases, the Responsible Entities must identify and document the exception and describe the mitigating steps they are taking to secure the assets in lieu of the modern solution.

Regarding the comments #3, #4, and #5 related to scope, the Standard reflects the Standard Authorization Request which excluded distribution, nuclear generation, and telecommunication infrastructure. The Drafting Team cannot exceed the scope of the SAR.

A SAR reflects the industry consensus on the scope of any particular standard to be developed. Once SAR has been approved for standards drafting, the scope cannot be changed.

The NERC Reliability Standards process would require new SARs to address these scope issues

resources, and avoid excessive reliance on one boundary or layer of defense from cyber attacks. While we recognize the need to prioritize and prevent excessive requirements, we believe the current scope is overly restrictive, and excludes a significant portion of generation, and thereby significant vulnerabilities, in some areas. This is addressed in our specific comments on CIP-002-1, (and also CIP-003-1 through 009-1), which follow.
b)--Additional cautions and guidance for control systems - in the form of specific requirements and references to key industry documents, to assure that the measures applied do not result in systems failures and reduced reliability instead of reduced risk. These cautions and guidance are necessary to address the special considerations needed when applying many normal security practices to control systems and control system networks -- particularly the bulk of legacy systems in operation today. Many do not have any ability to provide most of the required security features, and can be adversely affected by the application of other requirements. One good example is the requirement to do port scans (CIP 005-1, R4.2). Many legacy control networks are halted by port scans. The standard should include this caution, and suggest the use of alternatives to identify open ports on operational systems which have not been specifically designed and demonstrated to support this kind of testing without production failures. In general, more specific guidance on how to apply these requirements to the many legacy systems in use today should be provided.
c)--Mandatory additional protection for inadequate legacy systems -- The phrase "where technically feasible" is used in a number of locations throughout the document. In many of these cases, alternatives are required. However, in others, no alternatives are required. Clearly stated requirements to add protection or barriers to cyber attack ("mitigation measures"), where they cannot be configured or incorporated into existing systems, should be added. It is not acceptable, in our view, to identify unacceptable risks, and then leave them because the existing equipment cannot be appropriately hardened. Appropriate countermeasures, to reduce risks to acceptable levels, should be required in all cases.

Addressing these concerns does not mean significant revision to this set of standards, or significant delay, in our opinion. It can be done effectively with minor changes and references in the generic text and in several specific locations. We suggest some of the specifics below. We believe these considerations are important to prevent the standards from being counterproductive or missing significant vulnerabilities.

3. Scope - Distribution assets that could have cyber impacts on transmission assets are excluded. All distribution assets that could have cyber impacts on Bulk Electric system assets should be included, to meet the objectives of the Standards. This comment also applies to the identical sections of the remaining standards (CIP-003 -- CIP-009).

4. Scope - Exclusion 3.2.1 should be removed; it excludes some of the larger generators that would otherwise be included under R1.1.4, and the NRC's requirements should be coordinated with, not independent of these requirements. This comment also applies to the identical sections of the remaining standards, (Section 4.2.1 of CIP-003 -- CIP-009).

5. Scope - Exclusion 3.2.2 should be removed; even when those communications systems are provided by others, the defined entities are still ultimately responsible for their proper operation and security. This comment also applies to the identical sections of the remaining standards, (Section 4.2.2 of CIP-003 -- CIP-009).

Drafting Team Responses to General Comments

Name Laurent Webber

Entity Western Area Power Administration

Comments

The categorization of Critical Cyber Assets and the subsequent requirements are still very proscriptive and allow very little room for applying a risk assessment process that directs resources to those areas that pose the most risk. Blindly following the NERC Cyber Security Standard may cause the utility industry to expend all available cyber security resources in protecting equipment that poses little risk, leaving no resources to protect high-risk equipment. The standard does not forbid a risk assessment process, but the standard demands so much be done for equipment on the NERC "list" that companies will be unwilling to expend further resources beyond the required "list."

The apparent assumption that "routable protocols" are high risk and other protocols are low risk is one example of oversimplification and/or an "off the cuff" risk assessment. The nature of data communications is rapidly changing and it is ridiculous to assume that out-dated equipment and protocols will be more secure than modern data communications. Certainly each entity should be able to weigh the threats and vulnerabilities to evaluate risks and apply the best technology to support reliability, security, and good business practices. An unintended consequence of the NERC Cyber Security Standard could easily be a compromise of reliability as entities delay the implementation of newer technology, better communications, and faster response techniques.

In conference calls, webcasts, personal conversations, and responses to comments Drafting Team members have referred to the FAQs or other supporting documents. This is not adequate. The Cyber Security Standard must stand on its own. Auditors will not go back to the FAQs and Standard Development Highlights to interpret what the Drafting Team meant, they will take a very strict and literal interpretation of the Cyber Security Standard. These standards must be written with enough clarity and definition to solidly stand on their own. The FAQ's should not used to add definition or clarity to standards since they are not part of the standards.

Response:

The list of "Required Critical Assets" in CIP-002 R1 has been removed. The identification of Critical Assets is to be done using a risk-based assessment. Please see the revised CIP-002 and responses to comments for CIP-002.

The standards allow each Responsible Entity to determine how it will implement the requirements.

The Drafting Team has reviewed and clarified the requirements in each standard to the extent possible. However, the requirement statements cannot contain examples or similar explanatory text to help Responsible Entities understand the requirements in their own contexts. This is the purpose of the FAQs. Highlights is merely to point out significant differences between drafts, not for use as an auditing tool.

Auditors will rely on the documentation created pursuant to. the these standards to determine compliance with these standards.

Drafting Team Responses to Comments on Definitions

Commentor	Raymond A'Brial
Organization	Central Hudson Gas & Electric Corp
Agree	No

Critical Asset

These standard definition has not been approved by the industry. This draft opens these definitions to changes by the industry.

change

Critical Assets: Those facilities, systems, and equipment which, if destroyed, damaged, degraded, or otherwise rendered unavailable, would have a significant impact on the ability to serve large quantities of customers for an extended period of time, would have a detrimental impact on the reliability or operability of the Bulk Electric System, or would cause significant risk to public health and safety.

to

Critical Assets: Those facilities, systems, and equipment which, if destroyed, damaged, degraded, or otherwise rendered unavailable, would have a significant detrimental impact on the reliability or operability of the Bulk Electric System.

Rational

A detrimental impact is too subjective. We suggest "significant adverse impact", which is defined as
<<
With due regard for the maximum operating capability of the affected systems, one or more of the following conditions arising from faults or disturbances, shall be deemed as having significant adverse impact:

transient instability

o -- Any instability that cannot be demonstrably contained to a well-defined small or radial portion of the system local area.

unacceptable system dynamic response

The definition has been revised to reflect industry consensus.

	o -- An unacceptable system dynamic response is characterized by an oscillatory response to a contingency that is not demonstrated to be clearly positively damped within 30 seconds of the initiating event. unacceptable equipment tripping: Unacceptable equipment tripping is characterized by either one of the following: o -- Tripping of an un-faulted bulk power system element (element that has already been classified as bulk power system) of under planned system conditions due to operation of a protection system in response to a stable power swing o -- Operation of a Type I or Type II Special Protection System in response to a condition for which its operation is not required voltage levels in violation of applicable emergency limits o -- loadings on transmission facilities in violation of applicable emergency limits >> The phrase public health and safety could include all hospitals. This may be outside the current BES definition. Entities may include or exclude such facilities, depending on their local need(s) or as part of their risk based assessment. Large quantities is a subjective term. Those words are beyond the scope of NERC's BES.	
Critical Cyber Asset		
Cyber Asset	IEDs that are connected the critical operational network should be protected according the Cyber Security Standard.	The definition does not preclude IEDs.
	This definition is an incomplete sentence, even in terms of the particular format followed by the other definitions.	The format of the definition has been revised.
	Also, the reference to "data" is unclear. Does this mean data in transit as well as in storage? Does it include business data? All backup data? Only the data required by these Standards to be maintained? SEE ALSO CIP-009-R4.	The term "data" is intentionally broad. The requirements of each CIP standard qualify the data to be considered.
Cyber Security Incident		

Electronic Security Perimeter		
Physical Security Perimeter	change from The physical six-wall border surrounding computer rooms, telecommunications rooms, operations centers, and other locations in which Critical Cyber Assets are housed and for which access is controlled. to The physical six-wall border surrounding computer rooms, telecommunications rooms, operations centers, and other locations in which Critical Cyber Assets are housed, where pratical, and for which access is controlled. Rational Some IEDs are in transformers. These IEDs should be protected according to these Cyber Security Standards. Drawing a physical security perimeter around these devices is not as simple as protecting a PC.	The definition has been revised to reflect industry consensus. Technical feasibility is more appropriately addressed in the requirements of each CIP standard.
	Some allowance must be made in the standards for differences in interpretation among regions and entities. Moreover, some recognition must be made of the fact that the ultimate standard of behavior for Responsible Entities is the legal principle of "reasonable business judgement." Resources are limited, and no asset or entity can ever be totally secure against any and all possible or potential cyber disruptions. For example, even the federal regulations requiring data security (a form of cybersecurity) in implementing the Health Insurance Portability and Accountability Act (HIPAA) generally refer to "reasonable" implementation. See also http://www.hhs.gov/ocr/hipaa/guidelines/incidentalud.pdf (federal agency explanatory document clarifying that "reasonable" data safeguards will be determined by what is appropriate under the particular individual circumstances of each covered entity). Therefore, we suggest the inclusion of similar phraseology in the Standards, with a "definition" indicating that compliance with any "reasonableness" requirement under the NERC Cybersecurity Standards will be determined by each Responsible Entity in a manner appropriate to it, and not subject to second-guessing during a compliance audit. Suggested Additional Definition: "Reasonable: The quality of measures such as controls, methodologies, plans, safeguards, or otherwise, that permit implementation of this Standard as appropriate to each individual Responsible Entity implementing this Standard under its own	Interpretation and implementation using reasonable business judgment has been added to the purpose statement of each CIP standard. A FAQ addresses reasonable business judgment.

reasonable business judgement, in consideration of such factors as the size of the entity, the nature of its activities, the nature of the risks it faces, administrative and financial burdens, and the potential impact on the public, the electric grid, and its own business of harm to its critical cyber, and associated physical, assets."

Drafting Team Responses to Comments on Definitions

Commentor	Ori Artman
Organization	Teltone
Agree	Yes
Critical Asset	
Critical Cyber Asset	
Cyber Asset	
Cyber Security Incident	
Electronic Security Perimeter	
Physical Security Perimeter	

Drafting Team Responses to Comments on Definitions

Commentor	Steve Badgett	
Organization	Riverside Public Utilitities	
Agree	No	
Critical Asset		
Critical Cyber Asset		
Cyber Asset	We are a mid-sized distribution utility, with no bulk electric assets, and a small amount of peaking generation. -- Draft 2 defined "Cyber Assets" as "those programmable electronic devices and communication networks including hardware, software, and data associated with bulk electric system assets" Draft 3 now defines "Cyber Assets" as "those programmable electronic devices and communication networks including hardware, software, and data", without any reference to the bulk electric system. -- Our utility is primarily a Distribution Provider (in the terms of the NERC Functional Model), without any assets associated with the bulk electric system. We do have a minor amount of generation, however, and according to the NERC Functional Model, we are also a Generation Owner, a Generation Operator, and a Load-Serving Entity. As a consequence, we are subject to compliance with the Security Standards. -- According to the Draft-2 definition of "Cyber Assets", our utility did not have any "Cyber Assets", consequently did not have any "Critical Cyber Assets", and therefore was exempt from the requirements of CIP-003-1 through CIP-009-1. (Compliance with CIP-002-1 was required however.) -- Because of the change in the definition of "Cyber Assets" (eliminating the reference to the bulk electric system), our utility now finds that it now does have "Cyber Assets". Since our utility has equipment which, if destroyed or damaged, certainly "would have a significant impact on the ability to serve large quantities of customers for an extended period of time" and certainly "would cause a significant risk to public health and safety", we also have "Critical Assets". And, following from the changed definition, our utility finds it now has "Critical Cyber Assets". -- Consequently, if we follow the logic of the definitions, according to the Draft 3 standard, we are now subject to the requirements of CIP-003-1 through CIP-009-1. We do not think that this represents NERC's intent, but is nevertheless a consequence of the changed definition.	The definitions are intentionally broad, as they will be added to NERC's "Glossary of Terms Used in Reliability Standards" for potential use in other Reliability Standards. For the purposes of these CIP standards, the requirements of CIP-002 further qualify the definition of Critical Asset and Critical Cyber Asset.

Drafting Team Responses to Comments on Definitions

Cyber Security Incident

Electronic Security Perimeter

Physical Security Perimeter

Drafting Team Responses to Comments on Definitions

Commentor	Terry Baker	
Organization	Platte River Power Authority	
Agree	No	
Critical Asset	"Large quantities of load for an extended period of time" is to arbitrary. Time period needs to be stated, and the load quantity needs to defined as a percentage of system load or a specific MW value.	The definition has been revised to reflect industry consensus.
Critical Cyber Asset		
Cyber Asset		
Cyber Security Incident		
Electronic Security Perimeter		
Physical Security Perimeter		

Drafting Team Responses to Comments on Definitions

Commentor	Terry Bilke
Organization	Midwest ISO
Agree	No
Critical Asset	
Critical Cyber Asset	
Cyber Asset	
Cyber Security Incident	
Electronic Security Perimeter	
Physical Security Perimeter	

Drafting Team Responses to Comments on Definitions

Commentor	Pat Bourassa	
Organization	Wisconsin Public Service Corporation	
Agree	No	
Critical Asset	The current definition of "Critical" cyber assets is insufficient. It is not reasonable to mandate that any and every computer component located within four (or six) walls of a critical asset would ipso facto be considered critical. Please consider language that would allow companies to use reasonable judgement for determining "Critical Cyber Assets."	This definition serves as a broad basis. Responsible Entities are to use a risk assessment to define their Critical Cyber Assets. Please refer to CIP-002.
Critical Cyber Asset		
Cyber Asset		
Cyber Security Incident		
Electronic Security Perimeter		
Physical Security Perimeter		

Drafting Team Responses to Comments on Definitions

Commentor	Laurence W. Brown	
Organization	Edison Electric Institute	
Agree	No	
Critical Asset		
Critical Cyber Asset	This definition is an incomplete sentence, even in terms of the particular format followed by the other definitions. Also, the reference to "data" is unclear. Does this mean data in transit as well as in storage? Does it include business data? All backup data? Only the data required by these Standards to be maintained? SEE ALSO CIP-009-R4.	Please see responses to Ray A'Brial, Central Hudson Gas & Electric Corp.
Cyber Asset		
Cyber Security Incident		
Electronic Security Perimeter		
Physical Security Perimeter		
Additional	Some allowance must be made in the standards for differences in interpretation among regions and entities. Moreover, some recognition must be made of the fact that the ultimate standard of behavior for Responsible Entities is the legal principle of "reasonable business judgement." Resources are limited, and no asset or entity can ever be totally secure against any and all possible or potential cyber disruptions. For example, even the federal regulations requiring data security (a form of cybersecurity) in implementing the Health Insurance Portability and Accountability Act (HIPAA) generally refer to "reasonable" implementation. See also http://www.hhs.gov/ocr/hipaa/guidelines/incidentalud.pdf (federal agency explanatory document clarifying that "reasonable" data safeguards will be determined by what is appropriate under the particular individual circumstances of each covered entity). Therefore, we suggest the inclusion of similar phraseology in the Standards, with a "definition" indicating that compliance with any "reasonableness" requirement under the NERC Cybersecurity Standards will be determined by each Responsible Entity in a manner appropriate to it, and not subject to second-guessing during a compliance audit. Suggested Additional Definition: "Reasonable: The quality of measures such as controls, methodologies, plans, safeguards, or otherwise, that permit implementation of this Standard as appropriate to each individual Responsible Entity implementing this Standard under its own reasonable business judgement, in consideration of such factors as the size of the	

entity, the nature of its activities, the nature of the risks it faces, administrative and financial burdens, and the potential impact on the public, the electric grid, and its own business of harm to its critical cyber, and associated physical, assets."

Drafting Team Responses to Comments on Definitions

Commentor	Peter Burke	
Organization	American Transmission Company	
Agree	No	
Critical Asset		
Critical Cyber Asset		
Cyber Asset	American Transmission Company concurs with the comments submitted separately by the Edison Electric Institute.	Please see responses to Laurence W. Brown, Edison Electric Institute.
Cyber Security Incident	American Transmission Company concurs with the comments submitted separately by the Midwest Reliability Organization.	
Electronic Security Perimeter		
Physical Security Perimeter		
	American Transmission Company concurs with the comments submitted separately by the Edison Electric Institute and by the Midwest Reliability Organization.	

Commentor	Marc Butts	
Organization	Southern Company	
Agree	No	
Critical Asset	The words "damaged, degraded," should be deleted. Using "or otherwise rendered unavailable," should be sufficient. The words “damaged” and "degraded" are too broad and could be misinterpreted.	The definition has been revised to reflect industry consensus.
Critical Cyber Asset		
Cyber Asset	The standard is written primarily with tangible, physical assets in mind. However, this base definition upon which “critical cyber assets” rests includes the words “data” and “software”. If “data" is included as a critical cyber asset for example, then vast numbers of requirements can not be met in the remaining standards. In addition, the reference to “data” is unclear. Such open-ended language is so ambiguous that there are serious concerns as to whether full compliance is possible.	These terms, including "data" are intentionally broad. The requirements of each CIP standard qualify these terms as necessary.
Cyber Security Incident	Delete the word "suspicious" because it is too broad and could be misinterpreted.	Responsible Entities are expected to use reasonable business judgment when interpreting these definitions and implementing the requirements of the CIP standards. Please see the FAQs.
Electronic Security Perimeter		
Physical Security Perimeter		
	The Levels of Noncompliance lean towards the extreme when compared with other NERC standards, such as the Version 0 Operating standards. For instance, it appears in the Version 0 standards the intent is to only flag as noncompliant those things that are discrete and measurable and auditable and that are of sufficient importance. Compare this to the cyber standards where we seem to be looking for the smallest of things in order to generate a non-compliance. Compare CIP-008 with CIP-001 which both concern incident reporting. We need some middle ground and some common severity levels. A Level 4 cyber non-compliance should be as 'bad' as a Level 4 operating non-compliance, etc.	The levels of noncompliance have been rewritten in most CIP standards.
	There are many non-compliance levels that revolve around making updates to documentation within a certain amount of time after a change. However, there is no requirement to maintain a list of all the various changes (nor should there be). As a result, there is nothing to audit to prove or disprove the non-compliance. We suggest dropping these levels and reviewing all non-compliance levels from the auditor	The levels of noncompliance have been rewritten in most CIP standards.

perspective as to what an audit team would use to verify the requirement was met. Auditing a document to insure it was reviewed and signed off on a regular basis as outlined in the standard is easily verified by an auditor. Auditing a document to insure that it was updated within 30 days of some change is not. Such open-ended requirements are so ambiguous that there are serious concerns as to whether full compliance is possible.

For example, there is no description of what types of changes need to be tracked, or what triggers the timeline for making updates to the documentation regarding such changes.

Commentor Linda Campbell

Organization FRCC

Agree No

Critical Asset

We believe the definition of Critical Asset must be modified. We will not support approval of this standard until modification is made.

“Critical Asset” in Draft 2 was previously identified as "Bulk Electric System Asset" in Draft 1. Areas of concern are:

1. The Drafting Team responded to the FRCC Comments on the definition of Critical Assets in Draft 2 by simply stating that this definition had been “approved by NERC’s Critical Infrastructure Protection Committee on September 16, 2004” as well as the Control Systems Security Working Group and the Risk Assessment Working Group.

a. If there was never an intention of revising this definition, why wasn’t this stated in the Draft Standard? Why ask for public comments on Draft comment form?

b. The point of an open process is for the industry to come to consensus. We would like to assume that any definition approved by a NERC committee would be open to change. The Draft Standard and its definitions are starting points for discussion by industry participants.

i. If comments received in Draft 1 and 2 showed a desire for a clearer definition, it should have been the Drafting Team’s task to take that definition back to the committee so further work.

ii. This definition has implications on many reliability standards, not just those regarding critical infrastucture protection. The CIPC is not the only group of individuals to provide input on this definition.

iii. Why was only the definition of “Critical Asset” unchangeable, while changes were allowed for “Cyber Assets,” Cyber Security Incident,” and “Electronic Security Perimeter?”

2. The definition should help Responsible Entities identify Critical Assets that impact the "Bulk Electric System" reliability and not make any ambiguous references such as "large quantities", "extended period of time", "detrimental impact", or "significant impact." NERC’s Glossary of Terms Used in Reliability Standards (Version 0 - Effective, April 1, 2005) has already defined the Bulk Electric System as being "defined by the Regional Reliability Organization, the electrical generation resources, transmission lines, interconnections with neighboring systems, and associated equipment generally operated at voltages of 100kV or higher. Radial transmission facilities serving only load with one transmission source are generally not included in this definition."

a. None of the definitions in the NERC Glossary use the words, "large quantities", "extended", "detrimental impact", or "significant impact." NERC standards and definitions should not be left open to interpretation.

b. The standards drafting team received 16 comments (out of 54 sets of

The definition has been modified to reflect industry consensus.

comments or 29.6%) to Draft 1 regarding the ambiguities of these words. In response, the drafting team stated on page 226 of 808 of the "Cyber Security Comments and Drafting Team Responses" that "Such phrases as "large quantities of customers" and "extended period of time" have been removed." In fact only the name has been changed, the definition remain exactly same as in Draft 1.

c. The standards drafting team received 16 comments (out of 63 sets of comments or 25.4%) in Draft 2 regarding the ambiguities of words such as "large quantities", "extended period of time", "detrimental impact", and "significant impact."

d. This definition will be added to the NERC Glossary upon approval, when that happens the definition can be utilized by and have impact on other NERC Standards, therefore this standard should be very specific.

3. The definition as written in this standard would allow for "scope creep." Scope creep results from a failure to establish clear definitions. It should not be the intent of this standard to impact Responsible Entities more than necessary. NERC Reliability Standards should only apply to the facilities of the bulk electric system. By including "cause signficant risk to public health and saftey, the definition now implies facilities all the way down to the distribution level. NERC reliability standards should only apply to the bulk electric system.

Proposed language would be:
Critical Asset: Those facilities, systems, and equipment, which if destroyed, degraded, or otherwise rendered unavailable, would affect the reliability of the bulk electric system.

Critical Cyber Asset

Cyber Asset

Cyber Security Incident

Electronic Security Perimeter

Physical Security Perimeter

Drafting Team Responses to Comments on Definitions

Commentor	Gary Campbell	
Organization	MAIN	
Agree	Yes	
Critical Asset		
Critical Cyber Asset		
Cyber Asset		
Cyber Security Incident		
Electronic Security Perimeter		
Physical Security Perimeter		
Additional	What is a discrete electronic perimeter?	Please see the FAQs.

Drafting Team Responses to Comments on Definitions

Commentor	Roger Champagne	
Organization	Hydro-Québec TransÉnergie	
Agree	No	
Critical Asset	These standard definition has not been approved by the industry. This draft opens these definitions to changes by the industry. change Critical Assets: Those facilities, systems, and equipment which, if destroyed, damaged, degraded, or otherwise rendered unavailable, would have a significant impact on the ability to serve large quantities of customers for an extended period of time, would have a detrimental impact on the reliability or operability of the Bulk Electric System, or would cause significant risk to public health and safety. to Critical Assets: Those facilities, systems, and equipment which, if destroyed, damaged, degraded, or otherwise rendered unavailable, would have a significant detrimental impact on the reliability or operability of the Bulk Electric System. Rational A detrimental impact is too subjective. We suggest "significant adverse impact", which is defined as << With due regard for the maximum operating capability of the affected systems, one or more of the following conditions arising from faults or disturbances, shall be deemed as having significant adverse impact: transient instability o -- Any instability that cannot be demonstrably contained to a well-defined small or radial portion of the system local area. unacceptable system dynamic response	The definition has been modified to reflect industry consensus.

	o -- An unacceptable system dynamic response is characterized by an oscillatory response to a contingency that is not demonstrated to be clearly positively damped within 30 seconds of the initiating event. unacceptable equipment tripping: Unacceptable equipment tripping is characterized by either one of the following: o -- Tripping of an un-faulted bulk power system element (element that has already been classified as bulk power system) of under planned system conditions due to operation of a protection system in response to a stable power swing o -- Operation of a Type I or Type II Special Protection System in response to a condition for which its operation is not required voltage levels in violation of applicable emergency limits loadings on transmission facilities in violation of applicable emergency limits >> The phrase public health and safety could include all hospitals. This may be outside the current BES definition. Entities may include or exclude such facilities, depending on their local need(s) or as part of their risk based assessment. Large quantities is a subjective term. Those words are beyond the scope of NERC's BES.	
Critical Cyber Asset		
Cyber Asset		
Cyber Security Incident		
Electronic Security Perimeter		
Physical Security Perimeter	Change The physical six-wall border surrounding computer rooms, telecommunications rooms, operations centers, and other locations in which Critical Cyber Assets are housed and for which access is controlled. to	The definition has been revised to " The physical, completely enclosed ("six-wall") border…" to reflect industry consensus. Technical feasibility is addressed in the requirements of the each standard as appropriate.

The physical six-wall border surrounding computer rooms,
telecommunications rooms, operations centers, and other locations in which Critical Cyber Assets are
housed, where pratical, and for which access is controlled.

Rational
With the introduction of IED, equipment are cyber asset by definition. So "six-wall" is something impossible for most of those equipment.

Drafting Team Responses to Comments on Definitions

Commentor	Larry Conrad	
Organization	Cinergy	
Agree	No	
Critical Asset	There are differences between how words are defined in the definition section and what is included in the scope of the term when that term is used within the standard. There should be consistency between the definition and the meaning of the word when used within the standard or the difference should be explained in the standard. For Critical Assets, if impacts on ability to serve large quantities of customers and significant risk to pulic health and safety are part of the definition but not included in the scope of the term when it is used in the standard, this should be made clear in the text of the standard.	The definitions are intentionally broad. They will be included in NERC's Glossary of Terms Used in Reliability Standards" for use in other standards. The requirements of each CIP standard qualify these definitions as appropriate.
Critical Cyber Asset	There should be consistency between the definition and the way the word is used within the standard or the difference should be explained in the standard. Definition section states that Critical Cyber Assets are those cyber assets essential to the reliable operation of Critical Assets. Section 002 states critical cyber assets use a routable protocol or are dial up accessible, but there is no reference in 002 as to whether the assets are essential. Either change the definition or modify the standard language so that the meaning of words are used consistently or differences are explained in the standard.	See responses above.
Cyber Asset	Cyber Asset definition section says: Those programmable electronic devices and communication networks including hardware, software, and data. Since communication networks are specifically excluded in CIP 002, the words "communication networks" should be removed from the definition or CIP 002 should be modified to explain the difference between the definition section and the scope of what is included when the words are used in CIP 002.	The definition is intentionally broad. CIP-002 qualifies the definition.
Cyber Security Incident		
Electronic Security Perimeter		
Physical Security Perimeter	The six wall border may be surrounding the asset, rather than surrounding the room in which the asset is kept. Modify the definition to: "The physical six-wall border surrounding computer rooms, telecommunications rooms, operations centers, and other locations or enclosures in which Critical Cyber Assets are housed and for which access is controlled."	The definition has been revised to reflect industry consensus.
Additional	Need definition of what constitutes a "reportable" incident	CIP-008 R1.1 further qualifies the definition of reportable incident.

Drafting Team Responses to Comments on Definitions

Commentor	Larry Conrad
Organization	ECAR Critical Infrastructure Protection Panel
Agree	Yes
Critical Asset	
Critical Cyber Asset	
Cyber Asset	
Cyber Security Incident	
Electronic Security Perimeter	
Physical Security Perimeter	

Drafting Team Responses to Comments on Definitions

Commentor	Theodore Creedon, P.E.
Organization	Creedon Engineering
Agree	Yes
Critical Asset	
Critical Cyber Asset	
Cyber Asset	
Cyber Security Incident	
Electronic Security Perimeter	
Physical Security Perimeter	

Drafting Team Responses to Comments on Definitions

Commentor	Joel De Granda
Organization	Florida Power and Light
Agree	No

Critical Asset

We believe the definition of Critical Asset must be modified. We will not support approval of this standard until modification is made.

“Critical Asset” in Draft 2 was previously identified as "Bulk Electric System Asset" in Draft 1. Areas of concern are:

1. The Drafting Team responded to the FRCC Comments on the definition of Critical Assets in Draft 2 by simply stating that this definition had been “approved by NERC’s Critical Infrastructure Protection Committee on September 16, 2004” as well as the Control Systems Security Working Group and the Risk Assessment Working Group.

a. If there was never an intention of revising this definition, why wasn’t this stated in the Draft Standard? Why ask for public comments on Draft comment form?

b. The point of an open process is for the industry to come to consensus. We would like to assume that any definition approved by a NERC committee would be open to change. The Draft Standard and its definitions are starting points for discussion by industry participants.

i. If comments received in Draft 1 and 2 showed a desire for a clearer definition, it should have been the Drafting Team’s task to take that definition back to the committee so further work.

ii. This definition has implications on many reliability standards, not just those regarding critical infrastucture protection. The CIPC is not the only group of individuals to provide input on this definition.

iii. Why was only the definition of “Critical Asset” unchangeable, while changes were allowed for “Cyber Assets,” Cyber Security Incident,” and “Electronic Security Perimeter?”

2. The definition should help Responsible Entities identify Critical Assets that impact the "Bulk Electric System" reliability and not make any ambiguous references such as "large quantities", "extended period of time", "detrimental impact", or "significant impact." NERC’s Glossary of Terms Used in Reliability Standards (Version 0 - Effective, April 1, 2005) has already defined the Bulk Electric System as being "defined by the Regional Reliability Organization, the electrical generation resources, transmission lines, interconnections with neighboring systems, and associated equipment generally operated at voltages of 100kV or higher. Radial transmission facilities serving only load with one transmission source are generally not included in this definition."

a. None of the definitions in the NERC Glossary use the words, "large quantities", "extended", "detrimental impact", or "significant impact." NERC standards and definitions should not be left open to interpretation.

b. The standards drafting team received 16 comments (out of 54 sets of

The definition has been revised to reflect industry consensus.

comments or 29.6%) to Draft 1 regarding the ambiguities of these words. In response, the drafting team stated on page 226 of 808 of the "Cyber Security Comments and Drafting Team Responses" that "Such phrases as "large quantities of customers" and "extended period of time" have been removed." In fact only the name has been changed, the definition remain exactly same as in Draft 1.

c. The standards drafting team received 16 comments (out of 63 sets of comments or 25.4%) in Draft 2 regarding the ambiguities of words such as "large quantities", "extended period of time", "detrimental impact", and "significant impact."

d. This definition will be added to the NERC Glossary upon approval, when that happens the definition can be utilized by and have impact on other NERC Standards, therefore this standard should be very specific.

3. The definition as written in this standard would allow for "scope creep." Scope creep results from a failure to establish clear definitions. It should not be the intent of this standard to impact Responsible Entities more than necessary. NERC Reliability Standards should only apply to the facilities of the bulk electric system. By including "cause signficant risk to public health and saftey, the definition now implies facilities all the way down to the distribution level. NERC reliability standards should only apply to the bulk electric system.

Proposed language would be:
Critical Asset: Those facilities, systems, and equipment, which if destroyed, degraded, or otherwise rendered unavailable, would affect the reliability of the bulk electric system.

Critical Cyber Asset

Cyber Asset

Cyber Security Incident

Electronic Security Perimeter

Physical Security Perimeter

Commentor	Richard Engelbrecht
Organization	RGE
Agree	No

Critical Asset

These standard definition has not been approved by the industry. This draft opens these definitions to changes by the industry.

change

Critical Assets: Those facilities, systems, and equipment which, if destroyed, damaged, degraded, or
otherwise rendered unavailable, would have a significant impact on the ability to serve large quantities of
customers for an extended period of time, would have a detrimental impact on the reliability or
operability of the Bulk Electric System, or would cause significant risk to public health and safety.

to

Critical Assets: Those facilities, systems, and equipment which, if destroyed, damaged, degraded, or
otherwise rendered unavailable, would have a significant detrimental impact on the reliability or
operability of the Bulk Electric System.

Rational

A detrimental impact is too subjective. We suggest "significant adverse impact", which is defined as
<<
With due regard for the maximum operating capability of the affected systems, one or more of the following conditions arising from faults or disturbances, shall be deemed as having significant adverse impact:

transient instability

o -- Any instability that cannot be demonstrably contained to a well-defined small or radial portion of the system local area.

unacceptable system dynamic response

The definition has been revised to reflect industry consensus.

o -- An unacceptable system dynamic response is characterized by an oscillatory response to a contingency that is not demonstrated to be clearly positively damped within 30 seconds of the initiating event.

unacceptable equipment tripping:

Unacceptable equipment tripping is characterized by either one of the following:

o -- Tripping of an un-faulted bulk power system element (element that has already been classified as bulk power system) of under planned system conditions due to operation of a protection system in response to a stable power swing

o -- Operation of a Type I or Type II Special Protection System in response to a condition for which its operation is not required

voltage levels in violation of applicable emergency limits

o -- loadings on transmission facilities in violation of applicable emergency limits
>>

The phrase public health and safety could include all hospitals. This may be outside the current BES definition. Entities may include or exclude such facilities, depending on their local need(s) or as part of their risk based assessment.

Large quantities is a subjective term. Those words are beyond the scope of NERC's BES.

Critical Cyber Asset

Cyber Asset

Cyber Security Incident

Electronic Security Perimeter

Physical Security Perimeter

Commentor Ken Fell

Organization New York ISO

Agree No

Critical Asset

These standard definition has not been approved by the industry. This draft opens these definitions to changes by the industry.

change

Critical Assets: Those facilities, systems, and equipment which, if destroyed, damaged, degraded, or
otherwise rendered unavailable, would have a significant impact on the ability to serve large quantities of
customers for an extended period of time, would have a detrimental impact on the reliability or
operability of the Bulk Electric System, or would cause significant risk to public health and safety.

to

Critical Assets: Those facilities, systems, and equipment which, if destroyed, damaged, degraded, or
otherwise rendered unavailable, would have a significant detrimental impact on the reliability or
operability of the Bulk Electric System.

Rational

A detrimental impact is too subjective. We suggest "significant adverse impact", which is defined as
<<
With due regard for the maximum operating capability of the affected systems, one or more of the following conditions arising from faults or disturbances, shall be deemed as having significant adverse impact:

transient instability

o -- Any instability that cannot be demonstrably contained to a well-defined small or radial portion of the system local area.

unacceptable system dynamic response

The definition has been revised to reflect industry consensus.

o -- An unacceptable system dynamic response is characterized by an oscillatory response to a contingency that is not demonstrated to be clearly positively damped within 30 seconds of the initiating event.

unacceptable equipment tripping:

Unacceptable equipment tripping is characterized by either one of the following:

o -- Tripping of an un-faulted bulk power system element (element that has already been classified as bulk power system) of under planned system conditions due to operation of a protection system in response to a stable power swing

o -- Operation of a Type I or Type II Special Protection System in response to a condition for which its operation is not required

voltage levels in violation of applicable emergency limits

o -- loadings on transmission facilities in violation of applicable emergency limits
>>

The phrase public health and safety could include all hospitals. This may be outside the current BES definition. Entities may include or exclude such facilities, depending on their local need(s) or as part of their risk based assessment.

Large quantities is a subjective term. Those words are beyond the scope of NERC's BES.

Critical Cyber Asset

Cyber Asset

Cyber Security Incident

Electronic Security Perimeter

Physical Security Perimeter

Commentor Francis Flynn

Organization National Grid USA

Agree No

Critical Asset

These standard definition has not been approved by the industry. This draft opens these definitions to changes by the industry.

change

Critical Assets: Those facilities, systems, and equipment which, if destroyed, damaged, degraded, or
otherwise rendered unavailable, would have a significant impact on the ability to serve large quantities of
customers for an extended period of time, would have a detrimental impact on the reliability or
operability of the Bulk Electric System, or would cause significant risk to public health and safety.

to

Critical Assets: Those facilities, systems, and equipment which, if destroyed, damaged, degraded, or
otherwise rendered unavailable, would have a significant adverse impact on the reliability or
operability of the Bulk Electric System.

Rational

A detrimental impact is too subjective. We suggest "significant adverse impact", which is defined as
<<
With due regard for the maximum operating capability of the affected systems, one or more of the following conditions arising from faults or disturbances, shall be deemed as having significant adverse impact:

transient instability

o -- Any instability that cannot be demonstrably contained to a well-defined small or radial portion of the system local area.

unacceptable system dynamic response

The definition has been revised to reflect industry consensus.

o -- An unacceptable system dynamic response is characterized by an oscillatory response to a contingency that is not demonstrated to be clearly positively damped within 30 seconds of the initiating event.

unacceptable equipment tripping:

Unacceptable equipment tripping is characterized by either one of the following:

o -- Tripping of an un-faulted bulk power system element (element that has already been classified as bulk power system) of under planned system conditions due to operation of a protection system in response to a stable power swing

o -- Operation of a Type I or Type II Special Protection System in response to a condition for which its operation is not required

voltage levels in violation of applicable emergency limits

o -- loadings on transmission facilities in violation of applicable emergency limits
>>

The phrase public health and safety could include all hospitals. This may be outside the current BES definition. Entities may include or exclude such facilities, depending on their local need(s) or as part of their risk based assessment.

Large quantities is a subjective term. Those words are beyond the scope of NERC's BES.

Critical Cyber Asset

Cyber Asset

Cyber Security Incident

Electronic Security Perimeter

Physical Security Perimeter

Drafting Team Responses to Comments on Definitions

Commentor	Greg Fraser	
Organization	Manitoba Hydro	
Agree	No	
Critical Asset		
Critical Cyber Asset		
Cyber Asset	Suggest removing the word "Those" making the definition "Programmable electronic devices and communication networks including hardware, software, and data."	Modified as suggested.
Cyber Security Incident		
Electronic Security Perimeter		
Physical Security Perimeter		

Commentor	Jerry Freese	
Organization	American Electric Power	
Agree	No	
Critical Asset		
Critical Cyber Asset		
Cyber Asset		
Cyber Security Incident		
Electronic Security Perimeter		
Physical Security Perimeter	Based on the expanded scope of what is deemed as Critical Assets and subsequent Critical Cyber Assets in this standard, there would be a significant requirement to have six-walled boundary or other mentioned security enclosures for the critical cyber assets within many substations, generation facilities and other locations. This is not feasible nor practical in many substation or plant environment.	CIP-002 has been modified.

Drafting Team Responses to Comments on Definitions

Commentor	Edwin C. Goff III
Organization	Progress Energy
Agree	Yes
Critical Asset	
Critical Cyber Asset	
Cyber Asset	
Cyber Security Incident	
Electronic Security Perimeter	
Physical Security Perimeter	

Drafting Team Responses to Comments on Definitions

Commentor	Kenneth Goldsmith	
Organization	Alliant Energy	
Agree	No	
Critical Asset		
Critical Cyber Asset		
Cyber Asset		
Cyber Security Incident	The definition of a Cyber Security Incident sould not include the phrases: "or was an attempt to compromise" or "or was an attempt to disrupt". The definition of Incident includes "attempts to compromise" and "attempts to disrupt". It appears all attempts to compromise or disupt are to be reproted to ES ISAC. This is impractical as stated. It must be made clear that an entity can use judgment in reporting some "attempts" that exceed a threshold of seriousness whilen not reporting all attempts to compromise. Hundreds of events per day could be considered "attempts", and it would not be practical or beneficial to report them all. The answer to FAQ #7 for CIP-008 appears to acknowledge this, butthe wording of hte definitions themselves need to be worked further to eliminate this concern.	The definitions are intentionally broad. CIP-008 addresses reportable cyber security incidents.
Electronic Security Perimeter		
Physical Security Perimeter		

Drafting Team Responses to Comments on Definitions

Commentor	Kathleen Goodman
Organization	ISO New England Inc
Agree	Yes
Critical Asset	
Critical Cyber Asset	
Cyber Asset	
Cyber Security Incident	
Electronic Security Perimeter	
Physical Security Perimeter	

Drafting Team Responses to Comments on Definitions

Commentor	Tim Hattaway	
Organization	Alabama Electric Cooperative	
Agree	No	
Critical Asset	Defining all Balckstart generators regardless of size as cricial assets is not practical. This requirement will impose significant overhead on smaller entities. Even though the Blackstart unit may be listed in the control area's system restoration plan that in itself should not make the unit a critical asset. The requirement should be worded as follows: If the entity's peak load is less than 1% of the Interconnections peak load then the entities blackstart unit(s) can be considered exempt.	CIP-002 has been modified.
Critical Cyber Asset		
Cyber Asset		
Cyber Security Incident		
Electronic Security Perimeter		
Physical Security Perimeter		

Drafting Team Responses to Comments on Definitions

Commentor	Jerry Heeren	
Organization	MEAG Power	
Agree	No	
Critical Asset	Some general guidelines about terms "significant impact","large quantities of customers", "extended period of time", and "significant risk to public health and safety" would be helpful. Although the use of broad language makes it possible for individual entities to do what "makes sense", it adds a great deal of confusion as to what might be considered to be in compliance. Also, we again strongly suggest that the term "Bulk Electric System" needs to be defined clearly. NERC has created confusion by allowing varying definitions to appear in different locations. For example, NERC's Cyber Security Standards FAQ says the Bulk Electric System is above 35kV or as approved in a tariff filed with FERC; NERC's TOP-003-0 Standard shows the Bulk Electric System as greater than 100kV; NERC staff has verbally mentioned that the Bulk Electric System includes those systems above 100kV; the NERC Glossary of Terms defines Bulk Electric System as "commonly applied to the portion of an electric utility system that encompasses the electrical generation resources and bulk transmission system;" and finally, NERC's Version 0 Glossary says the Regional Reliability Organization should define Bulk Electric System, with 100kV as a minimum. MEAG Power believes that the Bulk Electric System should be defined as those systems that operate above 200kV. In Georgia and most places, the 100 kV to 200kV systems are primarily local load serving. MEAG's suggested definition of Bulk Electric System follows: "Bulk Electric System – A term commonly applied to the portion of an electric utility system that encompasses the electrical generation resources and high-voltage transmission system (above 200kV)." If there is not widespread acceptance for MEAG's proposed definition, it would be best to define Bulk Electric System as determined by each utility based upon their specific system configuration.	The definition has been revised. These terms are no longer referenced. NERC's "Glossary of Terms Used in Reliability Standards" is the definitive source for the definition of Bulk Electric System. These standards have been revised to remove confusion
Critical Cyber Asset		
Cyber Asset		
Cyber Security Incident		
Electronic Security Perimeter	Some examples of electronic security perimeters and/or guidelines for determining the logical boundaries would be helpful. Would an electronic security perimeter be defined by devices located at the perimeter that regulate and/or monitor the data flow between the critical cyber asset and the outside world? In addition, the criteria for identifying a discrete Electronic Security Perimeter would help distinguish between exempt and non-exempt Perimeters.	Please see the FAQs for examples.

Physical Security Perimeter		
	In section A.4, it would be beneficial for NERC to provide examples of, and clarify the definition of "Cyber assets associated with communication networks" for the exemptions. Does a router with a single or multiple T1 connections to a telecom provider fall under this category?	Please see the FAQs for examples.

Drafting Team Responses to Comments on Definitions

Commentor	Peter Henderson	
Organization	Independent Electricity System Operator (IESO)	
Agree	No	
Critical Asset		
Critical Cyber Asset		
Cyber Asset		
Cyber Security Incident		
Electronic Security Perimeter		
Physical Security Perimeter		
Additional	We suggest that definitions should be revised and be consistent with NERC Glossary of Terms (under development and/or approved). This is necessary to avoid any confusion and/or inconsistency in definitions and for their uniform application to the Industry.	These standards have been revised to remove definitions already included in NERC's "Glossary of Terms Used in Reliability Standards."

Drafting Team Responses to Comments on Definitions

Commentor	E. Nick Henery
Organization	SMUD
Agree	Yes
Critical Asset	
Critical Cyber Asset	
Cyber Asset	
Cyber Security Incident	
Electronic Security Perimeter	
Physical Security Perimeter	

Drafting Team Responses to Comments on Definitions

Commentor	Jack Hobbick
Organization	Consumers Energy
Agree	Yes
Critical Asset	
Critical Cyber Asset	
Cyber Asset	
Cyber Security Incident	
Electronic Security Perimeter	
Physical Security Perimeter	

Drafting Team Responses to Comments on Definitions

Commentor	Richard Kafka	
Organization	Pepco Holdings, Inc.	
Agree	No	
Critical Asset		
Critical Cyber Asset		
Cyber Asset	The reference to "data" needs to be clarified. Does this data include data in transit, data in storage, business data, and/or backup data? Is only the data required by these Standards to be maintained? Should secure storage be part of definition? Please reference CIP-009-R4.	The term "data" is intentionally broad. The requirements of each CIP standard qualifies data as appropriate.
Cyber Security Incident		
Electronic Security Perimeter		
Physical Security Perimeter		
Additional	Add "electronic security control and monitoring" to definition list from CIP-005-1, R1.5.	CIP-005 has been revised and this term is no longer used.

Drafting Team Responses to Comments on Definitions

Commentor	Tony Kroskey
Organization	Brazos Electric Power Cooperative
Agree	Yes
Critical Asset	
Critical Cyber Asset	
Cyber Asset	
Cyber Security Incident	
Electronic Security Perimeter	
Physical Security Perimeter	

Drafting Team Responses to Comments on Definitions

Commentor	Carol Krysevig	
Organization	Allegheny Energy Supply Co. LLC	
Agree	No	
Critical Asset		
Critical Cyber Asset		
Cyber Asset		
Cyber Security Incident	Revise 'suspicious event' to 'suspicion of malicious act'.	Industry consensus does not support this change.
Electronic Security Perimeter		
Physical Security Perimeter		

Commentor	John Lim	
Organization	Con Edison	
Agree	No	
Critical Asset	These standard definition has not been approved by the industry. This draft opens these definitions to changes by the industry. change Critical Assets: Those facilities, systems, and equipment which, if destroyed, damaged, degraded, or otherwise rendered unavailable, would have a significant impact on the ability to serve large quantities of customers for an extended period of time, would have a detrimental impact on the reliability or operability of the Bulk Electric System, or would cause significant risk to public health and safety. to Critical Assets: Those facilities, systems, and equipment which, if destroyed, damaged, degraded, or otherwise rendered unavailable, would have a significant detrimental impact on the reliability or operability of the Bulk Electric System. The phrase public health and safety could include assets not related to the Bulk Electric System. This may be outside the current BES definition. Entities may include or exclude such facilities, depending on their local need(s) or as part of their risk based assessment. Large quantities is a subjective term. Those words are beyond the scope of NERC's BES.	This definition has been revised.
Critical Cyber Asset		
Cyber Asset		
Cyber Security Incident		
Electronic Security Perimeter		
Physical Security Perimeter		

Drafting Team Responses to Comments on Definitions

Commentor	Deborah Linke	
Organization	Bureau of Reclamation	
Agree	No	
Critical Asset	No, Reclamation does not agree with all the definitions. Reclamation feels that there are too many definition problems and too much room for interpretation. The NERC standards need to be reliability-, delivery-, production-based standards that establish metrics for critical assets before the standard is finalized. With those in place it would be more straight-forward to say that critical cyber assets are those that directly support and enable operation of the real critical assets (generators, transmission lines, substations, switchyards). As it stands in the proposal, every entity may well define critical assets on the basis of what keeps them in business, not on the basis of what is necessary to support the nationwide power grid. This will have the long-term impact of raising production costs.	CIP-002 has been revised. The list of required Assets has been removed.
Critical Cyber Asset	Reclamation believes that a standard that uses a risk management program to identify all Critical Cyber Assets is more defensible and sounder than one that is equipment-based. For example routable protocols are automatically deemed to be critical. One could argue, given the definition in Section R1.2, Additional Critical Assets, that all cyber assets are critical given the broad definition in that section. The requirement to include “telemetering” as a Critical Asset in R1.1.2 along with this requirement that any dial-up accessible Cyber Asset be designated as a Critical Cyber Asset could be interpreted to imply that all dial-up meters are Critical Cyber Assets. Dial-up meters are not capable of cascading access to other power control equipment and should not be included as Critical Cyber Assets. We suggest specific language be added to say that Critical Cyber Assets include only those assets where remote control access or cascading access to other Critical Cyber Assets can be gained through dial-up access. R1.1.6: We suggest clarifying "initial system restoration." Is it only those lines and generators involved in restoring the first 10% of the system or the first 50% of the system? R1.1.7: We also suggest clarifying the phrase “Under control of a common system.” When individual under-frequency load-shedding relays are all set to identical frequencies, does that qualify as “under control of a common system”? R1.2: The phrase "due to unique system configurations or other unique requirements" needs explanation.	CIP-002 has been revised. The list of required Assets has been removed.

Drafting Team Responses to Comments on Definitions

Cyber Asset	Our general comment is that the NERC Cyber Security Standard is appropriate for system control centers, but when it is applied to all the generation facilities, transmission lines and substations listed Under Section B.R1.1, Required Critical Assets, the list of "Critical Cyber Assets" gets very large very quickly. It also seems that use of the definition as written would result in the inclusion of a great amount of low-risk equipment.	CIP-002 has been revised. The list of required Assets has been removed.
Cyber Security Incident	Cyber Security Incident: The standard definition proposed is not entirely consistent with the definition from NERC's IAW SOP. The IAW SOP more clearly delineates events with malicious origin and we suggest that this definition be used.	Gauged by comments received, industry consensus does not appear to support using the IAW SOP definition. However, the definition proposed here does not conflict with the IAW SOP.
Electronic Security Perimeter	Electronic Security Perimeter: Considerable space in CIP-005, R1 is devoted to further defining the Electronic Security Perimeter; this indicates that the definition needs to be further refined to be clear on its own.	The definition is intentionally broad so it can be used in other Reliability Standards if necessary. CIP-005 further qualifies the definition.
Physical Security Perimeter		

Drafting Team Responses to Comments on Definitions

Commentor	Greg Mason
Organization	Dynegy Generation
Agree	Yes
Critical Asset	
Critical Cyber Asset	
Cyber Asset	
Cyber Security Incident	
Electronic Security Perimeter	
Physical Security Perimeter	

Drafting Team Responses to Comments on Definitions

Commentor	Paul McClay	
Organization	Tampa Electric	
Agree	No	
Critical Asset	Please refer to FRCC comments	Please see responses to Linda Campbell, FRCC.
Critical Cyber Asset		
Cyber Asset		
Cyber Security Incident		
Electronic Security Perimeter		
Physical Security Perimeter		

Drafting Team Responses to Comments on Definitions

Commentor	David McCoy	
Organization	Great Plains Energy/Kansas City Power & Light	
Agree	Yes	
Critical Asset		
Critical Cyber Asset		
Cyber Asset	The reference to "data" should be eliminated. There is no way to tell if data in storage, data in transit or what is to be proteced for "Critical Cyber Assets." If it is left in, compliance would force documentation changes every time any data is changed.	The term "data" used in this definition is intentionally broad. The requirements of each CIP standard qualify the data to be considered.
Cyber Security Incident		
Electronic Security Perimeter		
Physical Security Perimeter	Reference to the six-wall perimeter should be eliminated. Responsible entities should be able to decide whether to cage-off the floor and ceiling based on their own risk assessments without having six walls prescribed.	The definition has been revised to "The physical, completely enclosed (“six-wall”) border…." Technical feasibility is addressed in the requirements of CIP-006..

Drafting Team Responses to Comments on Definitions

Commentor	William McEvoy	
Organization	Northeast Utilities	
Agree	No	
Critical Asset	Please remove "or would cause significant risk to public health and safety".	The definition has been revised and no longer includes this phrase.
Critical Cyber Asset		
Cyber Asset		
Cyber Security Incident		
Electronic Security Perimeter		
Physical Security Perimeter		

Drafting Team Responses to Comments on Definitions

Commentor	Patrick Miller
Organization	PacifiCorp
Agree	Yes
Critical Asset	
Critical Cyber Asset	
Cyber Asset	
Cyber Security Incident	
Electronic Security Perimeter	
Physical Security Perimeter	

Commentor	Don Miller	
Organization	First Energy Corp	
Agree	No	
Critical Asset	Your definition of Critical Asset is as follows: Those facilities, systems, and equipment which, if destroyed, damaged, degraded, or otherwise rendered unavailable, would have a significant impact on the ability to serve large quantities of customers for an extended period of time, would have a detrimental impact on the reliability or operability of the bulk electric system, or would cause significant risk to public health and safety.	The definition has been revised.
Critical Cyber Asset		
Cyber Asset		
Cyber Security Incident		
Electronic Security Perimeter		
Physical Security Perimeter		
	These standards you are giving a somewhat generic definition of a critical asset (see above). In Standard CIP-002-1 you proceed to identify required critical assets in R1.1. Then, in R1.2 you are telling the responsible entity to identify additional critical assets utilizing a risk-based assessment. You go on further to describe the criteria for additional critical assets using basically the same definition (with some minor differences) as used for critical assets. This seems contradictory and confusing. Perhaps you should also provide a separate definition for Additional Critical Assets. We would suggest the following: Additional Critical Assets: Those assets, other than the required critical assets previously identified, which the responsibility entity has determined have unique system configurations, unique requirements, or other unique characteristics. The asset may be considered critical if its destruction, incapacitation, or compromise would have a serious or an adverse effect on the company, the company's operation, or the company's image. You then go on to require a description of the risk-based assessment and the determining criteria that was utilized to identify these additional critical assets. The risk-based assessment tools, that we are aware of, are primarily used for the purpose of assessing risk, such as the level of risk, how much at risk or the level of vulnerability -- not for identifying critical assets. Therefore, we would suggest that here you eliminate the use of the term risk-based assessment and replace it with "critical asset identification methodology" or "basis for additional critical asset identification", or "appropriate assessment methodology applied to a particular entity's circumstances".	CIP-002 has been revised and no longer includes a list of Required Assets.

Drafting Team Responses to Comments on Definitions

Commentor	Jeff Mitchell
Organization	ECAR
Agree	Yes
Critical Asset	N/A
Critical Cyber Asset	
Cyber Asset	
Cyber Security Incident	
Electronic Security Perimeter	
Physical Security Perimeter	

Commentor	Scott Mix	
Organization	KEMA, Inc	
Agree	Yes	
Critical Asset		
Critical Cyber Asset		
Cyber Asset	The removal of the phrase "associated with Bulk Electric System assets" from the definition in Draft 3 has caused confusion in the industry, and has expanded the scope of standard beyond that which the drafting team has expected. The discussion that the scope is constrained to only Bulk Electric System assets is not supported by the Draft 3 wording that includes not only Bulk Electric System assets, but also those that "would have a significant impact on the ability to serve large quantities of customers for an extended period of time", or, "would cause a significant risk to public health and safety". Furthermore, the language in standard CIP-002 restricting the standard to "functions and tasks affecting the interconnected Bulk Electric System" only applies to requirement R1.2, Additional Critical Assets. Thus, for example, ALL control centers of applicable entities, including those of primarily Distribution utilities that are also Generator Owners and Load Serving Entities, that would otherwise not be subject to the NERC standards now are.	The definition is intentionally broad. CIP-002 further qualifies the definition.
Cyber Security Incident		
Electronic Security Perimeter		
Physical Security Perimeter		

Drafting Team Responses to Comments on Definitions

Commentor	Darrick Moe	
Organization	WAPA	
Agree	No	
Critical Asset		
Critical Cyber Asset		
Cyber Asset		
Cyber Security Incident	The definition of a Cyber Security Incident should be modified to make it clear that the phrases: “or was an attempt to compromise” and “or was an attempt to disrupt” only qualify as Incidents if they are in tandem with a malicious act or suspicious event. Above some threshold of seriousness, an entity should report “attempts”.	Use of the colon in the definition clearly links attempts to malicious acts or suspicious events. CIP-008 address reportable incidents.
Electronic Security Perimeter		
Physical Security Perimeter		

Drafting Team Responses to Comments on Definitions

Commentor	Selby Mohr
Organization	Sacramento Municipal Utility District
Agree	Yes
Critical Asset	
Critical Cyber Asset	
Cyber Asset	
Cyber Security Incident	
Electronic Security Perimeter	
Physical Security Perimeter	

Drafting Team Responses to Comments on Definitions

Commentor	Selby Mohr	
Organization	Sacramento Municipal Utility District	
Agree	Yes	
Critical Asset	CIP-002-1 R1.1.6. NERC’s proposal for classifying generating resources and transmission paths as Critical Assets appears to rely upon the whether a given generator or transmission path has a significant impact on the reliability of the whole interconnection of the Regional Reliability Organization. It is not clear if this same logic applies to classification of black start generators. For instance, a Balancing Authority/Load Serving entity may have black start generators for restoration of its own system, in the event of separation from the rest of the interconnection. If those black start generators are not relied upon by the Regional Reliability Organization for restoration of the interconnection as a whole, is it NERC’s intention that these types of black start generators be deemed as Critical Assets? CIP-002-1 R1.2. For the requirement on identifying Additional Critical Assets, is the emphasis on identifying only those systems that could have an impact on the whole interconnection of the Regional Reliability Organization? If a Balancing Authority/Load Serving entity had system components that would not affect the reliability of the whole interconnection but which could impact load serving capability of the Load Serving Entity can those assets be excluded from the Critical classification?	CIP-002 has been revised and no longer references Required Assets.
Critical Cyber Asset		
Cyber Asset		
Cyber Security Incident		
Electronic Security Perimeter		
Physical Security Perimeter		

Drafting Team Responses to Comments on Definitions

Commentor	Kurt Muehlbauer	
Organization	Exelon	
Agree	No	
Critical Asset		
Critical Cyber Asset		
Cyber Asset	Recommend excluding voice communication e.g. phones and radios over public networks.	The definition is intentionally broad. Each standard excludes Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters (See Section A.4.2.2 of each standard.)
Cyber Security Incident		
Electronic Security Perimeter		
Physical Security Perimeter		

Drafting Team Responses to Comments on Definitions

Commentor	Jeffrey Mueller	
Organization	PSEG Companies	
Agree	No	
Critical Asset		
Critical Cyber Asset		
Cyber Asset		
Cyber Security Incident		
Electronic Security Perimeter		
Physical Security Perimeter		
Additional	The PSEG Companies have reviewed and share the concerns expressed in the Comments of PJM and EEI. Accordingly, the PSEG Companies support the comments of PJM and EEI, and request that the concerns expressed in those comments be properly addressed in the next version of the draft standard.	Please see response to Laurence W. Brown, Edison Electric Institute.

Drafting Team Responses to Comments on Definitions

Commentor	Mitchell Needham
Organization	Tennessee Valley Authority
Agree	Yes
Critical Asset	
Critical Cyber Asset	
Cyber Asset	
Cyber Security Incident	
Electronic Security Perimeter	
Physical Security Perimeter	

Drafting Team Responses to Comments on Definitions

Commentor	Dave Norton	
Organization	Entergy Transmission	
Agree	No	
Critical Asset	Just a question: Is "personnel" a critical asset? It can be so deduced as the definition is written. Just an observation - does it matter?	The definition is limited to facilities, systems, and equipment.
Critical Cyber Asset		
Cyber Asset		
Cyber Security Incident		
Electronic Security Perimeter		
Physical Security Perimeter	The end of the definition now says: "...for which access is controlled." Consider: "...for which access control is required."	Gauging by comments received, the definition is clear as stated.

Drafting Team Responses to Comments on Definitions

Commentor	Doug Orlofske
Organization	Wisconsin Public Power Inc
Agree	Yes
Critical Asset	
Critical Cyber Asset	
Cyber Asset	
Cyber Security Incident	
Electronic Security Perimeter	
Physical Security Perimeter	

Drafting Team Responses to Comments on Definitions

Commentor	Kevin Perry	
Organization	Southwest Power Pool	
Agree	No	
Critical Asset	The terms "significant impact", "Large Quantities", "Significant Risk", and "Extended Period of Time" are vague and need to be better quantified. Would not a large, mostly rural area (such as about half of Arkansas) qualify for consideration, even though it does not have "large quantities" of customers? Would not an asset serving a critical US Government installation, such as the Army Ammunition Plant outside of Texarkana, Texas or the chemical weapons incinerator outside of Pine Bluff, Arkansas also qualify as a selection criteria even though it is not a large quantity of customers and does not directly contribute to the public health and safety?	The definition has been revised and longer references these terms.
Critical Cyber Asset		
Cyber Asset		
Cyber Security Incident		
Electronic Security Perimeter		
Physical Security Perimeter	The definition would be improved by defining the walls to be "concrete-to-concrete". There are sites today where door access is controlled by a card reader but someone can go "up-and-over" through the false ceiling.	The definition has been revised to "The physical, completely enclosed (“six-wall”) border…."

Drafting Team Responses to Comments on Definitions

Commentor	Tom Pruitt	
Organization	Duke Power Company	
Agree	No	
Critical Asset	This definition appears to include language the FAQ (See FAQ question #8 for CIP 002) indicates is excluded. Please explain this.	The definitions are intentionally broad for possible use in other Reliability Standards. The requirements of CIP-002 further qualify the definitions to limit the scope of applicable assets and reduce the implementation burden on Responsible Entities.
Critical Cyber Asset		
Cyber Asset	Inclusion of "communications networks" in this standard appears to be contradictory to Applicability section 3.2.2 of CIP-002 and sections 4.2.2 of CIPs 003-009, the Introduction document, and FAQ question #14 for CIP 002.	Communication networks are cyber assets; they are excluded by individual standard, not by definition. See Section A.4.2.2 of each standard CIP-002 through CIP-009.
Cyber Security Incident		
Electronic Security Perimeter		
Physical Security Perimeter	Replace six wall border with the word "enclosure." Some physical security perimeters could be fences or other non-roofed structures.	The definition has been revised to "The physical, completely enclosed ("six-wall") border…."

Drafting Team Responses to Comments on Definitions

Commentor	Duane Radzwion	
Organization	Consumers Energy	
Agree	No	
Critical Asset		
Critical Cyber Asset	The term is to vague. Section B, R2 and R2.1 do little to provide clarification, especially with regard to routable protocol. (See section R2.1 comments)	The definition is intentionally broad. Cip-002 further qualifies the definition to limit the scope of assets that fall under the requirements of the CIP standards.
Cyber Asset		
Cyber Security Incident		
Electronic Security Perimeter		
Physical Security Perimeter		

Drafting Team Responses to Comments on Definitions

Commentor	Howard Rulf
Organization	We Energies
Agree	Yes
Critical Asset	
Critical Cyber Asset	
Cyber Asset	
Cyber Security Incident	
Electronic Security Perimeter	
Physical Security Perimeter	

Drafting Team Responses to Comments on Definitions

Commentor	Howard Rulf
Organization	We Energies
Agree	Yes
Critical Asset	
Critical Cyber Asset	
Cyber Asset	
Cyber Security Incident	
Electronic Security Perimeter	
Physical Security Perimeter	

Drafting Team Responses to Comments on Definitions

Commentor	Randy Schimka
Organization	San Diego Gas and Electric Co.
Agree	Yes
Critical Asset	
Critical Cyber Asset	
Cyber Asset	
Cyber Security Incident	
Electronic Security Perimeter	
Physical Security Perimeter	

Drafting Team Responses to Comments on Definitions

Commentor	Lyman Shaffer
Organization	PG&E
Agree	Yes
Critical Asset	
Critical Cyber Asset	
Cyber Asset	
Cyber Security Incident	
Electronic Security Perimeter	
Physical Security Perimeter	

Drafting Team Responses to Comments on Definitions

Commentor	Neil Shockey
Organization	Southern California Edison
Agree	Yes
Critical Asset	
Critical Cyber Asset	
Cyber Asset	
Cyber Security Incident	
Electronic Security Perimeter	
Physical Security Perimeter	

Drafting Team Responses to Comments on Definitions

Commentor	William Smith
Organization	Allegheny Power
Agree	Yes
Critical Asset	
Critical Cyber Asset	
Cyber Asset	
Cyber Security Incident	
Electronic Security Perimeter	
Physical Security Perimeter	

Drafting Team Responses to Comments on Definitions

Commentor	Paul Sorenson
Organization	Open Access Technology International
Agree	Yes
Critical Asset	
Critical Cyber Asset	
Cyber Asset	
Cyber Security Incident	
Electronic Security Perimeter	
Physical Security Perimeter	

Commentor	Robert Strauss	
Organization	NYSEG	
Agree	No	
Critical Asset	These standard definition has not been approved by the industry. This draft opens these definitions to changes by the industry. change Critical Assets: Those facilities, systems, and equipment which, if destroyed, damaged, degraded, or otherwise rendered unavailable, would have a significant impact on the ability to serve large quantities of customers for an extended period of time, would have a detrimental impact on the reliability or operability of the Bulk Electric System, or would cause significant risk to public health and safety. to Critical Assets: Those facilities, systems, and equipment which, if destroyed, damaged, degraded, or otherwise rendered unavailable, would have a significant detrimental impact on the reliability or operability of the Bulk Electric System. Rational: A detrimental impact is too subjective. We suggest "significant adverse impact", which is defined as << With due regard for the maximum operating capability of the affected systems, one or more of the following conditions arising from faults or disturbances, shall be deemed as having significant adverse impact: transient instability o -- Any instability that cannot be demonstrably contained to a well-defined small or radial portion of the system local area. unacceptable system dynamic response o -- An unacceptable system dynamic response is characterized by an oscillatory response to a contingency that is not demonstrated to be clearly positively damped within 30 seconds of the initiating event. unacceptable equipment tripping:	The definition has been revised.

Unacceptable equipment tripping is characterized by either one of the following:

o -- Tripping of an un-faulted bulk power system element (element that has already been classified as bulk power system) of under planned system conditions due to operation of a protection system in response to a stable power swing

o -- Operation of a Type I or Type II Special Protection System in response to a condition for which its operation is not required

voltage levels in violation of applicable emergency limits

o -- loadings on transmission facilities in violation of applicable emergency limits
>>

The phrase public health and safety could include all hospitals. This may be outside the current BES definition. Entities may include or exclude such facilities, depending on their local need(s) or as part of their risk based assessment.

Large quantities is a subjective term. Those words are beyond the scope of NERC's BES

Critical Cyber Asset

Cyber Asset

Cyber Security Incident

Electronic Security Perimeter

Physical Security Perimeter

Drafting Team Responses to Comments on Definitions

Commentor	Ed Stuart
Organization	City of Austin, Austin Energy
Agree	Yes
Critical Asset	
Critical Cyber Asset	
Cyber Asset	
Cyber Security Incident	
Electronic Security Perimeter	
Physical Security Perimeter	

Drafting Team Responses to Comments on Definitions

Commentor	Karl Tammar
Organization	IRC
Agree	No
Critical Asset	
Critical Cyber Asset	
Cyber Asset	
Cyber Security Incident	
Electronic Security Perimeter	
Physical Security Perimeter	

Drafting Team Responses to Comments on Definitions

Commentor	Todd Thompson
Organization	PJM Interconnection
Agree	Yes
Critical Asset	
Critical Cyber Asset	
Cyber Asset	
Cyber Security Incident	
Electronic Security Perimeter	
Physical Security Perimeter	

Drafting Team Responses to Comments on Definitions

Commentor	Steven Townsend
Organization	Consumers Energy Co.
Agree	Yes
Critical Asset	
Critical Cyber Asset	
Cyber Asset	
Cyber Security Incident	
Electronic Security Perimeter	
Physical Security Perimeter	

Commentor	Martin Trence	
Organization	Xcel Energy - Northen States Power (NSP)	
Agree	No	
Critical Asset		
Critical Cyber Asset		
Cyber Asset	For purposes of a NERC Standard, the term Cyber Assets should be limited to those programmable electronic devices and communications networks, including hardware, software, and data necessary for operation of the Bulk Electric System. Please revise definition accordingly. Definition in present form too broad.	The definition is intentionally broad for possible use in other Reliability Standards. CIP-002 further qualifies the definition.
Cyber Security Incident		
Electronic Security Perimeter		
Physical Security Perimeter		

Drafting Team Responses to Comments on Definitions

Commentor	Rick Vermeers
Organization	Avistacorp
Agree	Yes
Critical Asset	
Critical Cyber Asset	
Cyber Asset	
Cyber Security Incident	
Electronic Security Perimeter	
Physical Security Perimeter	

Drafting Team Responses to Comments on Definitions

Commentor	Robert C. Webb	
Organization	Instrumentation, Systems and Automation Society	
Agree	No	
Critical Asset		
Critical Cyber Asset		
Cyber Asset		
Cyber Security Incident	This should also include unintentional cyber events.	The definition has been restricted to malicious acts or suspicious events to reflect industry consensus.
Electronic Security Perimeter	It is not clear whether the phrase "…and for which access is controlled" is intended as a requirement for the Electronic Security Perimeter's network, or is intended to exclude those networks or parts thereof which do not have access control. Regardless, the networks associated with the Critical Cyber Assets should be included, and thus the last phrase should be dropped. The requirement is adequately defined in CIP-005-1.	It is intended to be limiting.
Physical Security Perimeter	It is not clear whether the phrase "…and for which access is controlled" is intended as a requirement for the Physical Security Perimeter's network, or is intended to exclude those networks or parts thereof which do not have access control. Regardless, the physical location associated with the Critical Cyber Assets should be included, and thus the last phrase should be dropped. The requirement is adequately defined in CIP-006-1.	It is intended to be limiting.

Drafting Team Responses to Comments on Definitions

Commentor	Laurent Webber	
Organization	Western Area Power Administration	
Agree	No	
Critical Asset		
Critical Cyber Asset		
Cyber Asset	Clarify contradictory information as to communication; is it included or not? This definition specifically includes "communication networks", but the introduction of each CIP specifically exempts "communication networks."	Communication networks are cyber assets; they are excluded by individual standard, not by definition. See Section A.4.2.2 of each standard CIP-002 through CIP-009.
Cyber Security Incident	The drafting team defines cyber security incident here, but in CIP-008 R1 the team requires that each entity use the definition from NERC's IAW SOP. The IAW SOP more clearly delineates events with malicious origin. Instead of "Compromises, or was an attempt to compromise", the definition should read "Compromises, or was an attempt to compromise with malicious intent" and "Disrupts or was an attempt to disrupt with malicious intent".	CIP-008 has been revised; reference to the IAW SOP have been removed. The definition pertains to malicious acts and suspicious events.
Electronic Security Perimeter	Considerable space in CIP-005, R1 is devoted to further defining the Electronic Security Perimeter; this indicates that the term is ill-defined and poorly understood. Clarify what the logical border is.	The definition is intentionally broad. CIP-005 further qualifies the definition.
Physical Security Perimeter		

Drafting Team Responses to Comments on Definitions

Commentor	Michal Zeithammel	
Organization	Brascan Power	
Agree	Yes	
Critical Asset		
Critical Cyber Asset		
Cyber Asset	Obviously modems, routers, computers be included in "hardware". Brascan Power recommends that cables (e.g., 10BaseT, Fiber Optic) be specifically excluded from hardware and therefore cyber assets.	The definition is intentionally broad. The requirements of individual CIP standards further qualify the definition as appropriate.
Cyber Security Incident		
Electronic Security Perimeter		
Physical Security Perimeter		

Commentor Guy Zito

Organization NPCC

Agree No

Critical Asset

These standard definition has not been approved by the industry. This draft opens these definitions to changes by the industry.

change

Critical Assets: Those facilities, systems, and equipment which, if destroyed, damaged, degraded, or
otherwise rendered unavailable, would have a significant impact on the ability to serve large quantities of
customers for an extended period of time, would have a detrimental impact on the reliability or
operability of the Bulk Electric System, or would cause significant risk to public health and safety.

to

Critical Assets: Those facilities, systems, and equipment which, if destroyed, damaged, degraded, or
otherwise rendered unavailable, would have a significant detrimental impact on the reliability or
operability of the Bulk Electric System.

Rational

A detrimental impact is too subjective. We suggest "significant adverse impact", which is defined as
<<
With due regard for the maximum operating capability of the affected systems, one or more of the following conditions arising from faults or disturbances, shall be deemed as having significant adverse impact:

transient instability

o -- Any instability that cannot be demonstrably contained to a well-defined small or radial portion of the system local area.

unacceptable system dynamic response

o -- An unacceptable system dynamic response is characterized by an oscillatory

The definition has been revised.

response to a contingency that is not demonstrated to be clearly positively damped within 30 seconds of the initiating event.

unacceptable equipment tripping:

Unacceptable equipment tripping is characterized by either one of the following:

o -- Tripping of an un-faulted bulk power system element (element that has already been classified as bulk power system) of under planned system conditions due to operation of a protection system in response to a stable power swing

o -- Operation of a Type I or Type II Special Protection System in response to a condition for which its operation is not required

voltage levels in violation of applicable emergency limits

o -- loadings on transmission facilities in violation of applicable emergency limits
>>

The phrase public health and safety could include all hospitals. This may be outside the current BES definition. Entities may include or exclude such facilities, depending on their local need(s) or as part of their risk based assessment.

Large quantities is a subjective term. Those words are beyond the scope of NERC's BES.

Critical Cyber Asset

Cyber Asset

Cyber Security Incident

Electronic Security Perimeter

Physical Security Perimeter

CIP-002 Drafting Team Responses to Comments

Name	Raymond A'Brial
Entity	Central Hudson Gas & Electric Corp
Ready to Ballot:	No

General Comments

002-R1

R1.1 -- As worded, the list of "required" facilities appears far too rigid -- more strict even than the cybersecurity guidelines created by the nuclear industry to respond to federal requirements. Such a list must permit some reasonable flexibility in light of the vast differences among Responsible Entities in size and function. In particular, covering every "modification" would cover minor matters such as replacing bearings and setting relays. Also, one of the key elements to this Standard is performing a risk assessment to determine whether there are any critical cyber assetss, yet that process and concept is not articulated except as concerning "additional" assets.

Suggested Alternative Wording:
Modify the existing last sentence so that it ends with the phrase -
"... the addition><, removal><, or >reasonably substantive< modification of any Critical Asset."

Also, move and append the text from R1.2 (with minor changes) so that the paragraph ends with-
"... The Responsible Entity shall utilize a risk-based assessment to identify any >< Critical Assets><. The risk-based assessment must include a description of the assessment>,< including the determining criteria, potential impacts, evaluation procedure and results. For the purpose of this standard, >< Critical Assets consists of those facilities, systems, and equipment >that<, if destroyed, damaged, degraded, or otherwise rendered unavailable, would have a detrimental impact on the reliability, or operability, of the electric grid and critical operating functions and tasks affecting the interconnected Bulk Electric System."

R1.1.3 -- IROL is dynamic, and can change on a daily basis, thus what is already a very broad requirement becomes unnecessarily burdensome.

Suggested Alternative Wording:
"R1.2.2. Transmission substation elements in the >critical,< direct transfer path>s< >reasonably< associated with an Interconnection Reliability Operating Limit (IROL)."

R1.1.4 -- Indicative of the unintended breadth of the current language is, for instance, "under control of a common plant control system". This could not reasonably be meant to include such add-on systems as environmental controls.

Suggested Alternative Wording:

The Drafting Team has removed the list of "Required Critical Assets, " in favor of requiring the Responsible Entity to use a risk-based assessment to identify its Critical Assets. The Drafting Team does provide a list of assets that the Responsible Entity must consider as part of its risk assessment (see R1.2). This list includes some, not all, of the same assets previously referred to as "Required" but most have been reworded to add clarity. For example, the list of assets to be considered in a risk assessment does not include IROL or generating resources under control of a common plant control system that meet the criteria of 80% or greater of the largest single contingency within the Regional Reliability Organization. It does include blackstart generators and substations in the electrical path of transmission lines used for initial system restoration. An FAQ on blackstart has been drafted in response to comments requesting clarification.

"Generating resources>,< under >the reasonably direct< control of a common >< system>,< that meet the criteria of 80% or greater of the largest single contingency within the Regional Reliability Organization."

R1.1.6 -- Also indicating overbreadth, some "black start" facilities are simply not as important as others, and almost any facility could potentially be involved in a path related to some black-start scenario. It is unreasonable to expect entities to protect every facility to the same degree, yet the wording appears to indicate such an intent.

Suggested Alternative Wording:
"Systems, equipment and facilities >reasonably< critical to system restoration, including >critical< blackstart generators and substations in >< electrical path>s< of >critical< transmission lines used for initial system restoration."

R1.1.8 -- To reflect the suggested change to R1.1.3, above, and for the same reasons --

Suggested Alternative Wording:
"R1.1.8. Special Protection Systems whose misoperation can negatively affect elements >reasonably< associated with an IROL."

R1.2 -- Consistent with the comment above regarding R1 (the opening paragraph), the reference to assessments need to be elevated to cover all assets, rather than just "additional" assets. It is, however, appropriate to mention as clarification that the discovery of additional assets through a reasonable assessment is to be expected.

Suggested Alternative Wording:
"R1.2. Additional Critical Assets: >A reasonable risk-based assessment may identify additional critical assets.<"

OVERALL R.1 -- The current list of "required" facilities should be further clarified and made more realistic by reducing it, redesignating the "removed" facilities as assets that simply must be considered in any reasonable risk-based assessment.

Suggested Alternative Wording:
Combined with all of the other suggestions above, the new R1 would read as follows -
"R1. Critical Assets -- The Responsible Entity shall identify its Critical Assets and maintain a current list of all Critical Assets identified. The Responsible Entity shall review, and as necessary, update the list of Critical Assets annually, or within ninety calendar days of the addition, removal, or reasonably substantive modification of any Critical Asset. The Responsible Entity shall utilize a risk-based assessment to identify any Critical Assets. The risk-based assessment must include a description of the assessment including the determining criteria, potential impacts, evaluation procedure and results. For the purpose of this standard, Critical Assets consists of those facilities, systems, and equipment that, if destroyed, damaged, degraded, or otherwise rendered unavailable, would have a detrimental impact on the

	reliability, or operability, of the electric grid and critical operating functions and tasks affecting the interconnected Bulk Electric System. "R1.1. Required Critical Assets "R1.1.1. Control centers and backup control centers performing the functions listed in the Applicability section of this standard. "R1.1.2. Generating resources, under the reasonably direct control of a common system, that meet the criteria of 80% or greater of the largest single contingency within the Regional Reliability Organization. "R1.1.3. Generation control centers having control of generating resources that when summed meet the criteria of 80% or greater of the largest single contingency within the Regional Reliability Organization. "R1.2. Assets That Must be Assessed "R1.2.1. Systems, equipment and facilities critical to operating functions and tasks supporting control centers and backup control centers. These shall include telemetering, monitoring and control, automatic generation control, realtime power system modeling and real-time inter-utility data exchange. "R1.2.2. Transmission substation elements in the critical, direct transfer paths reasonably associated with an Interconnection Reliability Operating Limit (IROL). "R1.2.3. Systems, equipment and facilities reasonably critical to system restoration, including critical blackstart generators and substations in electrical paths of critical transmission lines used for initial system restoration. "R1.2.4. Systems, equipment and facilities critical to automatic load shedding under control of a common system capable of shedding 300 MW or more. "R1.2.5. Special Protection Systems whose misoperation can negatively affect elements reasonably associated with an IROL.	
002-R2	R2 -- First, this has the same problem with "modification" as does R1, as noted additional critical assets." Suggested Alternative Wording: The operative phrase should read, as above: "... the addition><, removal><, or >reasonably substantive< modification of ..."	The requirement to identify Critical Cyber Assets has been renumbered to above.R3. The review and update period has been to changed "review this list [of Critical Cyber Assets] at least annually, and update as necessary."
	Second, the closing phrase "have the following characteristics" is unclear. Does it operate exclusively or inclusively? In other words, should the phrase be clarified to read either "have >only< the following characteristics" or "have >at least< the following characteristics"?	The closing phrase has been modified to read "For the purpose of this standard, Critical Cyber Assets have at least one of the following characteristics:"
	R2.1 excepts generating station routable cyber assets from those that are critical "where a routable protocol does not extend beyond the physical boundary," yet the "Highlights" refers instead to the "electronic security perimeter." It is presumed that the Standard refers to the intended perimeter, but that is no longer certain. However, even if the Standard refers to the intended perimeter, it is unclear. For instance, the phrase "physical boundary" is undefined and could refer to walls or fences or property lines.	The characteristics have been clarified as using a routable protocol to communicate outside the Electronic Security Perimeter, or using a routable protocol within a Control Center. Therefore, a Cyber Asset using a routable protocol strictly within a generating station or substation does not have to be considered a Critical Cyber Asset. If the routable protocol crosses the boundary of the Electronic Security Perimeter, the Cyber Asset would be considered critical.
	Suggested Alternative Wording:	

	"R2.1. The Cyber Asset uses a routable protocol, unless the Cyber Asset is >located at< a substation or generation station >and its use of< a routable protocol does not extend >through or< beyond >any electronic or< physical >security perimeter associated with< the facility; or," R.2.2 -- If the phrase "have the following characteristics" is meant to be exclusive ("only"), then R2.2 appears to exclude "phone-home" modems. They may need to be covered, as they could be reset to answer-mode, or the answering phone might be subject to forwarding.	
002-R3	R3.3.2 -- Are SONET nodes exempted? They (as well as other communication equipment) could be used to shut down a data communication network via a denial-of-service attack. Even though they do not use routable protocol, they can be accessed via routable protocol.	Per Section 4 Applicability 4.2.2, the following are exempt from the standard: "Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters." Unless the Sonet nodes are within the Electronic Security Perimeter, they are outside the scope of the standard.
	What is the impact of Power Line Carrier (PLC) or Broadband over Power Line (BPL) technology on the electronic security perimeter? Is that simply a factor to be considered in a Responsible Entity's assessment? If so, what assessment criteria are available or should be used?	The technology used to transmit the routable protocol is outside the scope; the Electronic Security Perimter must be protected regardless of the communications methods. Please see CIP-005 for more information.
002-M1		
002-M2	There is no approved list of Critical Cyber Assets in R2. Remove the word "approved."	The measures has been rewritten. The word "approved" has been removed as suggested.
002-M3		
002-C1,1		
002-C1,2		
002-C1,3		
002-C1,4		
002-C2,1		
002-C2,2		
002-C2,3		
002-C2,4		

CIP-002 Drafting Team Responses to Comments

Name	Ori Artman
Entity	Teltone
Ready to Ballot:	Yes
General Comments	
002-R1	
002-R2	
002-R3	
002-M1	
002-M2	
002-M3	
002-C1,1	
002-C1,2	
002-C1,3	
002-C1,4	
002-C2,1	
002-C2,2	
002-C2,3	
002-C2,4	

CIP-002 Drafting Team Responses to Comments

Name	Steve Badgett
Entity	Riverside Public Utilitities
Ready to Ballot:	Yes

General Comments

002-R1

002-R2

002-R3

002-M1

002-M2

002-M3

002-C1,1

002-C1,2

002-C1,3

002-C1,4

002-C2,1

002-C2,2

002-C2,3

002-C2,4

CIP-002 Drafting Team Responses to Comments

Name	Terry Baker
Entity	Platte River Power Authority
Ready to Ballot:	Yes
General Comments	
002-R1	
002-R2	
002-R3	
002-M1	
002-M2	
002-M3	
002-C1,1	
002-C1,2	
002-C1,3	
002-C1,4	
002-C2,1	
002-C2,2	
002-C2,3	
002-C2,4	

CIP-002 Drafting Team Responses to Comments

Name	Terry Bilke
Entity	Midwest ISO
Ready to Ballot:	No
General Comments	
002-R1	
002-R2	
002-R3	
002-M1	
002-M2	
002-M3	
002-C1,1	
002-C1,2	
002-C1,3	
002-C1,4	
002-C2,1	
002-C2,2	
002-C2,3	
002-C2,4	

CIP-002 Drafting Team Responses to Comments

Name	Pat Bourassa	
Entity	Wisconsin Public Service Corporation	
Ready to Ballot:	No	
General Comments	Although there are critical assets to be protected, the focus of the CIP-002 is on methodology and documentation of systems rather than the actual protection of identified critical assets.	CIP-002 puts forth requirements for identifying and documenting Critical Assets and their associated Critical Cyber Assets. The requirements for protecting and securing the Critical Cyber Assets on the documented and approved list are defined in CIP-003 through CIP-009.
	There should be a standard methodology created to identify and document critical assets. This would unburden the asset owner from developing unique methodologies for identification and impose consistancy across organizations that are required to comply. Is having a corporate "risk management policy" for the CIP standards part of the risk-based assessment requirements? (This policy would define items such as risk mng objectives/techniques, defined cyber risks, management and control, organizations policy and structure, IT infrastructure.)	A single,electric industry approved risk-based assessment methodology for identifying critical Bulk Electric Sytem assets does not exist. The Responsible Entity is free to choose an existing risk-based assessment methodology or adapt a methodology for this purpose. The criteria and documentation for this methodology can be part of an existing corporate risk management policy which should minimize the burden on the Responsible Entity. NERC has published a compendium of some risk assessment methodologies -- please go to www.esisac.com/library.html for more information.
	Are JOU RTU's which control generation to be included as a critical asset by all JOU parties?	The Critical Cyber Asset owners are responsible for compliance with these standards. Responsibility for compliance should be determined by specific agreements and contracts between the parties.
002-R1		
002-R2		
002-R3		
002-M1		
002-M2		
002-M3		
002-C1,1		
002-C1,2		
002-C1,3		
002-C1,4		
002-C2,1		
002-C2,2		
002-C2,3		
002-C2,4		

CIP-002 Drafting Team Responses to Comments

Name	Laurence W. Brown
Entity	Edison Electric Institute
Ready to Ballot:	No

General Comments

002-R1

R1.1 -- As worded, the list of "required" facilities appears far too rigid -- more strict even than the cybersecurity guidelines created by the nuclear industry to respond to federal requirements. Such a list must permit some reasonable flexibility in light of the vast differences among Responsible Entities in size and function. In particular, covering every "modification" would cover minor matters such as replacing bearings and setting relays. Also, one of the key elements to this Standard is performing a risk assessment to determine whether there are any critical cyber assets, yet that process and concept is not articulated except as concerning "additional" assets.

Suggested Alternative Wording:
Modify the existing last sentence so that it ends with the phrase -
"... the addition><, removal><, or >reasonably substantive< modification of any Critical Asset."

Also, move and append the text from R1.2 (with minor changes) so that the paragraph ends with-
"... The Responsible Entity shall utilize a risk-based assessment to identify any >< Critical Assets><. The risk-based assessment must include a description of the assessment>,< including the determining criteria, potential impacts, evaluation procedure and results. For the purpose of this standard, >< Critical Assets consists of those facilities, systems, and equipment >that<, if destroyed, damaged, degraded, or otherwise rendered unavailable, would have a detrimental impact on the reliability, or operability, of the electric grid and critical operating functions and tasks affecting the interconnected Bulk Electric System."

R1.1.3 -- IROL is dynamic, and can change on a daily basis, thus what is already a very broad requirement becomes unnecessarily burdensome.

Suggested Alternative Wording:
"R1.2.2. Transmission substation elements in the >critical,< direct transfer path>s< >reasonably< associated with an Interconnection Reliability Operating Limit (IROL)."

R1.1.4 -- Indicative of the unintended breadth of the current language is, for instance, "under control of a common plant control system". This could not reasonably be meant to include such add-on systems as environmental controls.

Suggested Alternative Wording:

The Drafting Team has removed the list of "Required Critical Assets, " in favor of requiring the Responsible Entity to use a risk-based assessment to identify its Critical Assets. The Drafting Team does provide a list of assets that the Responsible Entity must consider as part of its risk assessment (see R1.2). This list includes some, not all, of the same assets previously referred to as "Required" but most have been reworded to add clarity. For example, the list of assets to be considered in a risk assessment does not include IROL or Generating resources under control of a common plant control system that meet the criteria of 80% or greater of the largest single contingency within the Regional Reliability Organization. It does include blackstart generators and substations in the electrical path of transmission lines used for initial system restoration. An FAQ on blackstart has been drafted in response to comments requesting clarification.

"Generating resources>,< under >the reasonably direct< control of a common >< system>,< that meet the criteria of 80% or greater of the largest single contingency within the Regional Reliability Organization."

R1.1.6 -- Also indicating overbreadth, some "black start" facilities are simply not as important as others, and almost any facility could potentially be involved in a path related to some black-start scenario. It is unreasonable to expect entities to protect every facility to the same degree, yet the wording appears to indicate such an intent.

Suggested Alternative Wording:
"Systems, equipment and facilities >reasonably< critical to system restoration, including >critical< blackstart generators and substations in >< electrical path>s< of >critical< transmission lines used for initial system restoration."

R1.1.8 -- To reflect the suggested change to R1.1.3, above, and for the same reasons --

Suggested Alternative Wording:
"R1.1.8. Special Protection Systems whose misoperation can negatively affect elements >reasonably< associated with an IROL."

R1.2 -- Consistent with the comment above regarding R1 (the opening paragraph), the reference to assessments need to be elevated to cover all assets, rather than just "additional" assets. It is, however, appropriate to mention as clarification that the discovery of additional assets through a reasonable assessment is to be expected.

Suggested Alternative Wording:
"R1.2. Additional Critical Assets: >A reasonable risk-based assessment may identify additional critical assets.<"

OVERALL R.1 -- The current list of "required" facilities should be further clarified and made more realistic by reducing it, redesignating the "removed" facilities as assets that simply must be considered in any reasonable risk-based assessment.

Suggested Alternative Wording:
Combined with all of the other suggestions above, the new R1 would read as follows -

"R1. Critical Assets -- The Responsible Entity shall identify its Critical Assets and maintain a current list of all Critical Assets identified. The Responsible Entity shall review, and as necessary, update the list of Critical Assets annually, or within ninety calendar days of the addition, removal, or reasonably substantive modification of any Critical Asset. The Responsible Entity shall utilize a risk-based assessment to identify any Critical Assets. The risk-based assessment must include a description of the assessment including the determining criteria, potential impacts, evaluation procedure and results. For the purpose of this standard, Critical Assets

	consists of those facilities, systems, and equipment that, if destroyed, damaged, degraded, or otherwise rendered unavailable, would have a detrimental impact on the reliability, or operability, of the electric grid and critical operating functions and tasks affecting the interconnected Bulk Electric System. "R1.1. Required Critical Assets "R1.1.1. Control centers and backup control centers performing the functions listed in the Applicability section of this standard. "R1.1.2. Generating resources, under the reasonably direct control of a common system, that meet the criteria of 80% or greater of the largest single contingency within the Regional Reliability Organization. "R1.1.3. Generation control centers having control of generating resources that when summed meet the criteria of 80% or greater of the largest single contingency within the Regional Reliability Organization. "R1.2. Assets That Must be Assessed "R1.2.1. Systems, equipment and facilities critical to operating functions and tasks supporting control centers and backup control centers. These shall include telemetering, monitoring and control, automatic generation control, realtime power system modeling and real-time inter-utility data exchange. "R1.2.2. Transmission substation elements in the critical, direct transfer paths reasonably associated with an Interconnection Reliability Operating Limit (IROL). "R1.2.3. Systems, equipment and facilities reasonably critical to system restoration, including critical blackstart generators and substations in electrical paths of critical transmission lines used for initial system restoration. "R1.2.4. Systems, equipment and facilities critical to automatic load shedding under control of a common system capable of shedding 300 MW or more. "R1.2.5. Special Protection Systems whose misoperation can negatively affect elements reasonably associated with an IROL.	
002-R2	R2 -- First, this has the same problem with "modification" as does R1, as noted additional critical assets." Suggested Alternative Wording: The operative phrase should read, as above: "... the addition><, removal><, or >reasonably substantive< modification of ..." Second, the closing phrase "have the following characteristics" is unclear. Does it operate exclusively or inclusively? In other words, should the phrase be clarified to read either "have >only< the following characteristics" or "have >at least< the following characteristics"? R2.1 excepts generating station routable cyber assets from those that are critical "where a routable protocol does not extend beyond the physical boundary," yet the "Highlights" refers instead to the "electronic security perimeter." It is presumed that the Standard refers to the intended perimeter, but that is no longer certain. However, even if the Standard refers to the intended perimeter, it is unclear. For instance, the phrase "physical boundary" is undefined and could refer to walls or fences or property lines.	The requirement to identify Critical Cyber Assets has been renumbered to above.R3. The review and update period has been to changed "review this list [of Critical Cyber Assets] at least annually, and update as necessary."

	Suggested Alternative Wording: "R2.1. The Cyber Asset uses a routable protocol, unless the Cyber Asset is >located at< a substation or generation station >and its use of< a routable protocol does not extend >through or< beyond >any electronic or< physical >security perimeter associated with< the facility; or," R.2.2 -- If the phrase "have the following characteristics" is meant to be exclusive ("only"), then R2.2 appears to exclude "phone-home" modems. They may need to be covered, as they could be reset to answer-mode, or the answering phone might be subject to forwarding.	
002-R3	R3.3.2 -- Are SONET nodes exempted? They (as well as other communication equipment) could be used to shut down a data communication network via a denial-of-service attack. Even though they do not use routable protocol, they can be accessed via routable protocol.	Per Section 4 Applicability 4.2.2, the following are exempt from the standard: "Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters." Unless the Sonet nodes are within the Electronic Security Perimeter, they are outside the scope of the standard.
	What is the impact of Power Line Carrier (PLC) or Broadband over Power Line (BPL) technology on the electronic security perimeter? Is that simply a factor to be considered in a Responsible Entity's assessment? If so, what assessment criteria are available or should be used?	The technology used to transmit the routable protocol is outside the scope; the Electronic Security Perimter must be protected regardless of the communications methods. Please see CIP-005 for more information.
002-M1		
002-M2		
002-M3		
002-C1,1		
002-C1,2		
002-C1,3		
002-C1,4		
002-C2,1	How would an auditor determine compliance within any particular time period? SEE BELOW General Comment 2, regarding the removal of paperwork items from Levels of Non-Compliance thoughout the Cybersecurity Standards.	The requirement for updating within a ninety day time period has been removed. This level of non-compliance has been dropped.
002-C2,2		
002-C2,3		
002-C2,4		

Name	Peter Burke	
Entity	American Transmission Company	
Ready to Ballot:	No	
General Comments	American Transmission Company concurs with the comments submitted separately by the Edison Electric Institute and by the Midwest Reliability Organization.	Please see responses to Laurence W. Brown, Edison Electric Institute.
002-R1	American Transmission Company concurs with the comments submitted separately by the Edison Electric Institute and by the Midwest Reliability Organization.	
002-R2	American Transmission Company concurs with the comments submitted separately by the Edison Electric Institute.	
002-R3	American Transmission Company concurs with the comments submitted separately by the Edison Electric Institute.	
002-M1		
002-M2		
002-M3		
002-C1,1		
002-C1,2		
002-C1,3		
002-C1,4		
002-C2,1	American Transmission Company concurs with the comments submitted separately by the Edison Electric Institute.	
002-C2,2		
002-C2,3		
002-C2,4		

CIP-002 Drafting Team Responses to Comments

Name	Marc Butts
Entity	Southern Company
Ready to Ballot:	No

General Comments		
002-R1	R1 The requirement calls for updating the critical asset list "within ninety calendar days of the addition of, removal of, or modification to any Critical Asset". Suggest rewording this to "within ninety calendar days of the addition or removal of a Critical Asset". Including ANY modifications in this requirement is overly broad. Only those modifications that would cause an asset to come on or drop off the critical asset list should be included, and such modifications would be covered under the proposed new language. R1.1.1 - R1.1.8 - In R1.1.6, we suggest adding the word "primary" prior to the word "blackstart" in the statement "including blackstart generators and substations". This would provide some certainty in designating what blackstart generators are covered in the standard. R1.1.3 - IROL list - IROL is dynamic, and can change on a daily basis, thus what is already a very broad requirement becomes unnecessarily burdensome. R1.1.4, R1.1.5 - There should be a standard and clear definition for the term "largest single contingency". The value can vary by region, but the definition should not (and currently it does). It needs to be defined in a deterministic and stable manner. You can not have the requirements of CIP-003 to CIP-009 applying to REQUIRED critical assets that are determined based on some real-time grid condition, or quarterly adjusted number, or even annual . For example, a hot August afternoon should not suddenly bring assets into scope of a cyber security standard. We suggest this be defined as "the nameplate MW rating of the largest single generating unit within the Regional Reliability Organization". R1.1.6-This requirement to include all blackstart generators seems to make the critical asset list "upside down", requiring more very small units and less of the larger baseload units. R.1.1.6 is overbroad if it includes every unit that is involved in the blackstart. We suggest this definition be more specific. For example., there could be multiple paths for any blackstart configuration. Clarification is needed as to whether all paths are within the scope of the standard. R1.2 Clarification is needed as to what the difference is between the definition of 'critical asset' and 'additional critical asset'? In the alternative, we suggest removing this definition.	The Drafting Team has removed the list of "Required Critical Assets, " in favor of requiring the Responsible Entity to use a risk-based assessment to identify its Critical Assets. The Drafting Team does provide a list of assets that the Responsible Entity must consider as part of its risk assessment (see R1.2). This list includes some, not all, of the same assets previously referred to as "Required" but most have been reworded to add clarity. For example, the list of assets to be considered in a risk assessment does not include IROL or Generating resources under control of a common plant control system that meet the criteria of 80% or greater of the largest single contingency within the Regional Reliability Organization. It does include blackstart generators and substations in the electrical path of transmission lines used for initial system restoration. An FAQ on blackstart has been drafted in response to comments requesting clarification.
002-R2	R2 - Including ANY modifications in this requirement is overly broad. Only those modifications that would cause an asset to come on or drop off the critical asset list should be included, and such modifications would be covered under the proposed new language.	The requirement to identify Critical Cyber Assets has been renumbered to R3. The review and update period has been to changed "review this list [of Critical Cyber Assets] at least annually, and update as necessary."
002-R3		

CIP-002 Drafting Team Responses to Comments

002-M1		
002-M2		
002-M3		
002-C1,1		
002-C1,2		
002-C1,3		
002-C1,4		
002-C2,1	2.1 Level 1 - We suggest dropping this level of non-compliance due solely to the fact that there is nothing for an audit team to audit against. This level of non-compliance is based on "modifications" to critical assets which is overly broad and is not required to be documented (nor should it be).	The levels of non-compliance have been rewritten.
002-C2,2		
002-C2,3		
002-C2,4		

CIP-002 Drafting Team Responses to Comments

Name	Linda Campbell	
Entity	FRCC	
Ready to Ballot:	Yes	
General Comments	Purpose: The purpose and the requirements don’t match in regards to the use of a risk-based assessment procedure. R1.2 is the only requirement (to identify "additional critical assets") where such a procedure is mentioned. The purpose statement indicates the Critical Cyber Assets will be identified through the use of a risk-based assessment. The committee should clarify their intent. Draft #2 required that the Responsible Entity use "their preferred risk-based assessment" to identify its Critical Assets. Now Draft #3 has made a large change requiring the Responsible Entity to have a list of assets that are automatically deemed a "Critical Asset" by CIP-002-1.	The Drafting Team has removed the list of "Required Critical Assets, " in favor of requiring the Responsible Entity to use a risk-based assessment to identify its Critical Assets. The Drafting Team does provide a list of assets that the Responsible Entity must consider as part of its risk assessment (see R1.2). This list includes some, not all, of the same assets previously referred to as "Required" but most have been reworded to add clarity. For example, the list of assets to be considered in a risk assessment does not include IROL or Generating resources under control of a common plant control system that meet the criteria of 80% or greater of the largest single contingency within the Regional Reliability Organization. It does include blackstart generators and substations in the electrical path of transmission lines used for initial system restoration. An FAQ on blackstart has been drafted in response to comments requesting clarification.
002-R1	R1.1.6 - Clarify this section by adding wording, "including critical blackstart generators and substations...." as well as "system restoration" As was pointed out at one of the EEI conference calls, some generators and substations have the potential to be used in blackstart, but are not critical to blackstart, as there are multiple paths that could be used. We believe this distinction should be reflected in the verbiage. "System restoration" is very board and can include distribution facilities. R1.1.3 - IROL's can change depending on system conditions. By definition, critical assets may change with system conditions. Maintenance of the "Critical Asset" list will be time consuming if a given asset is deemed critical on day one is not critical on day twenty. By the time the responsible entity must update their Critical Asset list (within 90 days), the asset in question could have been and not been a critical asset several times.	See above.
002-R2	R2.1 is in conflict with the Development Highlights (page 2 of 4) in the area of routable protocols at substation. Is the perimeter the electronic, as stated in the Highlights or physical as stated in the standard that the protocol cannot extend beyond?	The characteristics have been clarified as using a routable protocol to communicate outside the Electronic Security Perimeter, or using a routable protocol within a Control Center. Therefore, a Cyber Asset using a routable protocol strictly within a generating station or substation does not have to be considered a Critical Cyber Asset. If the routable protocol crosses the boundary of the Electronic Security Perimeter, the Cyber Asset would be considered critical.
002-R3		
002-M1	What if there are no "additional critical assets," the only ones that require a risk-based assessment?	See response to General Comments above.
002-M2		

CIP-002 Drafting Team Responses to Comments

002-M3		
002-C1,1	In the applicability section A.3.1.10 and A.3.1.11, RRO's and NERC are included. Who has the monitoring responsibility for a RRO or NERC? Add Self-Certification and Audit information to this section. Proposed language would be: 1.1.-Complaince Monitoring Responsibility Regional Reliability Organization. 1.1.1.-The Compliance Monitor will request a self-certification annually. 1.1.2.-The Compliance Monitor will perform an audit at least once every three (3) calendar years.	NERC will monitor the RROs and a third party without vested interest in the outcome will monitor NERC. Self-certification has been added under "Additional Compliance Information."
002-C1,2		
002-C1,3	To complement a audit every three years, the data retention period should be 3 years.	The data retention period matches the requirement. Only the compliance monitor is required to keep records of an audit for 3 years. The Responsible Entity may choose to retain data longer.
002-C1,4		
002-C2,1	2.2.1 Clarification is needed, the intent of the level is to ensure that lists are updated when a change happens. There is no room in the non-compliance level for the eventuality that there are no changes with in the 90 days period	The levels of noncompliance have been rewritten.
002-C2,2		
002-C2,3		
002-C2,4	C2.2.4. must list all the documents that do not exist or there is no difference between level 4 non-complaince and level 3.	The levels of noncompliance have been rewritten.

Name	Gary Campbell	
Entity	MAIN	
Ready to Ballot:	No	
General Comments		
002-R1	R1.1.4 What is meant by common plant control system? Are you refering to the controls which control the units or the EMS system which may move the units or is it sime other meaning. In either case it seems that you will be including more plants than the 80% or greater of the largest single contingency requuires when identifying those losses which would jeapordize the reliability of the transmission system. I think we may need to consider for this requirement how they are connected to the outside world more. R1.1.5 I think this should be re-examined for the same reasons. R1.1.6 What is meant by initial system restoration? Are you meaning, inital restoration of a MISO area, a BAs area? In either case, I think you might want to word this requirement so it references the black start capability plan that BAs are required to have developed to be part of their emergency restoration plan. This plan identifies those blackstart units, their critical path and the steam unit to be started in the event of a system restoration. Otherwise the requiremetn as worded may mean any black start unit in an area which would mean protecting possibly alot more which may not be essential. In R1.1 I suggest rewording it to say "The assets shall be identified Critical Assets. As stated "Required assets" could mean I must have these assets.	The Drafting Team has removed the list of Required Critical Assets. Please see response to Ray A'Brial, Central Hudson Gas & Electric Corp.
002-R2		
002-R3		
002-M1	I suggest the opening statement for all three measures should read " The Responsible Entity shall have following to demonstrate full compliance with the requirements of this standard:"	Each of the measures has been reworded.
002-M2		
002-M3		
002-C1,1		
002-C1,2		
002-C1,3	why does the Responsible entity only have retain data for one year yet the RRO must maintain data for three years. I would think it would be naturally benefital for the responsible entity to maintain its records for a longer period of time and reduce security considerations.	The data retention period matches the requirement. Only the compliance monitor is required to keep records of an audit for 3 years. The Responsible Entity may choose to retain data longer.
002-C1,4		
002-C2,1		

002-C2,2

002-C2,3

002-C2,4

CIP-002 Drafting Team Responses to Comments

Name	Roger Champagne	
Entity		
Ready to Ballot:	No	
General Comments		
002-R1	Remove R1.1. Rational NERC Standards must fall within NERC's scope which is the Bulk Electric System. Some of these requirements are beyond the BES definition. This list is too prescriptive and contradicts the concept of each entity performing their risk based assessment. This list exceeds the original scope. During the June 2005 NERC webcast a question and answer demonstrate that this standard does not clearly define which entity is responsible. The question was "there is an element that belongs in this Standard. This element is owned by a Transmission Owner. The element is operated by a Transmission Operator. Who is responsible for this element? The chair answered that the Operator is responsible. Three other members of this Drafting Team do not agree.	The Drafting Team has removed the list of "Required Critical Assets, " in favor of requiring the Responsible Entity to use a risk-based assessment to identify its Critical Assets. The Drafting Team does provide a list of assets that the Responsible Entity must consider as part of its risk assessment (see R1.2). This list includes some, not all, of the same assets previously referred to as "Required" but most have been reworded to add clarity. For example, the list of assets to be considered in a risk assessment does not include IROL or Generating resources under control of a common plant control system that meet the criteria of 80% or greater of the largest single contingency within the Regional Reliability Organization. It does include blackstart generators and substations in the electrical path of transmission lines used for initial system restoration. An FAQ on blackstart has been drafted in response to comments requesting clarification.
	Combine R1 and R1.2. Eliminate the "additional critical assets" since they are outside the BES definition. Rational: Risk based assessment should apply to all Critical Assets.	The Critical Cyber Asset owners are responsible for compliance with these standards. Responsibility for compliance should be determined by specific agreements and contracts between the parties.
002-R2	Change R2 from modification to any Critical Asset or Critical Cyber Asset to modification to any Critical Cyber Asset. Rational: Requirements for Critical Assets are covered in R1	The requirement to identify Critical Cyber Assets has been renumbered to R3. The review and update period has been to changed "review this list [of Critical Cyber Assets] at least annually, and update as necessary."
002-R3		
002-M1		
002-M2	There is no approved list of Critical Cyber Assets in R2. Remove the word "approved."	The measures have been rewritten to refer back to the requirements.
002-M3		
002-C1,1		
002-C1,2		
002-C1,3		
002-C1,4		
002-C2,1		
002-C2,2		
002-C2,3		

002-C2,4

CIP-002 Drafting Team Responses to Comments

Name	Larry Conrad	
Entity	Cinergy	
Ready to Ballot:	No	
General Comments	Scope and meaning of words used in each section should be consistent with definition section. If there are differences between the definition section and the scope of what is included in the standard when the word is used, then the difference should be explained in the standard. At present the reader must rely on the FAQ's to clear up confusion created by the inconsistencies in the existing language. Examples include: Critical Assets, Cyber Assets, and Critical Cyber Assets.	The definition of Critical Asset and the Critical Assets identified under CIP-002 are now aligned. The references to ability to serve large quantities of customers for an extended period of time and significant risk to public health and safety have been removed from the definition of Critical Asset.
002-R1	R1.1.4: If a generating resource, identified as a critical cyber asset, is off line, such as due to an outage, it no longer crosses the threshold meeting the criteria of 80% or greater of the largest single contingency within the RRO. If the event is documented, is the responsible entity still required to comply with all aspects of the standard, especially with regards to the physical perimeter and personnel entry to the area? R1.1.5: Does not specify being under the control of a common system. Is the intent of this requirement to address only units that share a common control room and a common operating system? Assuming that the combined generation summation crosses the RRO's threshold, but individually the generation does not cross the threshold, if 2 generating units DO NOT share a common operating system, would they be considered Required Critical Assets? R1.2: When will additional guidance be provided regarding what is expected in the risk assessment? R1.2: Definition section states that Critical Assets (1) impact ability to serve large quantities of customers...(2) have detrimental impact on reliability...and (3) would cause significant risk to public health and safety. R1.2. only addresses reliability but does not reference (1) or (2) above. There should be consistency between the definition and the way the word is used within the standard or the difference should be explained in the standard. The text of CIP 002 should be modified so that the scope of what is included when "critical asset" is used in the standard is made clear. R1.2: What are examples of "any additional Critical Assets due to unique system configurations or other unique requirements" at a generating station? Is the intent of the standard to capture every or many support systems of the generating unit in the risk assessment process? In R1.1.1, what is the standard referring to (what is the definition of...) Control Center and backup control center? It says performing functions of the applicability section that lists just about everything including generator operator and owner. Are	The list of Required Critical Assets has been removed. Responsible Entities must use their risk-based assessment to identify Critical Cyber Assets. A single,electric industry approved risk-based assessment methodology for identifying critical Bulk Electric Sytem assets does not exist. The Responsible Entity is free to choose an existing risk-based assessment methodology or adapt a methodology for this purpose. The criteria and documentation for this methodology can be part of an existing corporate risk management policy which should minimize the burden on the Responsible Entity. NERC has published a compendium of some risk assessment methodologies -- please go to www.esisac.com/library.html for more information.

	generating station control rooms included under this category? Or, does generation fall strictly under R1.1.4 thru 1.1.6.?	
002-R2	Definition section states that Critical Cyber Assets are those cyber assets essential to the reliable operation of Critical Assets. Section 002 states critical cyber assets are those which use a routable protocol or are dial up accessible, but there is no reference in 002 as to whether the assets are essential. Words like critical cyber assets should be used consistently in both the definitions and in text. If differences exist, they should be explained in the standard language.	CIP-002 qualifies the definition of Critical Cyber Assets to reduce the implementation impact of the cyber security standards. This qualification is done in CIP-002 R2 by using the phrase "For the purpose of this standard" and the technical attributes of routable protocol and dial-up accessible. The word essential is still appropriate in the Critical Cyber Asset definition.
002-R3		
002-M1		
002-M2		
002-M3		
002-C1,1		
002-C1,2		
002-C1,3		
002-C1,4		
002-C2,1		
002-C2,2		
002-C2,3		
002-C2,4		

CIP-002 Drafting Team Responses to Comments

Name	Larry Conrad	
Entity	ECAR Critical Infrastructure Protection Panel	
Ready to Ballot:	No	
General Comments		
002-R1	R1.1.3 & R1.1.8 - Identificaton of IROL's is not clear. The meaning depends upon a definition in a different standard that is not clear. Recommendation: Either identify exactly which locations are IROL's within each region, such as ECAR, or else eliminate the IROL requirements references. If IROL requirement is removed, any later references to related measures or non-compliance should be changed as appropriate.	The list of Required Critical Assets, including IROLs, has been removed.
	R1.2 - Definition section states that Critical Assets (1) impact ability to serve large quantities of customers...(2) have detrimental impact on reliability...and (3) would cause significant risk to public health and safety. R1.2 only addresses reliability but does not reference that the ability to serve large quantities of customers and risks to public health and safety can be ignored for the purpose of this standard. The text of CIP 002 should be modified so that the relationship between the definition and how the definition is being used within the text of CIP 002 is made clear. At present there are differences between how words are defined in the definition section and what is included when the same word is used within the text.	The definition of Critical Asset and the Critical Assets identified under CIP-002 are now aligned. The references to ability to serve large quantities of customers for an extended period of time and significant risk to public health and safety have been removed from the definition of Critical Asset.
002-R2	Definition section states that Critical Cyber Assets are those cyber assets essential to the reliable operation of Critical Assets. Section 002 states critical cyber assets use a routable protocol or are dial up accessible, but there is no reference in 002 as to whether the assets are essential. This is similar to the comments on R1.2. Words like critical cyber assets should be used consistently in both the definitions and in text or differences need to be identified and explained in the standard language.	CIP-002 qualifies the definition of Critical Cyber Assets to reduce the implementation impact of the cyber security standards. This qualification is done in CIP-002 R2 by using the phrase "For the purpose of this standard" and the technical attributes of routable protocol and dial-up accessible. The word essential is still appropriate in the Critical Cyber Asset definition.
002-R3		
002-M1		
002-M2		
002-M3		
002-C1,1		
002-C1,2		
002-C1,3		
002-C1,4		

CIP-002 Drafting Team Responses to Comments

002-C2,1

002-C2,2

002-C2,3

002-C2,4

CIP-002 Drafting Team Responses to Comments

Name	Theodore Creedon, P.E.	
Entity	Creedon Engineering	
Ready to Ballot:	Yes	
General Comments	I agree.	
002-R1	R1.1.2 Needs to consider security for communications not under the control of the utility. I.e. internet, ISDN lines, etc. Encryption is recommended.	The standards reflect the Standard Authorization Request (SAR), which excluded communication links. The drafting team must respect the scope of the SAR and not extend it during standards development. The SAR reflects industry consensus on the scope of the standard to be developed.
002-R2		
002-R3		
002-M1		
002-M2		
002-M3		
002-C1,1		
002-C1,2		
002-C1,3		
002-C1,4		
002-C2,1		
002-C2,2		
002-C2,3		
002-C2,4		

CIP-002 Drafting Team Responses to Comments

Name	Joel De Granda	
Entity	Florida Power and Light	
Ready to Ballot:	No	
General Comments		
002-R1		
002-R2	R2.1 is in conflict with Development Highlights page 2 of 4 in the area of routable protocols at substation. Is the perimeter the electronic, as stated in the Highlights or physical as stated in the standard that the protocol cannot extend beyond?	R2 has been modified to clarify the intent for assets using routable protocols.
002-R3		
002-M1		
002-M2		
002-M3		
002-C1,1		
002-C1,2		
002-C1,3		
002-C1,4		
002-C2,1		
002-C2,2		
002-C2,3		
002-C2,4		

CIP-002 Drafting Team Responses to Comments

Name Richard Engelbrecht

Entity RGE

Ready to Ballot: No

General Comments

002-R1 Remove R1.1

Rational

NERC Standards must fall within NERC's scope which is the Bulk Electric System. Some of these requirements are beyond the BES definition.

This list is too prescriptive and contradicts the concept of each entity performing their risk based assessment.

This list exceeds the original scope.

During the June 2005 NERC webcast a question and answer demonstrate that this standard does not clearly define which entity is responsible. The question was "there is an element that belongs in this Standard. This element is owned by a Transmission Owner. The element is operated by a Transmission Operator. Who is responsible for this element? The chair answered that the Operator is responsible. Three other members of this Drafting Team do not agree.

Combine R1 and R1.2. Eliminate the "additional critical assets" since they are outside the BES definition.

Rational

Risk based assessment should apply to all Critical Assets.

Please see responses to Roger Champagne, Hydro-Québec TransÉnergie.

002-R2 Change R2 from

modification to any Critical Asset or Critical Cyber Asset

to

modification to any Critical Cyber Asset

Rational

Requirements for Critical Assets are covered in R1

CIP-002 Drafting Team Responses to Comments

002-R3

002-M1

002-M2 There is no approved list of Critical Cyber Assets in R2. Remove the word "approved."

002-M3

002-C1,1

002-C1,2

002-C1,3

002-C1,4

002-C2,1

002-C2,2

002-C2,3

002-C2,4

CIP-002 Drafting Team Responses to Comments

Name	Ken Fell	
Entity	New York ISO	
Ready to Ballot:	No	
General Comments		
002-R1	Remove R1.1 Rational NERC Standards must fall within NERC's scope which is the Bulk Electric System. Some of these requirements are beyond the BES definition. This list is too prescriptive and contradicts the concept of each entity performing their risk based assessment. This list exceeds the original scope. During the June 2005 NERC webcast a question and answer demonstrate that this standard does not clearly define which entity is responsible. The question was "there is an element that belongs in this Standard. This element is owned by a Transmission Owner. The element is operated by a Transmission Operator. Who is responsible for this element? The chair answered that the Operator is responsible. Three other members of this Drafting Team do not agree. Combine R1 and R1.2. Eliminate the "additional critical assets" since they are outside the BES definition. Rational Risk based assessment should apply to all Critical Assets.	Please see responses to Roger Champagne, Hydro-Québec TransÉnergie.
002-R2	Change R2 from modification to any Critical Asset or Critical Cyber Asset to modification to any Critical Cyber Asset Rational Requirements for Critical Assets are covered in R1	

CIP-002 Drafting Team Responses to Comments

002-R3

002-M1

002-M2 There is no approved list of Critical Cyber Assets in R2. Remove the word "approved."

002-M3

002-C1,1

002-C1,2

002-C1,3

002-C1,4

002-C2,1

002-C2,2

002-C2,3

002-C2,4

CIP-002 Drafting Team Responses to Comments

Name Francis Flynn

Entity National Grid USA

Ready to Ballot: No

General Comments

002-R1

Remove R1.1

Rational

NERC Standards must fall within NERC's scope which is the Bulk Electric System. Some of these requirements are beyond the BES definition.

This list is too prescriptive and contradicts the concept of each entity performing their risk based assessment.

This list exceeds the original scope.

During the June 2005 NERC webcast a question and answer demonstrate that this standard does not clearly define which entity is responsible. The question was "there is an element that belongs in this Standard. This element is owned by a Transmission Owner. The element is operated by a Transmission Operator. Who is responsible for this element? The chair answered that the Operator is responsible. Three other members of this Drafting Team do not agree.

Combine R1 and R1.2. Eliminate the "additional critical assets" since they are outside the BES definition.

From

R1. Critical Assets - The Responsible Entity shall identify its Critical Assets and maintain a current list of all Critical Assets identified. The Responsible Entity shall review, and as necessary, update the list of Critical Assets annually or within ninety calendar days of the addition of, removal of, or modification to any Critical Asset.

To

R1. The Responsible Entity shall utilize a risk-based assessment method for identifying Critical Assets. The risk-based assessment method must include a description of the method including the determining criteria, potential impacts, and evaluation procedure.

Rational - Risk based assessment should apply to all Critical Assets

Please see responses to Roger Champagne, Hydro-Québec TransÉnergie.

002-R2	Change R2 from modification to any Critical Asset or Critical Cyber Asset to modification to any Critical Cyber Asset Rational Requirements for Critical Assets are covered in R1
002-R3	
002-M1	
002-M2	There is no approved list of Critical Cyber Assets in R2. Remove the word "approved."
002-M3	
002-C1,1	
002-C1,2	
002-C1,3	
002-C1,4	
002-C2,1	
002-C2,2	
002-C2,3	
002-C2,4	

CIP-002 Drafting Team Responses to Comments

Name	Greg Fraser	
Entity	Manitoba Hydro	
Ready to Ballot:	No	
General Comments	The purpose in CIP-002-1 should be numbered similar to the other standards CIP-003-1 to CIP-009-1. 3.2 Applicability Add assets making the statement "The following entities and assets are exempt from this standard:"	The purpose has been numbered similar to CIP-003 through CIP-009. Applicability 4.2 has been modified to read "The following are exempt from this standard:".
002-R1	The required list of critical assets in R1 should be limited to a high-level list of critical assets such as lines, functions or facilities. The level of detail of the Critical Assets does not need to be as detailed as the Critical Cyber Asset list.	The list of Required Critical Assets has been removed. The assets required to be considered in your risk assessment is limited to a high-level list of assets as suggested.
002-R2		
002-R3		
002-M1		
002-M2	Replace " An approved list of..." with "The list of..." making M2 read "The list of Critical Cyber Assets as identified under Requirement R2."	The measures have been rewritten to refer back to requirements.
002-M3	Add reference in M3 to R3 by adding "...as identified under Requirement R3."	The measures have been rewritten to refer back to requirements.
002-C1,1		
002-C1,2		
002-C1,3		
002-C1,4		
002-C2,1		
002-C2,2		
002-C2,3		
002-C2,4		

CIP-002 Drafting Team Responses to Comments

Name	Jerry Freese	
Entity	American Electric Power	
Ready to Ballot:	No	
General Comments	Critical Assets should only include those assets (equipment and networks) from which one could do damage to the entire system, or at least as substantial part of it. The critical assets should include the control systems that reach out to the stations and plants, but not the individual stations and plants themselves. That is not to say that the stations and plants are not extremely important components to the grid, but in the context of CIP, they should not be considered "critical assets" nor should they be a part of the "security perimeter". A possible alternative would be to classify the substations and plants as "sub-critical assets" and specify that measures be in place to prevent access from these locations to other critical or sub-critical assets. In other words, if someone were to break in a station, we should insure that any damage that is done is limited to that station.	The list of Required Critical Assets has been removed. The Critical Assets are to be determined by the Responsible Entity's performance of a risk assessment.
002-R1	R 1.1.2 All the equipment associated with the "real-time inter-utility data exchange" cannot and should not be part of the "critical assets." The equipment that processes the data should be in scope, but the communications gear (routers) used exchange this data have to be configured the same on both ends. To achieve this, these systems are normally managed by a third party. Normally, this means that the individual utility does not even have administrative access to the equipment. It would make more sense to specify that these inter-utility links be configured and handled like other "external" links and that the data be encrypted to ensure maximum security. R.1.1.3 Is unclear. Clarify what a "direct transfer path" assocaited with an IROL. Is this simply all facilities comprising an IROL realted facility? R1.1.4 is unclear. "Generating resources.. that meet 80% or greater of the largest single contingency within the RRO" is confusing. A single contingency could be (for example) the loss of a transmission line or a generating unit. What is 80% of a transmission line outage in context of this requirement? R1.1.5 is unclear for the same reason as R1.1.4 R 1.1.6 is overly inclusive. Each blackstart scenario will be unique. Although a blackstart plan will include a preferred path, the plan itself is based on a hypothsis of a modelled event. there is no certainity that such a restoration path will be available during an actual restoration. Therefore inclusion of "substations in the electrical path of transmission lines for initial restoration" is either arbituary or simply impractical and unworkable. I have heard of interpretations of this to mean only stations that are in the black	(Draft 3 R1.1.2) The list of Required Critical Assets has been removed. Reference to real-time inter-utility data exchange has been moved to R3 and is now treated as a Critical Cyber Asset rather than a Critical Asset. The reference is intended to refer to the master end equipment and not the communication link. The Responsible Entity has to include routers if those routers are access points to the Electronic Security Perimter as described in CIP-005. If those routers are managed by a third-party then they must comply with the standards through contractual arrangements. If the Responsible Entity does not consider the routers part of the Electronic Security Perimter, then they could be considered part of the communications and, therefore, out of scope of these standards. Blackstart using a preferred path in a restoration plan without additional contingencies was the intent of this criteria. It was not intended that radial tapped stations be included as Critical Assets in system restoration. The 300 MW limit is described in FAQ 5: The DOE EIA-417 report form requires filing a report after an "uncontrolled loss of 300 MW or more of firm system loads for more than 15 minutes from a single incident."

	start power flow path. I have heard others more strictly interpret this to include tapped stations. In my opinion tapped stations really don't pose a risk, and thus, would provide limited benefit. However, there are many tapped stations, and if they are included would double or triple the associated compliance "book-keeping". I would strongly urge that radial tapped distribution stations be exempted from this standard, because they have very little impact on bulk power transport, and therefore, are not a critical facility, even if they happen to be tapped off of a black start path. R1.1.7 The 300 MW cut-off appears arbituary. Please justify. R 1.1.8 The transmission system should reliably operate following the loss of any single contingency -- including the loss or misoperation of an SPS. Therefore inclusion of SPS is unnecessary and arbituary. R 1.2 requires a "risk-based" assessment to identify any additional Critical Assets due to unique system configurations or other additional requirements". However the test is simply "detrimental impact on the reliability, .. Is this measurable? How is this type of assessment mesured against C.M.2?	
002-R2	Based on the expanded scope set forth in CIP-002 R1 for the Critical Assets and the subsequently expanded scope of the Critical Cyber Assets and the Electronic Security Perimeter, it would be impractical and infeasible to meet the obligations set forth in this requirement.	The list of Required Critical Assets has been removed.
002-R3		
002-M1		
002-M2		
002-M3		
002-C1,1		
002-C1,2		
002-C1,3		
002-C1,4		
002-C2,1		
002-C2,2		
002-C2,3		
002-C2,4		

CIP-002 Drafting Team Responses to Comments

Name	Edwin C. Goff III	
Entity	Progress Energy	
Ready to Ballot:	No	
General Comments		
002-R1	It should be better defined that only blackstart generators and substations critical to initial system restoration and stabilization are considered Critical Assets. In other words, just because a unit or substation is blackstart capable does not mean it is a Critical Asset. Only those units and substations used for initial restoration of Critical Assets should be deemed Critical Assets themselves. Another perspective, we discussed we would like to get clarification on is wheather blackstart generators and substations should fall under the cyber security rules or not. You would have to have 2 separate events, i.e. a cyber or event that caused the blackout and then another cyber event specific to the cyber generation asset. Even nuclear does not have to consider 2 simultaneous events for accidents.	The revised requirement R1 should permit Responsible Entities to use their risk-based assessment to determine which facilities are critical blackstart facilities. System restoration -- recovering from a system event -- is considered a critical function for the electric grid.
002-R2	If a critical asset has a routable protocol which does not extend beyond the physical boundary of the facility, but the routable protocol connects to non routable protocol which does extend beyond the boundary of the facility, is this considered a critical cyber asset? If a critical asset has a routable protocol which does not extend beyond the physical boundary of the facility, except for a VPN connection to a remote maintenance console, is this considered a critical cyber asset? It is unclear by definition whether PC/terminals established within an organization, outside of the System Control Center, for purposes of VIEW-ONLY access of EMS or Transmission data information would be considered critical cyber assets. For the following configuration would NERC consider the end-user PC's displaying EMS one-line screens to be critical cyber assets: e.g. the EMS at the System Control Center "pushes" a copy of all display data to a web-based server located external to the secure electronic perimeter, then various corporate PC's access the web-based server to display near real-time EMS generation and transmission one line displays and alarms. Since the end-user PC's do not directly connect to the EMS hosts with a routable protocol, would these PC's be excluded as critical cyber assets?	In a Control Center this cyber asset would be considered a Critical Cyber Asset, while in a generating station or substation it would not be a Critical Cyber Asset. This has been clarified in the requirement. The Drafting Team is not sure what the commenter was really asking regarding a VPN connection to a remote console and therefore, cannot provide a response. If these Cyber Assets are not dial-up accessible or use a routable protocol then they would not be considered Critical Cyber Assets. In this situation the Responsible might need to give consideration for CIP-003 R4 Information Protection.
002-R3		
002-M1		
002-M2		
002-M3		
002-C1,1		

002-C1,2
002-C1,3

002-C1,4

002-C2,1

002-C2,2

002-C2,3

002-C2,4

CIP-002 Drafting Team Responses to Comments

Name	Kenneth Goldsmith	
Entity	Alliant Energy	
Ready to Ballot:	No	
General Comments		
002-R1	Mandating that entities maintain list of "all" critical assets, adds significant additional overhead for insufficient benefit. An entity may have thousands of critical assets, and only a few critical cyber assets. It is only the critical cyber assets that need to be the focus of these requirements. The words "and maintain a current list of all Critical Assets identified" should be eliminated from R1 and associated changes should be made as applicable in CIP-002. The change would not impact the other CIP(s), which are focused on cyber assets. R1.1.2 should be eliminated. R1.1.1 does a fine job of covering control center and backup control center functions; leaving R1.1.2 in simply causes undue confusion.	Without a list of Critical Assets, the Responsisble Entity will be unable to identify and verify associated Critical Cyber Assets. However, the Drafting Team has removed the list of Required Critical Assets and replaced it with a list of high-level assets that must be considered as part of the Responsible Entity's risk assessment. The review and update period has been to changed review at least annually, and update as necessary. Draft 3 R.1.1.2 has been removed.
002-R2		
002-R3		
002-M1		
002-M2		
002-M3		
002-C1,1		
002-C1,2		
002-C1,3		
002-C1,4		
002-C2,1		
002-C2,2		
002-C2,3		
002-C2,4		

CIP-002 Drafting Team Responses to Comments

Name	Kathleen Goodman	
Entity	ISO New England Inc	
Ready to Ballot:	No	
General Comments	It is felt that CIP002 through CIP009 go beyond the intended scope of the original SAR for 1300. The final SAR for 1300, dated March 8, 2004, clearly states the Urgent Action Standard (U/A) 1200 is the basis for development of a permanent standard to replace it. The intent of both the U/A 1200 and SAR 1300 is to establish a minimum set of cyber security best practices as a standard baseline for general cyber protection of a reliable BES. U/A 1200 specifically excluded process control systems, distributed control systems, or electronic relays installed in generating stations, switching stations and substations. SAR 1300 made general reference to these stations in the initial definition of Critical Cyber Assets. However, that reference has been removed in the current Critical Cyber Assets definition, and has not re-appeared in the new Critical Assets definition. SAR 1300 does say that responsible entities will use a risk-based assessment methodology to identify critical cyber assets. In this regard, it does seem reasonable to require the risk-based assessment be used to identify assets and functions critical to a reliable BES, as there is an obvious correlation between critical assets and there supporting cyber assets being therefore critical themselves. But each entity must be allowed to conduct its own assessment, based on criteria defined by their Regional Reliability Organization (RRO) and/or more specifically their Control Area, as well as their own operational environment, without specific reference to process control systems, distributed control systems, or electronic relays installed in generating stations, switching stations and substations.	The SAR for 1300 included the following statement: "This cyber security standard shall primarily focus on electronic systems, which include hardware, software, data, related communications networks, control systems as they impact electric system operations, and personnel." This statement includes process control systems, distributed control systems, or electric systems installed in generating stations, switching stations and substations. Therefore, the drafting team does not believe it has extended the scope of the SAR. CIP-002--CIP-009 provide a minimum set of requirements that must be complied with rather than a set of best practices.. The revised requirement R1 allows a Responsible Entity to use a risk-based assessment to identify all the Critical Assets.
002-R1	Based on the general comments above, R1.1 should be removed, R1.2 should be de-bulleted and incorporated within the R1 statement.	The Drafting Team has removed the list of "Required Critical Assets, " in favor of requiring the Responsible Entity to use a risk-based assessment to identify its Critical Assets. The Drafting Team does provide a list of assets that the Responsible Entity must consider as part of its risk assessment (see R1.2). This list includes some, not all, of the same assets previously referred to as "Required" but most have been reworded to add clarity. For example, the list of assets to be considered in a risk assessment does not include IROL or generating resources under control of a common plant control system that meet the criteria of 80% or greater of the largest single contingency within the Regional Reliability Organization.
002-R2	Move second sentence regarding reviews to R3.	The review and update should remain separate from senior management approval. The senior management approval is an annual requirement whereas the review and update is intended to be an ongoing activity.

002-R3	Simply title R3 as "Reviews," and establish all review and approval requirements here.	See above.
002-M1		
002-M2	Remove the word "approved."	Removed as suggested.
002-M3	All review and approval metrics should be present here.	The measures have been rewritten and refer back to the requirements.
002-C1,1	None of the compliance statements are preceeded with the letter "C." It would help if they are made so.	The drafting team may not change the NERC-approved standard template.
002-C1,2		
002-C1,3	It is not clear when you mean documents, records, or data. These are three distinct items and should not be referenced interchangeably. Please clarify.	The Drafting Team has revised the standards for consistency and uses the terms as follows: DATA: information in a raw form. RECORDS: objective evidence that an activity has occurred. Records typically provide a snapshot in time of past actions and events, and can be used to demonstrate compliance. Records can only be modified or revised in compliance with proper and auditable trails. LOGS: Generally, collections of records of events that are generated automatically or by following a manual process. They identify who or what caused the event to be written and are time-stamped to indicate when the event occurred. DOCUMENTS: demonstrate what an organization does and plans to do and instruct employees how they should perform their tasks. Documents include but are not limited to policies, processes and procedures, specifications, drawings, maps, etc. A document can be in paper or electronic format. Please see the FAQs.
002-C1,4		
002-C2,1		
002-C2,2		
002-C2,3		
002-C2,4		

CIP-002 Drafting Team Responses to Comments

Name	Tim Hattaway
Entity	Alabama Electric Cooperative
Ready to Ballot:	Yes
General Comments	
002-R1	
002-R2	
002-R3	
002-M1	
002-M2	
002-M3	
002-C1,1	
002-C1,2	
002-C1,3	
002-C1,4	
002-C2,1	
002-C2,2	
002-C2,3	
002-C2,4	

CIP-002 Drafting Team Responses to Comments

Name	Jerry Heeren	
Entity	MEAG Power	
Ready to Ballot:	No	
General Comments	We again strongly suggest that the term "Bulk Electric System" needs to be defined clearly. NERC has created confusion by allowing varying definitions to appear in different locations. For example, NERC's Cyber Security Standards FAQ says the Bulk Electric System is above 35kV or as approved in a tariff filed with FERC; NERC's TOP-003-0 Standard shows the Bulk Electric System as greater than 100kV; NERC staff has verbally mentioned that the Bulk Electric System includes those systems above 100kV; the NERC Glossary of Terms defines Bulk Electric System as "commonly applied to the portion of an electric utility system that encompasses the electrical generation resources and bulk transmission system;" and finally, NERC's Version 0 Glossary says the Regional Reliability Organization should define Bulk Electric System, with 100kV as a minimum. MEAG Power believes that the Bulk Electric System should be defined as those systems that operate above 200kV. In Georgia and most places, the 100 kV to 200kV systems are primarily local load serving. MEAG's suggested definition of Bulk Electric System follows: "Bulk Electric System -- A term commonly applied to the portion of an electric utility system that encompasses the electrical generation resources and high-voltage transmission system (above 200kV)." If there is not widespread acceptance for MEAG's proposed definition, it would be best to define Bulk Electric System as determined by each utility based upon their specific system configuration.	The NERC Glossary is the definitive source of definitions associated with approved NERC standards.
002-R1	In Section R1.2, ICCP should be exempt if ICCP is communicating across a private network. This would be more consistent with the intent of R2.1 where the "routable protocol" does not extend past the physical boundary.	Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters are exempt under Applicability 4.2.2.
002-R2	In Section R2.1, the term "Routable Protocol" needs to be capitalized and defined in the Definitions Section of this document. The definition should be similar to the one used in Question #9 of the Draft #3 Frequently Asked Questions(FAQ's).	Routable protocol is well accepted and understood in the IT industry and the drafting team believes it is inappropriate to include this term in the NERC Glossary of Terms.
002-R3		
002-M1		
002-M2		
002-M3		
002-C1,1		
002-C1,2		
002-C1,3		
002-C1,4		
002-C2,1		

002-C2,2

002-C2,3

002-C2,4

CIP-002 Drafting Team Responses to Comments

Name	Peter Henderson	
Entity	Independent Electricity System Operator (IESO)	
Ready to Ballot:	No	
General Comments		
002-R1	Remove R1.1 Rational NERC Standards must fall within NERCO's scope which is the Bulk Electric System. Some of these requirements are beyond the BES definition.	The Drafting Team has removed the list of "Required Critical Assets, " in favor of requiring the Responsible Entity to use a risk-based assessment to identify its Critical Assets. The Drafting Team does provide a list of assets that the Responsible Entity must consider as part of its risk assessment (see R1.2). This list includes some, not all, of the same assets previously referred to as "Required" but most have been reworded to add clarity. For example, the list of assets to be considered in a risk assessment does not include IROL or Generating resources under control of a common plant control system that meet the criteria of 80% or greater of the largest single contingency within the Regional Reliability Organization. It does include blackstart generators and substations in the electrical path of transmission lines used for initial system restoration. An FAQ on blackstart has been drafted in response to comments requesting clarification.
002-R2		
002-R3		
002-M1		
002-M2	Delete the word "approved" in M2 as Requirement R2 does not impose a requirement for the list of Critical Cyber Assets to be formally approved. Alternatively, delete M2 all together as the requirement for a formally approved list of Critical Cyber Assets is specified in R3 and M3	Measures have been rewritten to refer back to requirements.
002-M3		
002-C1,1		
002-C1,2		
002-C1,3		
002-C1,4		
002-C2,1		
002-C2,2		
002-C2,3		
002-C2,4		

CIP-002 Drafting Team Responses to Comments

Name	E. Nick Henery	
Entity	SMUD	
Ready to Ballot:	No	
General Comments	The Drafting Team will need to go through the Standard and assign responsibility to each function from the functional model like the Version 0 STD. For this Standard to enforceable the generic use of Responsible Entity is the same as the generic use of Control Area. Even if the Standard lists the different functions it leaves open the possibility of misinterpretation as to which function is truly responsible.	The Responsible Entities are clearly enumerated in the standard Section A, item 4.
002-R1		
002-R2		
002-R3		
002-M1		
002-M2		
002-M3		
002-C1,1		
002-C1,2		
002-C1,3		
002-C1,4		
002-C2,1		
002-C2,2		
002-C2,3		
002-C2,4		

CIP-002 Drafting Team Responses to Comments

Name	Jack Hobbick	
Entity	Consumers Energy	
Ready to Ballot:	No	
General Comments	Consumers Energy has also submitted comments via the ECAR CIPP	Please see responses to Larry Conrad, ECAR CIPP.
002-R1		
002-R2	The newer version of the FAQs has a modifed treatment of the "routable protocol" issue. This is a clearer treatment of the topic. However,it give examples of "routable protocol Implementations", and include "DNP running over IP, [and] Modbus running over IP." We believe this creates the appearance of contradiction, and serves only to introduce confusion. Any IP packet (excluding limited broadcast) is routable, no matter what application layer information it contains, and specific mention of "xxx-over-IP" only clouds this simple fact. If protocols such as DNP, Modbus, etc. are to be mentioned at all, it should only be in the context of a specific exclusion, as is quite correctly done two paragraphs later, where they are classified as "not considered routable."	The FAQ has been updated.
002-R3		
002-M1		
002-M2		
002-M3		
002-C1,1		
002-C1,2		
002-C1,3		
002-C1,4		
002-C2,1		
002-C2,2		
002-C2,3		
002-C2,4		

CIP-002 Drafting Team Responses to Comments

Name Richard Kafka

Entity Pepco Holdings, Inc.

Ready to Ballot: No

General Comments		
002-R1	The intent to clarify Draft 2 on what was required and what should utilized a risk-based assessment was achieved. However it is felt that some of the required items should be left to a risk based assessment (e.g. R1.1.3 and R1.1.8 can change hourly, daily, seasonaly as the IROL can change due to system configurations, loading, & generation. This could become rather broad and burdensome.) The following are a couple of options in addressing this issue: Option 1: Every item under R1.1 is required for review by risk based assessment. Option 2: Segregate into required critical assets (no risk-based assessment) and those under a risk based- assessment. In addition to R1.1.1. being required (no risk based assessment). I would offer that R.1.1.4 and R1.1.5 should be required. R1.1.6: Please clarify the application of the phrase "... in the electrical path of trans lines used for initial system restoration". What T&D assets are included in scope from a blackstart perspective (e.g. generator substation, transmission substations, substations with load)? What blackstart genertaor assets are included? If a unit has blackstart capability but is not part of the blackstart plan are these assets Critical Assets? In a response to our comment offered in Draft 2, it stated that the word "plan" was going to be added (i.e. blackstart plan) in order to clarify if all black start units were included. The word plan appears not to have been added to Draft 3. Clarify modification to any critical asset. Does this include painting, modifications to documentation, adding oil to equipment, maintenance, repairs? R1.2. The Risk Assessment Whitepaper is not available yet but is needed to have a better understanding of R1.2 and CIP-002.	The Drafting Team has removed the list of "Required Critical Assets, " in favor of requiring the Responsible Entity to use a risk-based assessment to identify its Critical Assets. The Drafting Team does provide a list of assets that the Responsible Entity must consider as part of its risk assessment (see R1.2). This list includes some, not all, of the same assets previously referred to as "Required" but most have been reworded to add clarity. For example, the list of assets to be considered in a risk assessment does not include IROL or Generating resources under control of a common plant control system that meet the criteria of 80% or greater of the largest single contingency within the Regional Reliability Organization. It does include blackstart generators and substations in the electrical path of transmission lines used for initial system restoration. An FAQ on blackstart has been drafted in response to comments requesting clarification. NERC's compendium of risk assessment methodologies is available from www.esisac.com/library.html.
002-R2	R2.1: We agree with the addition noted in this requirement that excludes cyber assets in generation stations using routable protocols that do not extend "beyond the physical boundary of the facility". The language used in the Draft 3 Highlights pg2 note is inconsistent, instead referring to routable protocols extending "through the electronic security perimeter." Please clarify this inconsistency. Please distingush "accessable by routable protocl" vs "using routable protocol". Please clarify "modification" as noted above in R1. The closing phrase "have the following characteristics" is unclear. Does it operate exclusively or inclusively? In other words, should the phrase be clarified to read either "have >only< the following characteristics" or "have >at least< the following characteristics"?	The routable protocol characteristics has been clarified. The requirement "to review and update the list of Critical Assets within ninety days of the addition of, removal of, or modification to any Critical Asset or Critical Cyber Asset" has been removed. The requirement now reads "The Responsible Entity shall review this list at least annually, and update as necessary." The closing phrase "...having the following characteristics:" has been modified to "For the purpose of this standard, Critical Cyber Assets have at least one of the following characteristics:".

002-R3		
002-M1		
002-M2		
002-M3		
002-C1,1		
002-C1,2		
002-C1,3		
002-C1,4		
002-C2,1	How would an auditor determine compliance within any particular time period?	The levels of noncompliance have been rewritten.
002-C2,2		
002-C2,3		
002-C2,4		

CIP-002 Drafting Team Responses to Comments

Name	Tony Kroskey	
Entity	Brazos Electric Power Cooperative	
Ready to Ballot:	No	
General Comments	Subsection 2.0, Purpose, suggest changing the text "ensure reliable operation" to "ensure secure and reliable operation". Subsection 3.2, should remove word "entities".	Security is a component of reliability. Applicability 4.2 has been modified to read "The following are exempt from this standard:".
002-R1		
002-R2		
002-R3		
002-M1		
002-M2		
002-M3		
002-C1,1		
002-C1,2		
002-C1,3		
002-C1,4		
002-C2,1		
002-C2,2		
002-C2,3		
002-C2,4		

CIP-002 Drafting Team Responses to Comments

Name	Carol Krysevig	
Entity	Allegheny Energy Supply Co. LLC	
Ready to Ballot:	No	
General Comments	D1.3.1 - Suggest that the latest risk assessment be kept beyond one year if no changes have been made. D2.1 -- Add '(if applicable)' after 'with changes'. D2.2 -- Add '(if applicable)' after 'updated'. D2.3 -- Sentence should read 'One or more required documents (as listed in M1, M2, and M3) are missing.' D2.4 -- Sentence should read 'No required documents (as listed in M1, M2, and M3) exist.'	The Responsible Entity is required to perform a risk assessment every year. The levels of noncompliance have been rewritten.
002-R1	R1 - Revise the term 'modification' to 'significant modification' or remove the term altogether. R1.1 - The list of required critical assets should be split into two categories -- Required and Required because of Entity's Risk Assessment process. R1.1.1. and R.1.1.2. should remain under Required Critical Assets. R1.1.3. through R1.1.8. should be listed for consideration under R1.2. Additional Critical Assets. This enables Entities to evaluate and justify why certain assets may be excluded from the critical asset list. For example, a Company with numerous black start power stations may determine that only some of these power stations are actually critical while others do not significantly play a role in system start up. How should the apparent conflict between R1.1.1. Control Centers and R1.1.5. Generation Control Centers be interpreted? Control Centers, R1.1.1, could be interpreted to include Generation Control Centers, R1.1.5. As we interpret, the Generation Control Centers are looked at differently than Transmission Control Centers and are not included in R1.1.1. Is this correct? R1.1.5 - Better define the word 'control'. Does this mean 'startup/shutdown' capability or just simple supervisory control of power station output (MW)? R1.2 -- Delete the verbiage 'due to unique system configurations or other unique requirements' since it does not add any value and the Risk Assessment will identify such items. R1.2 -- The definition for 'Additional Critical Assets' is different than the definition for 'Critical Assets' and should either be defined under Definitions or revised to match the 'Critical Assets' definition.	The requirement has been changed to "The Responsible Entity shall review this list at least annually, and update as necessary." The Drafting Team has removed the list of "Required Critical Assets, " in favor of requiring the Responsible Entity to use a risk-based assessment to identify its Critical Assets. The Drafting Team does provide a list of assets that the Responsible Entity must consider as part of its risk assessment (see R1.2). This list includes some, not all, of the same assets previously referred to as "Required" but most have been reworded to add clarity. For example, the list of assets to be considered in a risk assessment does not include IROL or Generating resources under control of a common plant control system that meet the criteria of 80% or greater of the largest single contingency within the Regional Reliability Organization. It does include blackstart generators and substations in the electrical path of transmission lines used for initial system restoration. An FAQ on blackstart has been drafted in response to comments requesting clarification.. Generation control centers are now included in the R1.2.1. Control includes start/shutdown and control of the power station output (MW).
002-R2	R2. - Remove reference to 'Critical Assets' as this is redundant with R1. Also, revise or remove the term 'modification' as stated in the first comment to R1 above as this could result in onerous work tracking all modifications.	The reference to Critical Assets has been removed. The requirement now reads "The Responsible Entity shall review this list at least annually, and update as necessary."
002-R3		
002-M1		

002-M2	M2 -- Revise the sentence to state 'The list of Critical Cyber Assets as identified under Requirement R2 and any supporting documentation.'	The measures have been rewritten to refer back the requirements.
002-M3		
002-C1,1		
002-C1,2		
002-C1,3		
002-C1,4		
002-C2,1		
002-C2,2		
002-C2,3		
002-C2,4		

CIP-002 Drafting Team Responses to Comments

Name	John Lim	
Entity	Con Edison	
Ready to Ballot:	No	
General Comments	Minor editorial correction on Purpose: This standard requires the identification and enumeration of the Critical Cyber Assets that support the reliable operation of the Bulk Electric System as identified through the application of a risk-based assessment procedure.	The risk assessment is used to identify Critical Assets, not Critical Cyber Assets.
002-R1	Remove R1.1. Rational: NERC Standards must fall within NERC's scope which is the Bulk Electric System. Some of these requirements are beyond the BES definition. This list is too prescriptive and contradicts the concept of each entity performing their risk based assessment. This list exceeds the original scope. During the June 2005 NERC webcast a question and answer demonstrate that this standard does not clearly define which entity is responsible. The question was "there is an element that belongs in this Standard. This element is owned by a Transmission Owner. The element is operated by a Transmission Operator. Who is responsible for this element? The chair answered that the Operator is responsible. Three other members of this Drafting Team do not agree. Combine R1 and R1.2. Eliminate the "additional critical assets" since they are outside the BES definition. Rational: Risk based assessment should apply to all Critical Assets.	Please see responses to Roger Champagne, Hydro-Québec TransÉnergie.
002-R2	Change R2 from modification to any Critical Asset or Critical Cyber Asset to modification to any Critical Cyber Asset. Rational: Requirements for Critical Assets are covered in R1.	
002-R3		
002-M1		
002-M2	There is no approved list of Critical Cyber Assets in R2. Remove the word "approved."	
002-M3		
002-C1,1		
002-C1,2		
002-C1,3		
002-C1,4		
002-C2,1		
002-C2,2		
002-C2,3		

002-C2,4

CIP-002 Drafting Team Responses to Comments

Name	Deborah Linke	
Entity	Bureau of Reclamation	
Ready to Ballot:	No	
General Comments	Reclamation believes that the entire standard would be better served by following a well-defined risk assessment procedure, considering threats, vulnerabilities, likelihood of occurrence, ease of recovery and level of impacts. We are also concerned about the breadth of the Supporting Critical Assets definition since this essentially requires that all remote equipment supporting control centers be included as critical assets.	The list of "Required Critical Assets" has been removed. All Critical Assets are now to be determined by the Responsible Entity using a s risk-based assessment. The Responsible Entity may identify some remote assets as Critical Assets as a result of the the risk-based assessment.
002-R1		
002-R2		
002-R3		
002-M1		
002-M2		
002-M3		
002-C1,1		
002-C1,2		
002-C1,3		
002-C1,4		
002-C2,1		
002-C2,2		
002-C2,3		
002-C2,4		

CIP-002 Drafting Team Responses to Comments

Name	Greg Mason	
Entity	Dynegy Generation	
Ready to Ballot:	No	
General Comments		
002-R1	R1.1.1 of CIP-002-1 and FAQ #12 state that a control center or generation control center that performs the Generation Owner or Generation Operator functions,but with monitoring only and no direct remote control capability must be considered a Required Critical Asset and protected under the cyber security standard. Furthermore,R1.1.2 of CIP-002-1 defines facilities that support control centers such as telemetering,monitoring and control,automatic generation control(AGC),etc. as Required Critical Assets. This type of control center or generation control center does not have the ability to directy control the output of a plant or take it off line since the unit/plant has ultimate control over the operation of the unit.Therefore,if this type of control center was destroyed,damaged,degraded or otherwise rendered unavailable it would not have a detrimental impact on the reliability or operability of the electric grid.Similarly,it does not seem that AGC,telemetering,etc. facilities for this type of facility should be considered Required Critical Assets since if these sytems,capabilities,etc. were rendered unavailable it would not compromise the reliability of the generating units or the electric grid since the unit/plant has ultimate contol over the operation of the unit. Therefore,these requirements need to be modified to eliminate these types of facilities from being defined as Required Critical Assets. Also,for a generation only control center R1.1.1 and R1.1.5 overlap and appear to be conflicting. For a generation only control center does R.1.1.5 take precedence over R.1.1.1?Do these requirements effectively state that generation only control centers having control of 80% or greater of the largest single contingency within the RRO are considered Required Critical Assets and that generation only control centers having control of less than 80 % of the largest single contingency within the RRO are not considered Required Critical Assets? This needs to be clarified.	The list of Required Critical Assets has been removed, however, certain assets must be considered during a risk-assessment. Control centers are among these. Reference to telemetering has been removed and references to automatic generation control, real-time power modeling, etc. have been moved into R3 - Critical Cyber Asset Identification.
002-R2		
002-R3		
002-M1		
002-M2		
002-M3		
002-C1,1		

CIP-002 Drafting Team Responses to Comments

002-C1,2
002-C1,3

002-C1,4

002-C2,1

002-C2,2

002-C2,3

002-C2,4

CIP-002 Drafting Team Responses to Comments

Name	Paul McClay	
Entity	Tampa Electric	
Ready to Ballot:	No	
General Comments	Purpose: The purpose and the requirements don’t match in regards to the use of a risk-based assessment procedure. R1.2 is the only requirement (to identify "additional critical assets") where such a procedure is mentioned. The purpose statement indicates the Critical Cyber Assets will be identified through the use of a risk-based assessment. The committee should clarify their intent.	Please see response to Linda Campbell, FRCC.
002-R1	R1.1.6 - Clarify this section by adding wording, "including critical blackstart generators and substations...." As was pointed out at one of the EEI conference calls, some generators and substations have the potential to be used in blackstart, but are not critical to blackstart, as there are multiple paths that could be used. We believe this distinction should be reflected in the verbiage.	
002-R2	R2.2 -- Based upon clarification in the FAQ, we believe the intent of including dialup accessible devices in the definition of critical cyber assets was to ensure that the dialup is properly secured as required in CIP005. However, without that clarification one could conclude that every dialup accessible device that controls a critical cyber asset would be subject to the entire body of cyber security standards. If the intent we interpret is correct (i.e. FAQ question 11 indicates the critical asset is not subject to CIP-006-1 and that is reinforced by FAQ 3 related to CIP-006-1), then additional clarification is required within the standard to ensure consistent interpretation across the industry.	
002-R3		
002-M1		
002-M2		
002-M3		
002-C1,1		
002-C1,2		
002-C1,3		
002-C1,4		
002-C2,1		
002-C2,2		
002-C2,3		
002-C2,4		

CIP-002 Drafting Team Responses to Comments

Name	David McCoy	
Entity	Great Plains Energy/Kansas City Power & Light	
Ready to Ballot:	No	
General Comments	The FAQ should give exampless of Critical Cyber Assets. For example, it should be made clear that Switzer Relays are not Critical Cyber Assets unless deemed so by risk assessment.	The Responsible Entity must apply a risk-based assessment to determine Critical Assets, not to determine Critical Cyber Assets. Critical Cyber Assets are those Cyber Assets that are essential to the operation of the Critical Assets.
002-R1	We cannot be foreced to update our list of Critical Assets after every modification, like a wiring change is made. The word "modification" should be dropped from R1.	This requirement now reads "The Responsible Entity shall review this list at least annually, and update as necessary."
	R1.1.6 - This requirement should be eliminated and left to each entity to decide based on their risk assessments. If this provision remains there needs to be clarification as to whether single or multiple blackstart paths are to be deemed critical.	The Drafting Team has removed the list of "Required Critical Assets, " in favor of requiring the Responsible Entity to use a risk-based assessment to identify its Critical Assets. The Drafting Team does provide a list of assets that the Responsible Entity must consider as part of its risk assessment (see R1.2). This list includes some, not all, of the same assets previously referred to as "Required" but most have been reworded to add clarity. For example, the list of assets to be considered in a risk assessment does not include IROL or Generating resources under control of a common plant control system that meet the criteria of 80% or greater of the largest single contingency within the Regional Reliability Organization. It does include blackstart generators and substations in the electrical path of transmission lines used for initial system restoration. An FAQ on blackstart has been drafted in response to comments requesting clarification.
002-R2	R2. - The requirement to update the list should not include the word "modifications." It is unreasonable to expect responsible entities to update their Critical Asset list every time a modification is made to any one of them (wiring changes, for example). R2.1. - "or is addressable by" should be added after the word "uses."	This requirement now reads "The Responsible Entity shall review this list at least annually, and update as necessary." R2.1 The intent is that the Cyber Asset uses the routable protocol.
002-R3		
002-M1		
002-M2		
002-M3		
002-C1,1		
002-C1,2		
002-C1,3		
002-C1,4		

CIP-002 Drafting Team Responses to Comments

002-C2,1

002-C2,2

002-C2,3

002-C2,4

CIP-002 Drafting Team Responses to Comments

Name	William McEvoy	
Entity	Northeast Utilities	
Ready to Ballot:	No	
General Comments		
002-R1	Remove R1.1. Rational: NERC Standards must fall within NERC's scope which is the Bulk Electric Electric System. Some of these requirements are beyond the BES definition. This list is too prescriptive and contradicts the concept of each entity performing their risk based assessment. We support Linda Campbell's concern that this list exceeds the original scope. During the June 2005 NERC webcast a question and answer demonstrate that this standard does not clearly define which entity is responsible. The question was "there is an element that belongs in this Standard. This element is owned by a Transmission Owner. The element is operated by a Transmission Operator. Who is responsible for this element? The chair answered that the Operator is responsible. Three other members of this Drafting Team do not agree. Combine R1 and R1.2. Eliminate the "additional critical assets" since they are outside the BES definition. Rational: Risk based assessment should apply to all Critical Assets.	Please see responses to Roger Champagne, Hydro-Québec TransÉnergie.
002-R2	Change R2 from modification to any Critical Asset or Critical Cyber Asset to modification to any Critical Cyber Asset. Rational: Requirements for Critical Assets are covered in R1.	
002-R3		
002-M1		
002-M2	There is no approved list of Critical Cyber Assets in R2. Remove the word "approved."	
002-M3		
002-C1,1		
002-C1,2		
002-C1,3		
002-C1,4		
002-C2,1		
002-C2,2		
002-C2,3		
002-C2,4		

CIP-002 Drafting Team Responses to Comments

Name	Patrick Miller
Entity	PacifiCorp
Ready to Ballot:	Yes
General Comments	
002-R1	
002-R2	
002-R3	
002-M1	
002-M2	
002-M3	
002-C1,1	
002-C1,2	
002-C1,3	
002-C1,4	
002-C2,1	
002-C2,2	
002-C2,3	
002-C2,4	

CIP-002 Drafting Team Responses to Comments

Name	Don Miller	
Entity	First Energy Corp	
Ready to Ballot:	Yes	
General Comments		
002-R1	R 1.1 Should be "Critical Asset Identification Criteria" R 1.2 Should be titled "Additional Critical Asset Identification Criteria"	R1 has been changed to "Critical Asset Identification Method" and R2 is "Critical Asset Identification."
002-R2		
002-R3		
002-M1		
002-M2		
002-M3		
002-C1,1		
002-C1,2		
002-C1,3		
002-C1,4		
002-C2,1		
002-C2,2		
002-C2,3		
002-C2,4		

CIP-002 Drafting Team Responses to Comments

Name	Jeff Mitchell	
Entity	ECAR	
Ready to Ballot:	No	
General Comments		
002-R1	The ECAR TSPP has discussed defining IROLs at length during several of its meetings. Since ECAR is a highly interconnected network in the central part of the Eastern Interconnection, it is much more difficult to identify a circuit or interface that is associated with an IROL. At any given time and under certain system conditions and during certain contingencies, any one circuit/interface could be associated with an IROL. Consequently, such an IROL listing in ECAR would need to be dynamic, and could reasonably be expected to change as frequently as on a daily basis. On the other hand, due to their location and reduced EHV network, some other Regions may be more readily able to define a circuit or interface associated with an IROL, which would remain in effect over a more sustained period of time. With that said, the TSPP strongly feels that the CIP proposed standards should NOT include reference to IROLs when defining critical assets. Associating critical assets with IROLs in the CIP proposed standards would add another layer of complexity when entities are determining IROLs. The standard should be written such that entities are allowed to consider facilities associated with IROLs in their risk assessment when defining critical assets, but would not be required to automatically include those facilities as critical assets. As noted above, the list of facilities associated with IROLs can be dynamic and as such does not lend itself to be automatically included in the critical asset list, which requires additional electronic and/or physical security controls. Automatically including facilities associated with IROLs as critical assets in the context of the proposed CIP standards could have the unintended consequence of discouraging entities from defining IROLs if they know the associated facilities will be subjected to additional requirements from the proposed CIP standard.	The references to IROLs have removed from this standard.
002-R2		
002-R3		
002-M1		
002-M2		
002-M3		
002-C1,1		
002-C1,2		
002-C1,3		

CIP-002 Drafting Team Responses to Comments

002-C1,4

002-C2,1

002-C2,2

002-C2,3

002-C2,4

CIP-002 Drafting Team Responses to Comments

Name	Scott Mix	
Entity	KEMA, Inc	
Ready to Ballot:	No	
General Comments	Since the standards have been split up into multiple standards, the titles should be made clearer so that they stand on their own. As suggested in the response to my Draft 2 comment, I am resubmitting the request to change the title of this standard to "Identification of Critical Cyber Assets".	The title of CIP-002 has been changed to "Critical Cyber Asset Identification."
002-R1		
002-R2		
002-R3		
002-M1		
002-M2		
002-M3		
002-C1,1		
002-C1,2		
002-C1,3		
002-C1,4		
002-C2,1		
002-C2,2		
002-C2,3		
002-C2,4		

CIP-002 Drafting Team Responses to Comments

Name	Darrick Moe	
Entity	WAPA	
Ready to Ballot:	No	
General Comments	Mandating that entities' maintain lists of all critical assets at the same level of detail as the Critical Cyber Asset list is significant additional overhead for insufficient benefit. An entity may have thousands of critical assets, and far fewer critical cyber The requirement to maintain a list of critical assets should clarify that the list only needs to be a high level list, such as listing substations and lines, and not a detailed list of all equipment. This change would not impact the other CIP(s), which are focused on cyber assets.	The list of Required Critical Assets has been removed. The assets required to be considered in your risk assessment is limited to a high-level list of assets .
002-R1	The language in R1.1.2 that says "automatic generation control, real-time power system modeling and real-time inter-utility data exchange" should be rolled into R1.1.1 as these pertain directly to control centers. The balance of R1.1.2 should be eliminated. R1.1.2 as written causes undue confusion. For example, what does "telemetering" and "monitoring" include? In R1.1.7, change "common system" to "common control system". This would clarify that frequency relays at different substations that are all set to trip at a common frequency do NOT qualify as a "common system", even though they will likely operate in tandem.	Reference to telemetering has been removed and references to automatic generation control, real-time power modeling, etc. have been moved into R3 - Critical Cyber Asset Identification.
002-R2		
002-R3		
002-M1		
002-M2		
002-M3		
002-C1,1		
002-C1,2		
002-C1,3		
002-C1,4		
002-C2,1		
002-C2,2		
002-C2,3		
002-C2,4		

CIP-002 Drafting Team Responses to Comments

Name	Selby Mohr	
Entity	Sacramento Municipal Utility District	
Ready to Ballot:	Yes	
General Comments		
002-R1	CIP-002-1 R1.1.6. NERC’s proposal for classifying generating resources and transmission paths as Critical Assets appears to rely upon the whether a given generator or transmission path has a significant impact on the reliability of the whole interconnection of the Regional Reliability Organization. It is not clear if this same logic applies to classification of black start generators. For instance, a Balancing Authority/Load Serving entity may have black start generators for restoration of its own system, in the event of separation from the rest of the interconnection. If those black start generators are not relied upon by the Regional Reliability Organization for restoration of the interconnection as a whole, is it NERC’s intention that these types of black start generators be deemed as Critical Assets? CIP-002-1 R1.2. For the requirement on identifying Additional Critical Assets, is the emphasis on identifying only those systems that could have an impact on the whole interconnection of the Regional Reliability Organization? If a Balancing Authority/Load Serving entity had system components that would not affect the reliability of the whole interconnection but which could impact load serving capability of the Load Serving Entity can those assets be excluded from the Critical classification?	The list of "Required Critical Assets" has been removed. Responsible Entities must consider blackstart generators in their risk-based assessment to determine Critical Assets. See FAQ. Critical Assets affect the reliability or operability of the Bulk Electric System. These Critical Assets may affect only a portion of the Bulk Electric System and not the whole RRO. The Responsible Entity can exclude assets that do not affect the reliability or operability of the Bulk Electric System.
002-R2		
002-R3		
002-M1		
002-M2		
002-M3		
002-C1,1		
002-C1,2		
002-C1,3		
002-C1,4		
002-C2,1		
002-C2,2		

CIP-002 Drafting Team Responses to Comments

002-C2,3

002-C2,4

CIP-002 Drafting Team Responses to Comments

Name Kurt Muehlbauer

Entity Exelon

Ready to Ballot: Yes

General Comments

The documentation and processes around the responsible entitys tasks are too prescriptive. The industry needs to be extremely careful to avoid the creation of purely documentation-based non-compliances. With increasing legal requirements for compliance, and the associated penalties for noncompliance, noncompliance should be reserved for real security issues. It is simply too easy to make a mistake in documentation in light of the constantly evolving cyber environment.

Each entity should develop its own processes in support of the requirements, and these processes should be required to contain provisions for periodic review and approval applicable to each requirement. The processes should also be required to produce reasonable documentation to demonstrate compliance. However, it is not necessary to specify the details of the documentation or review periods.

The above approach can be met by removing references to documentation from the requirements section. Then, in the measures section require each entity to reasonably document programs and processes that support the security requirements and to produce reasonable documentation required to demonstrate compliance to the security requirements. Please refer to our overall comments on defining reasonable.

If the above approach is taken, it will be possible to delete many of the sub-bullet points under each requirement (because the details will be specified by each entity in their program or process, as applicable). This will also ensure that documentation and excessive low-value administrative tasks are removed from the requirements.

The Drafting Team has reviewed the standards and removed prescription where possible. The prescriptiveness that remains is necessary to provide the clarity requested by a majority of commenters.

The documentation required by these standards allow Responsible Entities to demonstrate that the policies, processes, and procedures that they have implemented consistently comply with the requirements of these standards.

002-R1

Change this requirement so that control rooms are required critical assets, but all other critical assets are identified through a risk-based analysis. An asset’s true impact to the system should determine whether it is critical. We also believe that determination of criticality must be done by each entity with input from the entity’s RTO and regional reliability organization.

For example, a variety of criteria must be considered when determining whether or not a generation asset is critical. These include base load and peaking, the size of the region, the capacity factor and the geographical location.

Recommend rewording R1 as follows:

R1. Critical Assets -The Responsible Entity shall identify its Critical Assets and maintain a current list of all Critical Assets identified. The Responsible Entity shall utilize a risk-based assessment to identify any Critical Assets. The risk-based assessment must include a description of the assessment including the determining

The Drafting Team has removed the list of "Required Critical Assets, " in favor of requiring the Responsible Entity to use a risk-based assessment to identify its Critical Assets. The Drafting Team does provide a list of assets that the Responsible Entity must consider as part of its risk assessment (see R1.2). This list includes some, not all, of the same assets previously referred to as "Required" but most have been reworded to add clarity. For example, the list of assets to be considered in a risk assessment does not include IROL or Generating resources under control of a common plant control system that meet the criteria of 80% or greater of the largest single contingency within the Regional Reliability Organization. It does include blackstart generators and substations in the electrical path of transmission lines used for initial system restoration.

	criteria, potential impacts, evaluation procedure and results. For the purpose of this standard, Critical Assets consists of those facilities, systems, and equipment that, if destroyed, damaged, degraded, or otherwise rendered unavailable, would have a detrimental impact on the reliability, or operability, of the electric grid and critical operating functions and tasks affecting the interconnected Bulk Electric System. R1.1. Required Critical Assets R1.1.1. Control centers and backup control centers performing the functions listed in the Applicability section of this standard. R1.2. Assets that must be considered as part of the risk assessment include: R1.2.1. Systems, equipment and facilities critical to operating functions and tasks supporting control centers and backup control centers. These shall include telemetering, monitoring and control, automatic generation control, realtime power system modeling and real-time inter-utility data exchange. R1.2.2. Transmission substation elements in the critical, direct transfer paths reasonably associated with an Interconnection Reliability Operating Limit (IROL). R1.2.3. Systems, equipment and facilities reasonably critical to system restoration, including critical blackstart generators and substations in electrical paths of critical transmission lines used for initial system restoration. R1.2.4. Systems, equipment and facilities critical to automatic load shedding under control of a common system capable of shedding 300 MW or more. R1.2.5. Special Protection Systems whose misoperation can negatively affect elements reasonably associated with an IROL. R1.3. Additional Critical Assets: A reasonable risk-based assessment may identify additional critical assets. R1.2.6. Generating resources, under the reasonably direct control of a common system, that meet the criteria of 80 pct or greater of the largest single contingency	
002-R2	Recommend removing the sentence The Responsible Entity shall review and, as necessary, update the list of Critical Cyber Assets annually, or within ninety calendar days of the addition of, removal of, or modification to any Critical Asset or Critical Cyber Asset. Please see the general comments to this standard for our rationale. In place of this statement, we recommend adding a general measure in the measures section to the affect, Each entity shall have processes for maintaining their list of critical assets and critical cyber assets, which shall include provisions for periodic reviews and approvals.	The requirement to identify Critical Cyber Assets has been renumbered to R3. The review and update period has been to changed "review this list [of Critical Cyber Assets] at least annually, and update as necessary."
002-R3	Recommend removing R3. Please see the general comments to this standard for our rationale. In place of this statement, we recommend adding a general measure in the measures section to the affect, Each entity shall have processes for maintaining their list of critical assets and critical cyber assets, which shall include provisions for periodic reviews and approvals.	See response to General Comments, above.

CIP-002 Drafting Team Responses to Comments

002-M1	Refer to general, overall comments submitted on CIP-002 through CIP-009 regarding revision of the measures and compliance specification.	See response to General Comments, above.
002-M2	Refer to general, overall comments submitted on CIP-002 through CIP-009 regarding revision of the measures and compliance specification.	See response to General Comments, above.
002-M3	Refer to general, overall comments submitted on CIP-002 through CIP-009 regarding revision of the measures and compliance specification.	See response to General Comments, above.
002-C1,1	Refer to general, overall comments submitted on CIP-002 through CIP-009 regarding revision of the measures and compliance specification.	See response to General Comments, above.
002-C1,2	Refer to general, overall comments submitted on CIP-002 through CIP-009 regarding revision of the measures and compliance specification.	See response to General Comments, above.
002-C1,3	Refer to general, overall comments submitted on CIP-002 through CIP-009 regarding revision of the measures and compliance specification.	See response to General Comments, above.
002-C1,4	Refer to general, overall comments submitted on CIP-002 through CIP-009 regarding revision of the measures and compliance specification.	See response to General Comments, above.
002-C2,1	Refer to general, overall comments submitted on CIP-002 through CIP-009 regarding revision of the measures and compliance specification.	See response to General Comments, above.
002-C2,2	Refer to general, overall comments submitted on CIP-002 through CIP-009 regarding revision of the measures and compliance specification.	See response to General Comments, above.
002-C2,3	Refer to general, overall comments submitted on CIP-002 through CIP-009 regarding revision of the measures and compliance specification.	See response to General Comments, above.
002-C2,4	Refer to general, overall comments submitted on CIP-002 through CIP-009 regarding revision of the measures and compliance specification.	See response to General Comments, above.

CIP-002 Drafting Team Responses to Comments

Name	Jeffrey Mueller	
Entity	PSEG Companies	
Ready to Ballot:	No	
General Comments	The PSEG Companies have reviewed and share the concerns expressed in the Comments of PJM and EEI. Accordingly, the PSEG Companies support the comments of PJM and EEI, and request that the concerns expressed in those comments be properly addressed in the next version of the draft standard.	Please see responses to Laurence W. Brown, Edison Electric Institute.
002-R1		
002-R2		
002-R3		
002-M1		
002-M2		
002-M3		
002-C1,1		
002-C1,2		
002-C1,3		
002-C1,4		
002-C2,1		
002-C2,2		
002-C2,3		
002-C2,4		

CIP-002 Drafting Team Responses to Comments

Name	Mitchell Needham	
Entity	Tennessee Valley Authority	
Ready to Ballot:	No	
General Comments		
002-R1	R1.1.3 - This suggests a rather dynamic set of facilities, very difficult to manage. R1.1.4 - The use of RRO versus entity is confusing. TVA suggests this should be made similar to BAL-002, and specify power supply contingencies only. R1.1.5 - this could be included in R1.2 instead. It is unclear whether this is based on MW or some other measure. R1.1.6 - The inclusion of blackstart generators and associated transmission facilities is not needed here. These are assets to be deployed in the event of a cascading outage and are not reliability oriented. A better place would be to include any requirements in the EOP standards.	The Drafting Team has removed the list of "Required Critical Assets, " in favor of requiring the Responsible Entity to use a risk-based assessment to identify its Critical Assets. The Drafting Team does provide a list of assets that the Responsible Entity must consider as part of its risk assessment (see R1.2). This list includes some, not all, of the same assets previously referred to as "Required" but most have been reworded to add clarity. For example, the list of assets to be considered in a risk assessment does not include IROL or Generating resources under control of a common plant control system that meet the criteria of 80% or greater of the largest single contingency within the Regional Reliability Organization. It does include blackstart generators and substations in the electrical path of transmission lines used for initial system restoration. An FAQ on blackstart has been drafted in response to comments requesting clarification.
002-R2	TVA suggests adding back the R2.3 verbiage from draft 2: "Dial-up accessible Critical Cyber Assets which do not use a routable protocol require only an Electronic Security Perimeter for the remote electronic access without the associated Physical Security Perimeter.	Requirement R2 has been modified to read similar to the draft 2 version. However, as CIP-002 is to identify Critical Cyber Assets, it is not appropriate to include "require only an Electronic Security Perimeter for the remote electronic access without the associated Physical Security Perimeter." CIP-005 and CIP-006 communicate this intent.
002-R3		
002-M1		
002-M2		
002-M3		
002-C1,1		
002-C1,2		
002-C1,3		
002-C1,4		
002-C2,1	Level 1 might prove very difficult to determine, i.e. the ninety day requirement. Documentation could be difficult to verify.	The levels of noncompliance have been rewritten.
002-C2,2		
002-C2,3		
002-C2,4		

CIP-002 Drafting Team Responses to Comments

Name	Dave Norton
Entity	Entergy Transmission
Ready to Ballot:	No

General Comments

002-R1

R1: More specificity in the definition of "modification" appears appropriate to assure that the Standard applies only for significant, substantive changes.

R1.1.2: As written, one could interpret that every Remote Terminal Unit and/or communication path feeding information to one or more of the noted processes are themselves critical assets. This requirement's wording runs the risk of designating a large group of assets that are not in and of themselves critical. The process or processes may be critical, but the individual items of equipment that feed the processes are not necessarily critical. In addition, the list of processes identified in R1.1.2 may not be complete. At minimum, this section should be modified to establish practical limitations on what does and does not fit the description covered by this section. More to the point, loss of a single or small group of RTUs or communications paths does not necessarily mean the ability to perform critical tasks is lost, because of alternative means or compensating measures. We recommend that this section be deleted and that process-oriented criticalities be addressed under the "Additional Critical Asset" risk based assessment in R1.2.

R1.1.3:
What does "direct transfer path" mean? There needs to be more explicit criteria for how to apply this. There is no mention of direct transfer path in the NERC Version 0 Standards that we could find. Another approach for Transmission substation elements would be to identify them based on the risk assessment procedure in R1.2 below.

R1.1.4: What does this mean? If there is 5 generating units with individual programmable logic controllers that are monitored in one control room by a group of operators, and the sum of the capacity of the 5 generating units meet the criteria, do these resources qualify as "critical assets". Better yet, should they qualify? We recommend that the risk assessment procedure apply if the (large) size of an individual generating unit meets the stated criteria, and thereby would be considered critical by definition. A bit of clarity would add value here, perhaps starting with better definition of "largest single contingency."

R1.1.5: This should apply to regional balancing authorities, for example, but not the control room for a 5 generating unit facility. Again the Responsible Entity should have the option to apply the risk assessment procedure in R1.2 rather than have to strictly attend to generic critical asset designations. The key is to focus on the critical assets only.

The requirement "to review and update the list of Critical Assets within ninety days..." now reads "The Responsible Entity shall review this list at least annually, and update as necessary."

The Drafting Team has removed the list of "Required Critical Assets, " in favor of requiring the Responsible Entity to use a risk-based assessment to identify its Critical Assets. The Drafting Team does provide a list of assets that the Responsible Entity must consider as part of its risk assessment (see R1.2). This list includes some, not all, of the same assets previously referred to as "Required" but most have been reworded to add clarity. For example, the list of assets to be considered in a risk assessment does not include IROL or Generating resources under control of a common plant control system that meet the criteria of 80% or greater of the largest single contingency within the Regional Reliability Organization. It does include blackstart generators and substations in the electrical path of transmission lines used for initial system restoration. An FAQ on blackstart has been drafted in response to comments requesting clarification.

RTUs would be Critical Cyber Assets if they are essential to the operation of Critical Assets that have been identified as a result of the risk assessement.

(Draft 3 R1.1.2) References to monitoring and control, automatic generation control, real-time power system modeling and real-time inter-utility data exchange have been moved into R3 - Critical Cyber Asset Identification.

R1.1.6: "Substations in the electrical path" should apply only if there is a single transmission path available before the event. If there are multiple transmission paths (with associated substations), substation along a given or expected path should not be critical. Again the utility should have the option to apply the risk assessment procedure in R1.2.

R1.1.7: The Responsible Entity should have the option to apply the risk assessment procedure in R1.2 rather than have to strictly attend to broad-brush critical asset designations. The 'facilities' part of "Systems, equipment and facilities" could be interpreted to include the coffee pot in the system operator's kitchen.

R1.1.8: This criterion will likely miss a SPS that is deemed critical but that is not associated with an IROL. Again the Responsible Entity should have the option to apply the risk assessment procedure in R1.2 rather than have to strictly attend to generic critical asset designations.

R1.2: 1) Suggest modifying the first sentence to read: "The Responsible Entity shall utilize a risk-based assessment methodology of the Responsible Entity's choosing to identify any additional Critical Assets due to unique system configurations or other unique requirements." 2) What is a "detrimental impact"? How bad is bad?

002-R2

002-R3

002-M1

002-M2

002-M3

002-C1,1

002-C1,2

002-C1,3

002-C1,4

002-C2,1

002-C2,2

002-C2,3

002-C2,4

CIP-002 Drafting Team Responses to Comments

Name	Doug Orlofske
Entity	Wisconsin Public Power Inc
Ready to Ballot:	Yes
General Comments	
002-R1	
002-R2	
002-R3	
002-M1	
002-M2	
002-M3	
002-C1,1	
002-C1,2	
002-C1,3	
002-C1,4	
002-C2,1	
002-C2,2	
002-C2,3	
002-C2,4	

CIP-002 Drafting Team Responses to Comments

Name	Kevin Perry	
Entity	Southwest Power Pool	
Ready to Ballot:	No	
General Comments		
002-R1	R1.1.2: The requirement includes automatic generation control. A pure interpretation of requirement would apply to the SCADA system performing the AGC function and sending control signals to the generation units. To clarify the expectations, the requirement should include centralized SCADA systems performing AGC calculations and then sending the set points/deployment instructions to remote SCADA systems that in turn calculate and send the control signals to the generation units. An example would be a market operations system that is calculating deployment instructions to be sent to the generation authorities and balancing authorities via any number of means. Likewise, a scheduling or market operations system that calculates an NSI that is then sent to the balancing authority for inclusion in AGC regulation calculations would not necessarily be recognized as having an AGC function. The market or scheduling system is not directly controlling the units and may not even be running an AGC function, but in the grand scheme of things, potentially poses a risk to bulk transmission system reliability should it be compromised and the calculations that a traditional AGC system relies upon be adversely affected.	References to monitoring and control, automatic generation control, real-time power system modeling and real-time inter-utility data exchange have been moved into R3 - Critical Cyber Asset Identification. If the Responsible Entity is an Applicable Entity under Section A4 of the standard, systems such as you exemplify would be subject to the standards. The SAR excludes market operation systems and are, therefore, out of scope.
002-R2	R2.1: It would be better to state that any cyber asset used to control or operate a facility designated as a critical asset, regardless of its dial-up accessibility or support of routable protocols that do not extend beyond the facility, be designated as a critical cyber asset.	The technical characteristics of routable protocol and dial-up accessible are intended to limit the scope of Cyber Assets that Responsible Entities must consider critical. The requirement (now R3) has been reworded for clarity.
002-R3	Please clarify "Senior Manager". Is this a company executive, or simply the facility manager? Delegation of responsibility should not be permitted.	It is intended that the Senior Manager be at an Executive level, but it is up to the Responsible Entities to determine. Responsible Entities must define policies, exception handling, and delegation authority.
002-M1		
002-M2		
002-M3	Subject to revision of requirement R3, delegation of responsibility should not be permitted.	See response above.
002-C1,1		
002-C1,2		
002-C1,3		
002-C1,4		

CIP-002 Drafting Team Responses to Comments

002-C2,1	How does one propose to verify that changes to CA and CCA lists have not been updated within 90 calendar days? It might be better to change the requirements and compliance measures to require a documented quarterly review of all CA and CCA (not necessarily requiring a senior management signoff) with an indication where no changes were necessary.	The levels of noncompliance have been rewritten.
002-C2,2		
002-C2,3		
002-C2,4		

CIP-002 Drafting Team Responses to Comments

Name	Tom Pruitt	
Entity	Duke Power Company	
Ready to Ballot:	Yes	
General Comments	A.2 -- It would be helpful to use the same numbering scheme in section A of CIP-002 as is used in CIP-003 through CIP-009. Why is the Purpose not numbered in CIP-002 when it is numbered in all the rest? A.3.1 -- Given the critical role of the PSE, why are these standards not applicable to that entity? A.3.2.2 -- Appears to be inconsistent with definition of "Cyber Asset". A.4 -- This should reference the proposed Implementation Plan. Alternatively, the compliance implementation plan should be referenced in the compliance sections for all of CIP002 thru CIP 009.	The purpose has been numbered similar to CIP-003 through CIP-009. The standards reflect the Standard Authorization Request (SAR), which excluded PSEs. The drafting team must respect the scope of the SAR and not extend it during standards development. The SAR reflects industry consensus on the scope of the standard to be developed. The SAR also specifically excluded communication links. Although reviewed and voted upon by the industry, the Implementation is not part of the standard and cannot be referenced therein.
002-R1	R1.1.6 -- The section after the comma, i.e. "including blackstart generators and subations in the electrical path of transmision used for the initial system restoration" should be deleted. There may older facilities that are included as part of the plan and included in the diagram, but are not critical to overall recovery. Utilities should determine the critical assets for recovery based on individual evaluation. R1.1.7 -- Does this include the breakers, IEDs etc, in the field that are used to accomplish load shed? For instance, a control system sends a signal to a substation to open a breaker. Are the devices in the field, including the breaker, included in this inventory?	The Drafting Team has removed the list of "Required Critical Assets, " in favor of requiring the Responsible Entity to use a risk-based assessment to identify its Critical Assets. The Drafting Team does provide a list of assets that the Responsible Entity must consider as part of its risk assessment (see R1.2). This list includes some, not all, of the same assets previously referred to as "Required" but most have been reworded to add clarity. For example, the list of assets to be considered in a risk assessment does not include IROL or Generating resources under control of a common plant control system that meet the criteria of 80% or greater of the largest single contingency within the Regional Reliability Organization. It does include blackstart generators and substations in the electrical path of transmission lines used for initial system restoration. An FAQ on blackstart has been drafted in response to comments requesting clarification. The intention is to list high-level systems and facilities as Critical Assets. So, identifying the load shed system and then the facilities would be sufficient. The IEDs, etc. might be listed as Critical Cyber Assets.
002-R2	R2 -- Sentence two should strike the reference to Critical Assets. These are covered in R1. R2 -- The characteristics listed create a more restrictive definition that the Critical Cyber Assets definition listed elsewhere. Please reconcile this difference. R2.2 -- Does this mean that a cyber asset that is not dial-up accessible should NOT be considered a critical cyber asset?	The reference to Critical Assets has been removed. The technical characteristics of routable protocol and dial-up accessible are intended to limit the scope of Cyber Assets that Responsible Entities must consider critical. The requirement (now R3) has been reworded for clarity.
002-R3		

CIP-002 Drafting Team Responses to Comments

002-M1

002-M2

002-M3

002-C1,1

002-C1,2

002-C1,3

002-C1,4

002-C2,1

002-C2,2

002-C2,3

002-C2,4

CIP-002 Drafting Team Responses to Comments

Name	Duane Radzwion	
Entity	Consumers Energy	
Ready to Ballot:	No	
General Comments		
002-R1		
002-R2	Section R2 is far from being ready to go to ballot. The term "routable protocol" has been used without a clear definition of what constitutes a routable protocol. It appears the greatest potential for a cyber security incedent would come from systems and devices that are IP-based, and that is what the standard should specifically address. Additionally, there are errors in the definition in the FAQs, question #8, dated 12/30/04. These FAQs should help support and better explain the R2 requirement but instead reveal that there is a great deal of misconception about the routable protocol issue. Question 7 erroneously, calls Token Ring and DNP as routable protocols operating at Layer 3. However, Token Ring operates at Layer 2. DNP is not more routable than SC1801(RTU) Protocol. These only become routable when wrapped in something like TCP/IP. Prior to balloting this issue should be resolved to the point where there is no room left for interpretation (or misinterpretation) and that only those communication protocols that are highly vulnerable are addressed.	The FAQ has been modified for clarity.
002-R3		
002-M1		
002-M2		
002-M3		
002-C1,1		
002-C1,2		
002-C1,3		
002-C1,4		
002-C2,1		
002-C2,2		
002-C2,3		
002-C2,4		

CIP-002 Drafting Team Responses to Comments

Name	Howard Rulf	
Entity	We Energies	
Ready to Ballot:	No	
General Comments	3.2.2: It appears that data communication links between discrete electronic security perimeters is exempt. If this includes network equipment that carries EMS traffic (routable protocol), this should not be excluded. (Man in the middle attacks)	A.3.2.2 specifically exempts cyber assets associated with communication networks and data communication links between discrete Electronic Security Perimeters. Communication between discrete electronic perimeters is beyond the scope of this standard, as defined in the Standard Authorization Request (SAR). The SAR reflects industry consensus on the scope of the standard to be developed. The drafting team must respect that scope and not extend it during standard development.
002-R1		
002-R2		
002-R3		
002-M1		
002-M2		
002-M3		
002-C1,1		
002-C1,2		
002-C1,3		
002-C1,4		
002-C2,1		
002-C2,2		
002-C2,3		
002-C2,4		

CIP-002 Drafting Team Responses to Comments

Name	Randy Schimka	
Entity	San Diego Gas and Electric Co.	
Ready to Ballot:	No	
General Comments	We appreciate the work that went into the clarification of this draft of CIP-002.	
002-R1		
002-R2	R2.2 on page 5 states that if a Cyber Asset is dial-up accessible then it should be considered a Critical Cyber Asset. We don't agree with that conclusion; it depends on the function of that particular Cyber Asset. There needs to be additional qualifications with this definition or changes to make it clearer.	The dial-up accessible Cyber Asset must be essential to the operation of a Critical Asset to be considered a Critical Cyber Asset. Critical Assets are determined by risk assessment.
002-R3		
002-M1		
002-M2		
002-M3		
002-C1,1		
002-C1,2		
002-C1,3		
002-C1,4		
002-C2,1		
002-C2,2		
002-C2,3		
002-C2,4		

CIP-002 Drafting Team Responses to Comments

Name	Lyman Shaffer
Entity	PG&E
Ready to Ballot:	Yes
General Comments	
002-R1	
002-R2	
002-R3	
002-M1	
002-M2	
002-M3	
002-C1,1	
002-C1,2	
002-C1,3	
002-C1,4	
002-C2,1	
002-C2,2	
002-C2,3	
002-C2,4	

CIP-002 Drafting Team Responses to Comments

Name	Neil Shockey	
Entity	Southern California Edison	
Ready to Ballot:	No	
General Comments		
002-R1	Change R1.1.4 to read: Generating resources under operational control of a common plant control system, such as a distributed control system (DCS) or programmable logic controllers (PLCs), that meet the criteria of 80% or greater of the largest single contingency within the Balancing Authority. Change R1.1.5 to read: Generation control centers having AGC operational control of generating resources that when summed meet the criteria of 80% or greater of the largest single contingency within the Balancing Authority.	Draft 3 R1.1.4 has been renumbered to R1.2.3 and reworded to "Generation resources that support the reliable operation of the Bulk Electric System." Draft 3 R1.1.5 has been deleted. Generation control centers are now included in R1.1.2.
002-R2		
002-R3		
002-M1		
002-M2		
002-M3		
002-C1,1		
002-C1,2		
002-C1,3		
002-C1,4		
002-C2,1		
002-C2,2		
002-C2,3		
002-C2,4		

CIP-002 Drafting Team Responses to Comments

Name	William Smith
Entity	Allegheny Power
Ready to Ballot:	No

General Comments

002-R1

Sections R1.1.3 through R1.1.8 are too prescriptive and should be relocated to section R1.2 to be considered as part of the Responsible Entitie's risk-based assessment. An example of this would be an entity that operates several blackstart generators. The entity may determine through a risk-based assessment that they have a large enough number of blackstart generators that any individual blackstart generator does not constitute a critical asset.

Sections R1.1.1 and R1.1.5 appear to be conflicting. R1.1.1 requires that all control centers performing the functions of a generator owner or operator are required critical assets. R1.1.5 states that only generation control centers having control of generating resources that when summed meet the criteria of 80%" are required critical assets. R1.1.5 should be removed, or R1.1.1 should exclude generation control centers not meeting the requirements in R1.1.5.

Section R1.1.5- The word "control" needs to needs to be further defined to clarify if it refers to being able to control the status of a generating resource (such as bringing it on or off line), perform AGC functions (such as requesting the generating resource to change it's output within a limited regulating range), or both.

Section R1.2- the phrase "due to unique system configurations or other unique requirements" should be removed. Additional assets could be deemed critical for any reason determined by the risk-based assessment.

Section R1.2- the phrase: "additional critical assets consists of those facilities, systems, and equipment which, if destroyed, damaged, degraded, or otherwise rendered unavailable, would have a detrimental impact on the reliability, or operability, of the electric grid and critical operating functions and tasks affecting the interconnected Bulk Electric System" is not completely consistent with the definition of Critical Assets which is given in the definitions section. It should be modified appropriately.

The Drafting Team has removed the list of "Required Critical Assets, " in favor of requiring the Responsible Entity to use a risk-based assessment to identify its Critical Assets. The Drafting Team does provide a list of assets that the Responsible Entity must consider as part of its risk assessment (see R1.2). This list includes some, not all, of the same assets previously referred to as "Required" but most have been reworded to add clarity. For example, the list of assets to be considered in a risk assessment does not include IROL or Generating resources under control of a common plant control system that meet the criteria of 80% or greater of the largest single contingency within the Regional Reliability Organization. It does include blackstart generators and substations in the electrical path of transmission lines used for initial system restoration. An FAQ on blackstart has been drafted in response to comments requesting clarification.

002-R2

002-R3

002-M1

002-M2

002-M3

CIP-002 Drafting Team Responses to Comments

002-C1,1

002-C1,2

002-C1,3

002-C1,4

002-C2,1

002-C2,2

002-C2,3

002-C2,4

CIP-002 Drafting Team Responses to Comments

Name	Paul Sorenson	
Entity	Open Access Technology International	
Ready to Ballot:	Yes	
General Comments	Clarification for all CIP-002 through CIP-009 Standards: Under each of the standards "Applicability" sections, is it implied that responsibility for compliance also falls to any agent or other entity responsible for management/operation of critical cyber assets for that entity? Does this need to be explicitly stated, or is it intentional that responsibility falls on the named entities and they, in turn, are responsible for ensuring that any sub-contracted entities, etc., are in compliance with the standards?	It is intentional that the listed Responsible Entities ensure compliance with standards.
002-R1		
002-R2		
002-R3		
002-M1		
002-M2		
002-M3		
002-C1,1		
002-C1,2		
002-C1,3		
002-C1,4		
002-C2,1		
002-C2,2		
002-C2,3		
002-C2,4		

CIP-002 Drafting Team Responses to Comments

Name	Robert Strauss	
Entity	NYSEG	
Ready to Ballot:	No	
General Comments		
002-R1	Remove R1.1. Rational: NERC Standards must fall within NERC's scope which is the Bulk Electric System. Some of these requirements are beyond the BES definition. This list is too prescriptive and contradicts the concept of each entity performing their risk based assessment. This list exceeds the original scope. During the June 2005 NERC webcast a question and answer demonstrate that this standard does not clearly define which entity is responsible. The question was "there is an element that belongs in this Standard. This element is owned by a Transmission Owner. The element is operated by a Transmission Operator. Who is responsible for this element? The chair answered that the Operator is responsible. Three other members of this Drafting Team do not agree. Combine R1 and R1.2. Eliminate the "additional critical assets" since they are outside the BES definition. Rational: Risk based assessment should apply to all Critical Assets.	Please see responses to Roger Champagne, Hydro-Québec TransÉnergie.
002-R2	Change R2 from modification to any Critical Asset or Critical Cyber Asset to modification to any Critical Cyber Asset. Rational: Requirements for Critical Assets are covered in R1.	
002-R3		
002-M1		
002-M2	There is no approved list of Critical Cyber Assets in R2. Remove the word "approved."	
002-M3		
002-C1,1		
002-C1,2		
002-C1,3		
002-C1,4		
002-C2,1		
002-C2,2		
002-C2,3		
002-C2,4		

CIP-002 Drafting Team Responses to Comments

Name	Karl Tammar
Entity	IRC
Ready to Ballot:	Yes
General Comments	
002-R1	
002-R2	
002-R3	
002-M1	
002-M2	
002-M3	
002-C1,1	
002-C1,2	
002-C1,3	
002-C1,4	
002-C2,1	
002-C2,2	
002-C2,3	
002-C2,4	

CIP-002 Drafting Team Responses to Comments

Name Todd Thompson

Entity PJM Interconnection

Ready to Ballot: No

General Comments		
002-R1	In section R1.1 the phrase "Required Critical Assets" should be changed to "Required Assets to be Assessed to Determine Criticality". The reason for this is that R1.1.1 -- R1.1.8 may contain items that are not critical. The phrasing in R1.1 would make everything that falls under R1.1.1 -- R1.1.8 critical no matter what a company's risk assessment program finds.	The Drafting Team has removed the list of "Required Critical Assets, " in favor of requiring the Responsible Entity to use a risk-based assessment to identify its Critical Assets. The Drafting Team does provide a list of assets that the Responsible Entity must consider as part of its risk assessment (see R1.2). This list includes some, not all, of the same assets previously referred to as "Required" but most have been reworded to add clarity. For example, the list of assets to be considered in a risk assessment does not include IROL or Generating resources under control of a common plant control system that meet the criteria of 80% or greater of the largest single contingency within the Regional Reliability Organization. It does include blackstart generators and substations in the electrical path of transmission lines used for initial system restoration. An FAQ on blackstart has been drafted in response to comments requesting clarification.
002-R2		
002-R3		
002-M1		
002-M2	Delete the word "approved" in M2 as Requirement R2 does not impose a requirement for the list of Critical Cyber Assets to be formally approved. Alternatively, delete M2 all together as the requirement for a formally approved list of Critical Cyber Assets is specified in R3 and M3.	Measures have been rewritten to refer back to requirements.
002-M3		
002-C1,1		
002-C1,2		
002-C1,3		
002-C1,4		
002-C2,1		
002-C2,2		
002-C2,3		
002-C2,4		

CIP-002 Drafting Team Responses to Comments

Name	Steven Townsend	
Entity	Consumers Energy Co.	
Ready to Ballot:	No	
General Comments	Consumers Energy has also submitted comments via the ECAR CIPP.	Please see responses to Larry Conrad, ECAR CIPP.
	NERC has made statements that a guideline/white paper on Risk Based Assessments would be made available on their website. Still not finding anything on this on the website, when can we expect this information to be available?	The white paper is available at the ESISAC web site at www.esisac.com.
	The standard needs to distinguish between securing a System Control Center and securing a substation. A single substation will not have the same impact that a Control Center will have if it is compromised and the Physical and Electronic Access to a Control Center needs to be much more stringent than for a substation. The standard needs to recognize these differences.	CIP-002 through CIP-009 establish a set of minimum requirements for cyber security. They, by necessity, have been drafted to accommodate a variety of Critical Assets. The Responsible Entity may implement stricter requirements if it deems appropriate.
002-R1		
002-R2	Draft 2 stated that for Dial-up accessible critical assets that do not use a routable protocol, Electronic Access Control only is required. Draft 3 does not have this. statement. Does this mean that Physical Access Control is also required?	Requirement R2 has been modified to read similar to the draft 2 version. However, as CIP-002 is to identify Critical Cyber Assets, it is not appropriate to include "require only an Electronic Security Perimeter for the remote electronic access without the associated Physical Security Perimeter." CIP-005 and CIP-006 communicate this intent.
002-R3		
002-M1		
002-M2		
002-M3		
002-C1,1		
002-C1,2		
002-C1,3		
002-C1,4		
002-C2,1		
002-C2,2		
002-C2,3		
002-C2,4		

CIP-002 Drafting Team Responses to Comments

Name	Martin Trence
Entity	Xcel Energy - Northen States Power (NSP)
Ready to Ballot:	Yes
General Comments	
002-R1	
002-R2	
002-R3	
002-M1	
002-M2	
002-M3	
002-C1,1	
002-C1,2	
002-C1,3	
002-C1,4	
002-C2,1	
002-C2,2	
002-C2,3	
002-C2,4	

CIP-002 Drafting Team Responses to Comments

Name	Rick Vermeers
Entity	Avistacorp
Ready to Ballot:	Yes
General Comments	
002-R1	
002-R2	
002-R3	
002-M1	
002-M2	
002-M3	
002-C1,1	
002-C1,2	
002-C1,3	
002-C1,4	
002-C2,1	
002-C2,2	
002-C2,3	
002-C2,4	

CIP-002 Drafting Team Responses to Comments

Name	Robert C. Webb	
Entity	Instrumentation, Systems and Automation Society	
Ready to Ballot:	No	
General Comments	These comments were developed by members of the Instrumentation, Systems and Automation Society, (ISA), SP99, "Manufacturing and Control Systems Security" committee's leadership team. The overall committee is composed of over 200 members including many users, government representatives, academics, control systems manufactures, and engineers with expertise in automation and control systems. ISA's SP99 is working to develop control systems security standards that provide sufficient guidance to the control systems and IT domain stakeholders to assure that security risks can be appropriately reduced without adversely affecting the intended functionality of those systems. ISA has published over 150 pages of guidance specific to the application of cyber security to control systems, in the form of two technical reports: ISA's ANSI/ISA-TR99.00.01-2004, "Security Technologies for Manufacturing and Control Systems", and ANSI/ISA-TR99.00.02-2004, "Integrating Electronic Security into the Manufacturing and Control Systems Environment." Both highlight the unique aspects of control systems which must be considered when applying security procedures and technology to control systems. ISA's constituency includes both fossil and nuclear power plant automation practitioners, and ISA has active standards committees in both of these areas (SP77, Fossil Power Plant Standards, and SP67, Nuclear Power Plant Standards).	Regarding comment #2a, the exclusionary language concerning generation assets has been removed with the exception of nuclear generation which is excluded by the SAR. Because distribution assets are not considered part of the Bulk Electric System, these resources remain excluded as well. Regarding comment #2b, much of the prescriptive language on how certain security measures should be applied has been removed. For example, the requirement for port scans in CIP 005, R4.2 has been replaced by a requirement to review only ports and services required for operations are enabled. In addition, the Drafting Team has removed most references to "how" security measures should be applied throughout the Standards unless it is required for compliance purposes. Regarding comment #2c, language has been added to reflect the fact that some security solutions that are available today were not available when some legacy systems were designed and put into service. CIP-003, CIP-004, CIP-005, and CIP-006 contain language addressing exceptions to their policies that may be required to deal with legacy systems and facilities where modern security solutions are not technically possible. In these cases, the Responsible Entities must identify and document the exception and describe the mitigating steps they are taking to secure the assets in lieu of the modern solution. Regarding the comments #3, #4, and #5 related to scope, the Standard reflects the Standard Authorization Request which excluded distribution, nuclear generation, and telecommunication infrastructure. The Drafting Team cannot exceed the scope of the SAR. A SAR reflects the industry consensus on the scope of any particular standard to be developed. Once SAR has been approved for standards drafting, the scope cannot be changed. The NERC Reliability Standards process would require new SARs to address these scope issues.
002-R1	Minor comment, Grammar - Section R1.1.1. refers to "the functions listed in the Applicability section of this standard." However, Section 3 does not list functions. It lists entities. R.1.1.1 should be revised to state "...performing the functions of entities listed..."	The revised requirement corrects the error.

	Scope - The 80% limitations in R1.1.4 and R1.1.5 and the definitions in R2 exclude many cyber assets which either communicate directly with critical cyber assets or, for some entities, make up the majority of the generation. (Consider the case where an entity has one or a few very large generators. The single largest contingency could easily be 800 MW in such a case. And yet the bulk of the generation for that area could come from generators much less than 800 MW, and often more susceptible to cyber attack). In the case of an area with nuclear generation, all of the non nuclear generators could be excluded, and unless Section 3.2.1 is revised, no generation would be included. This doesn't make sense. It appears contrary to the definition of bulk electric systems.	In response to consensus comments, the list of assets to be considered no longer references IROL, 80% of the largest single contingency or generating control centers.
	Further, many smaller generators could be directly connected to control centers belonging to the entities defined in Section 3.1. While proper application of the definitions of "Electronic Perimeter" and CIP-005 should preclude these links from becoming avenues of attack, excluding them from these requirements limits application of adequate defense in depth. If the risk was limited, this might be appropriate. But in many situations, there may be more of these connections than connections with larger generators. From a cyber intrusion viewpoint, all are equally important. Thus it is not appropriate to exclude what may be the bulk of these connections.	CIP-005 defines requirements for protecting access points to the Electric Security Perimeter.
	All of this would suggest lower limit, like 20%, be applied, after some consideration of what % of generation would typically be included.	
	Alternatively, a statement could be added to R2 similar to: R2.3. The Cyber Asset has any kind of network connection to any of the otherwise defined critical cyber assets.	
	This is similar to the old R3 of Draft 2. Indeed, its intent is covered in CIP-005, as noted in the drafting group's discussion of the changes. However, as noted above, this move reduces appropriate defense in depth, and it also tends to discount smaller generation which might otherwise be included. Thus this alternative is not the preferred approach. It reduces the likelihood of identifying and addressing significant vulnerabilities.	
002-R2	Scope - R2.1 should not be limited to routable protocols. "Non-routable" control system protocols have also experienced cyber impacts; they can and do provide an unintentional but real path to attack parts of Critical Cyber Assets. The definition should include all electronically interconnected cyber assets, with final requirements for those assets determined through the risk based vulnerability analysis results, as developed in CIP -005-1, R4.	The technical characteristics of routable protocol and dial-up accessible are intended to limit the scope of implementation of the cyber security standards, as defined in the SAR. (See response to General Comments, above.)
002-R3		
002-M1		
002-M2		

CIP-002 Drafting Team Responses to Comments

002-M3

002-C1,1

002-C1,2

002-C1,3

002-C1,4

002-C2,1

002-C2,2

002-C2,3

002-C2,4

CIP-002 Drafting Team Responses to Comments

Name	Laurent Webber	
Entity	Western Area Power Administration	
Ready to Ballot:	No	
General Comments	Consider the "Law of unintended consequences." There is a real risk that reliability will be adversely impacted when entities avoid using modern communication (i.e. routable protocols) just to keep equipment off the "critical cyber asset" list. The Standard Authoring Committee has apparently "pre-defined" all the threats, vulnerabilities and impacts to be considered and turned that into a list of equipment at risk. It would be better to follow a well-defined risk assessment procedure, considering threats, vulnerabilities, likelihoods, and impacts. The Committee obviously feels it cannot trust the entities to do that.	The list of "Required Critical Assets" (which was included in draft 3 in a response to comments asking for more definition as to what constituted a Critical Asset, not because of a lack of trust on the Drafting Team's part), has been removed. All Critical Assets are now to be determined by the Responsible Entity using a risk-based assessment. A list of assets that must be considered during a risk assessment remains to satisfy commenters' request for guidance.
002-R1	R1: Why keep a list of all Critical Assets, when all the subsequent requirements only apply to Critical Cyber Assets? The list of Critical Cyber Assets should be adequate. R1.1.2: This requirement implies that all remote equipment supporting control centers be included as critical assets. If that is the intent, then the requirement is too broad. If the intent is to include all those functions and applications that exist in the control center, then put it in R1.1.1 and eliminate R1.1.2. At the very least, remove telemetering and clarify that communications is not one of those "supporting" functions. R1.1.3: Define "substation elements." R1.1.6: Clarify "initial system restoration." Is it only those lines and generators involved in restoring the first 10% of the system or the first 50% of the system? R1.1.7: The phrase "Under control of a common system" is unclear. When individual under-frequency load-shedding relays are all set to identical frequencies, does that qualify as "under control of a common system"? R1.2: Remove the phrase "due to unique system configurations or other unique requirements" or explain why it's there and what it means. R1.2: The sentence beginning "For the purpose of this standard, additional Critical Assets..." seems to be a somewhat contradictory repetition of the definition of Critical Asset or an attempt to extend the definition. The sentence should be removed.	Without a list of Critical Assets, the Responsible Entity will be unable to identify and verify associated Critical Cyber Assets. The list of "Required Critical Assets" has been removed in favor of requiring the Responsible Entity to use a risk-based assessment to identify its Critical Assets. The Drafting Team does provide a list of assets that the Responsible Entity must consider as part of its risk assessment (see R1.2). This list includes some, not all, of the same assets previously referred to as "Required" but most have been reworded to add clarity. For example, the list of assets to be considered in a risk assessment does not include IROL or generating resources under control of a common plant control system that meet the criteria of 80% or greater of the largest single contingency within the Regional Reliability Organization. It does include blackstart generators and substations in the electrical path of transmission lines used for initial system restoration. An FAQ on blackstart has been drafted in response to comments requesting clarification. Reference to telemetering has been removed and references to monitoring and control, automatic generation control, real-time power system modeling and real-time inter-utility data exchange are now included as examples of Critical Cyber Assets in R3.
002-R2	R2: This requirement refers to a list of Critical Assets which we recommended be eliminated from requirement R1.	See above.
	R2.1: The term "physical boundary" is not defined or clearly described. Is this the	The reference to "physical boundary" has been removed.

	same as "Physical Security Perimeter" in the definitions or does it extend outside the building to the facility fence? R2.2: The requirement to include "telemetering" as a Critical Asset in R1.1.2 along with this requirement that any dial-up accessible Cyber Asset be designated as a Critical Cyber Asset implies that all dial-up meters are Critical Cyber Assets. Dial-up meter are not capable of cascading access to other power control equipment and should not be included as Critical Cyber Assets. Remove "telemetering from R1.1.2, or better yet remove R1.1.2 entirely, and clarify that Critical Cyber Assets include only those assets where remote control access or cascading access to other Critical Cyber Assets can be gained through dial-up access. R2.2: Change the wording to read, "The Cyber Asset is dial-up accessible and can be used to perform control functions such as opening breakers or changing relay settings."	Reference to telemetering has been removed.
002-R3	R3 refers to the Critical Asset list that we recommended be eliminated from requirement R1.	See response, above.
002-M1	M1 refers to the Critical Asset list that we recommended be eliminated from requirement R1.	See response, above.
002-M2		
002-M3	M3 refers to the Critical Asset list that we recommended be eliminated from requirement R1.	See response, above.
002-C1,1		
002-C1,2		
002-C1,3		
002-C1,4		
002-C2,1		
002-C2,2		
002-C2,3		
002-C2,4		

CIP-002 Drafting Team Responses to Comments

Name	Michal Zeithammel	
Entity	Brascan Power	
Ready to Ballot:	No	
General Comments		
002-R1	CIP-002-1-R1.1.1 requires that all control centers be identified as Critical Assets. Why would a control center that does not control critical assets need to be identified as critical? Brascan Power recommends that R1.1.1 be reworded to include only control centers that control critical assets that fall under R1.1.2 through R.1.1.8 and R.1.2.	The Drafting Team has removed the list of "Required Critical Assets, " in favor of requiring the Responsible Entity to use a risk-based assessment to identify its Critical Assets. The Drafting Team does provide a list of assets that the Responsible Entity must consider as part of its risk assessment (see R1.2). This list includes some, not all, of the same assets previously referred to as "Required" but most have been reworded to add clarity. For example, the list of assets to be considered in a risk assessment does not include IROL or Generating resources under control of a common plant control system that meet the criteria of 80% or greater of the largest single contingency within the Regional Reliability Organization. It does include blackstart generators and substations in the electrical path of transmission lines used for initial system restoration. An FAQ on blackstart has been drafted in response to comments requesting clarification.
002-R2		
002-R3		
002-M1		
002-M2		
002-M3		
002-C1,1		
002-C1,2		
002-C1,3		
002-C1,4		
002-C2,1		
002-C2,2		
002-C2,3		
002-C2,4		

CIP-002 Drafting Team Responses to Comments

Name	Guy Zito
Entity	NPCC
Ready to Ballot:	Yes

General Comments		
002-R1	Remove R1.1. Rational: NERC Standards must fall within NERC's scope which is the Bulk Electric System. Some of these requirements are beyond the BES definition. This list is too prescriptive and contradicts the concept of each entity performing their risk based assessment. This list exceeds the original scope. During the June 2005 NERC webcast a question and answer demonstrate that this standard does not clearly define which entity is responsible. The question was "there is an element that belongs in this Standard. This element is owned by a Transmission Owner. The element is operated by a Transmission Operator. Who is responsible for this element? The chair answered that the Operator is responsible. Three other members of this Drafting Team do not agree. Combine R1 and R1.2. Eliminate the "additional critical assets" since they are outside the BES definition. Rational: Risk based assessment should apply to all Critical Assets.	Please see responses to Roger Champagne, Hydro-Québec TransÉnergie.
002-R2	Change R2 from modification to any Critical Asset or Critical Cyber Asset to modification to any Critical Cyber Asset. Rational: Requirements for Critical Assets are covered in R1.	
002-R3		
002-M1		
002-M2	There is no approved list of Critical Cyber Assets in R2. Remove the word "approved."	
002-M3		
002-C1,1		
002-C1,2		
002-C1,3		
002-C1,4		
002-C2,1		
002-C2,2		
002-C2,3		
002-C2,4		

CIP-003 Drafting Team Responses to Comments

Name	Raymond A'Brial
Entity	Central Hudson Gas & Electric Corp
Ballot:	No

General Comments		
003-R1	R1 should be rewritten to "each Entity shall have a Cyber Security Policy that includes the following." NERC Standards should be focused on Reliability not management structure.	This requirement has been reworded and reference to "structure of relationships" removed.
003-R2	change R2 to "The Responsible Entity shall assign a senior manager or delegate(s) with responsibility"	This requirement is similar to Sarbanes-Oxley requirements. One senior manager needs to be responsible for ensuring that the requirements of these cyber security standards are being implemented and followed.
003-R3	Change R3 to "Exceptions - Instances where the Responsible Entity accepts non-conformance with its cyber security policy". The requirement to document non-conformance with an Entity's cyber security policy is sensible, but the requirement for a senior manager to approve all of those non-conformances is not. Some non-conformances may occur for reasons that are understood and knowingly tolerated for valid reasons. One could reasonably require the senior manager concerned to approve these, which effectively signals informed consent. However, there may be instances where a non-conformance occurs which represents an error that is not acceptable to the Entity concerned one which needs correcting rather than approval.	The language of the standard states that the approval of exceptions to the policy can be approved by a delegate or delegates approved by the senior manager.
003-R4	The minimum should not include everything. Remove ", and any related security information". Replace Requirement 4.3 with words from Requirement 5.2	Changed to "..security configuration information". Requirement 4.3 deals with the classification of information related to Critical Cyber Assets. Requirement 5.2 deals specifically with the ability of personnel to access the information. The classification of sensitive information and the access restrictions to the information are two separate requirements.
003-R5	Remove R5 because it overlaps Requirement 4 in CIP004 and Requirement 6.1 in CIP007. This overlap is confusing. It is not clear how Requirement 4 in CIP003 is different from this Requirement.	CIP-004 addresses the physical and logical access to Critical Cyber Assets. CIP-003 deals with the restricting access to the protected information regarding Critical Cyber Assets. These two are not in conflict. CIP-007 requirement 6.1 deals with user and system accounts and is not in conflict with CIP-003.
003-R6	R6 should move to CIP007.	While a change management program includes things like testing, patch management and anti-virus elements, it is more appropriately considered a Security Management control and belongs in CIP-003.

CIP-003 Drafting Team Responses to Comments

003-M1		
003-M2		
003-M3		
003-M4		
003-M5	Remove M5 since R5 was removed	See comment on R5.
003-M6	Move to CIP007 since R6 was moved to CIP007	See comment on R6.
003-C1,1		
003-C1,2		
003-C1,3		
003-C1,4	This is confusing. We believe this refers to non-conformance with the Entity's cyber security policy.	You are correct. This section has been reworded for clarity.
003-C2,1	Compliance statement 2.1.1 imposes a requirement that is not identified in the requirements section. Specifically, 2.1.1 effectively imposes a requirement that the gap in designating a senior management representative be less than 10 days, which is not specified in the requirements section. Ten days was never specified before this. Requirement R1.4 requires annual review of the cyber security policy. This is not consistent with compliance statement 2.1.2 which suggests that an entity that reviews its policy every three years would be fully compliant. Compliance statement 2.1.3 imposes a requirement that is not identified in the requirements section. Remove 2.2.3 since M5 was removed.	Levels of noncompliance have been rewritten.
003-C2,2		
003-C2,3	Levels of noncompliance have been rewritten.	Levels of noncompliance have been rewritten.
003-C2,4	Compliance statement 2.4.3 should be revised to more clearly refer to a program for the identification and classification of information about Critical Cyber Assets. 2.4.5 and 2.4.6 should be removed since they depend on M5, which we removed	The program for the identification and classification of information about Critical Cyber Assets referenced in 2.4.2 is intended to address the program defined in R4.

CIP-003 Drafting Team Responses to Comments

Name	Ori Artman	
Entity	Teltone	
Ballot:	Yes	
General Comments		
003-R1		
003-R2		
003-R3		
003-R4	The information should be stored in a limited access database and the database itself should be encrypted.	The intent of the standard is not to prescribe how an entity is to protect the information but that there must be an information protection program.
003-R5		
003-R6		
003-M1		
003-M2		
003-M3		
003-M4		
003-M5		
003-M6		
003-C1,1		
003-C1,2		
003-C1,3		
003-C1,4		
003-C2,1		
003-C2,2		
003-C2,3		
003-C2,4		

CIP-003 Drafting Team Responses to Comments

Name	Steve Badgett
Entity	Riverside Public Utilitities
Ballot:	Yes

General Comments

003-R1

003-R2

003-R3

003-R4

003-R5

003-R6

003-M1

003-M2

003-M3

003-M4

003-M5

003-M6

003-C1,1

003-C1,2

003-C1,3

003-C1,4

003-C2,1

003-C2,2

003-C2,3

003-C2,4

CIP-003 Drafting Team Responses to Comments

Name	Terry Baker
Entity	Platte River Power Authority
Ballot:	Yes
General Comments	
003-R1	
003-R2	
003-R3	
003-R4	
003-R5	
003-R6	
003-M1	
003-M2	
003-M3	
003-M4	
003-M5	
003-M6	
003-C1,1	
003-C1,2	
003-C1,3	
003-C1,4	
003-C2,1	
003-C2,2	
003-C2,3	
003-C2,4	

CIP-003 Drafting Team Responses to Comments

Name	Terry Bilke
Entity	Midwest ISO
Ballot:	No
General Comments	
003-R1	
003-R2	
003-R3	
003-R4	
003-R5	
003-R6	
003-M1	
003-M2	
003-M3	
003-M4	
003-M5	
003-M6	
003-C1,1	
003-C1,2	
003-C1,3	
003-C1,4	
003-C2,1	
003-C2,2	
003-C2,3	
003-C2,4	

CIP-003 Drafting Team Responses to Comments

Name	Pat Bourassa	
Entity	Wisconsin Public Service Corporation	
Ballot:	No	
General Comments	If a formal change management process is in place today, (including testing, backout plans and with approvals for all changes not considered minor), would this be adequate or is it necessary to specifically flag critical cyber assets changes for reporting purposes?	As long as you have a formal change management process that includes your Critical Cyber Assets, this should suffice.
	Why was the concept of 'segregation of duties' introduced into the security management controls? The previous content on needing auditable physical and logical controls in place seemed to have covered this process thoroughly.	Segregation of duties is not referenced.
003-R1		
003-R2		
003-R3	Due to the lack of user account administration security and general system security in the plant control systems, many exceptions will be documented per the CIP requirements until the vendor supplied systems implement security functionality and the systems can feasibly be upgraded. Most deal with the CIP-007: Cyber Security -Systems Security Management.	Responsible Entities may write exceptions to their policies. Please see the FAQs on technical feasibility.
003-R4		
003-R5		
003-R6	Real time systems require real time changes in emergency situations. Approvals may impact the ability to make critical corrections in real time.	R1.1 requires Responsible Entities to include provisions for emergency situations in their cyber security policies.
003-M1		
003-M2		
003-M3		
003-M4		
003-M5		
003-M6		
003-C1,1		
003-C1,2		
003-C1,3		

CIP-003 Drafting Team Responses to Comments

003-C1,4

003-C2,1

003-C2,2

003-C2,3

003-C2,4

CIP-003 Drafting Team Responses to Comments

Name	Laurence W. Brown	
Entity	Edison Electric Institute	
Ballot:	No	
General Comments		
003-R1	The phrase "structure of relationships" seems to indicate that detailed organization charts are required. This appears overly burdensome, as such charts become outdated frequently. If such charts must be required, they should not be covered by the overall policy section, since policies do not change frequently.	This requirement has been reworded and reference to "structure of relationships" removed.
003-R2		
003-R3	Overall Must every emergency count as an exception that must be documented? Can certain predictable emergencies by provided for through policies? SEE BELOW General Comment 1, regarding the need for an exceptions policy, particularly for natural disasters or law enforcement situations. R.3.1 It is not clear whether this applies to any exception even after it is over (for instance, to assist in reviewing the entity's general application of exceptions), or only to exceptions that have lasted some period of time (and if so, then to what period).	R1.1 requires Responsible Entities to include provisions for emergency situations in their cyber security policies. All exceptions must be approved and documented. R1.1 addresses emergency situations.
003-R4		
003-R5		
003-R6	Just as with CIP-002-R1 and -R2, above, reference to "modifying" is excessive. Suggested Alternative Wording: Replace the word "modifying" with the phrase "reasonably substantial modification of."	The standard calls for establishing and documenting a change control and configuration management processes. How each entity defines this process is up to the individual entity.
003-M1		
003-M2		
003-M3		
003-M4		
003-M5		
003-M6		
003-C1,1		
003-C1,2		

CIP-003 Drafting Team Responses to Comments

003-C1,3		
003-C1,4		
003-C2,1	C2.1.1 The reference to "ten or more calendar days" actually constitutes a requirement, and no such requirement for a minimum time period appears in R2.	Levels of noncompliance have been rewritten.
003-C2,2		
003-C2,3		
003-C2,4		

CIP-003 Drafting Team Responses to Comments

Name	Peter Burke	
Entity	American Transmission Company	
Ballot:	No	
General Comments	American Transmission Company concurs with the comments submitted separately by the Edison Electric Institute and by the Midwest Reliability Organization.	Please see responses to Laurence W. Brown, Edison Electric Institute.
003-R1	American Transmission Company concurs with the comments submitted separately by the Edison Electric Institute and by the Midwest Reliability Organization.	
003-R2		
003-R3	American Transmission Company concurs with the comments submitted separately by the Edison Electric Institute and by the Midwest Reliability Organization.	
003-R4	American Transmission Company concurs with the comments submitted separately by the Midwest Reliability Organization.	
003-R5	American Transmission Company concurs with the comments submitted separately by the Midwest Reliability Organization.	
003-R6	American Transmission Company concurs with the comments submitted separately by the Edison Electric Institute.	
003-M1		
003-M2		
003-M3		
003-M4		
003-M5		
003-M6		
003-C1,1		
003-C1,2		
003-C1,3		
003-C1,4		
003-C2,1	American Transmission Company concurs with the comments submitted separately by the Edison Electric Institute.	
003-C2,2		

003-C2,3

003-C2,4

CIP-003 Drafting Team Responses to Comments

Name	Marc Butts	
Entity	Southern Company	
Ballot:	No	
General Comments		
003-R1		
003-R2		
003-R3		
003-R4	R4.1 - We believe this section is too inclusive. The "include at a minimum" statement could easily be interpreted to include almost all documents related to critical Cyber Assets and related security. For example, this section could easily be interpreted to include substation drawings, blue prints, building plans, generation control center plans, employee background information, facility access records, etc. We agree that some sections are intended to be, and should be, broad enough for some operator interpretation, however this section is too prescriptive and needs to be either broad enough to permit operator interpretation, or more narrowly defined. What is important to protect from a information safeguards perspective are the critical asset list, security plans, recovery plans, and system design. Based on this, we suggest wording similar to the following: At a minimum this shall include procedures, critical asset inventories, floor plans of computing centers (primary Energy Management System (EMS), EMS equipment layouts, EMS configurations, disaster recovery plans, and incident response plans. R4.1 - We suggest removing the phrase "and any related security information". This phrase is overly broad and raises serious concerns as to whether full compliance is possible. R4.2 - We suggest removing this section entirely. This section is adequately covered in section 4.1.	R4.1 defines a minimum list. A Responsible Entity can choose to include to protect other information as it deems appropriate using reasonable business judgment. The statement in R4.1 has been removed. R4.1 specifies types of information to be protected. R4.2 addresses the level of protection that may be applicable to the information mentioned in R4.1.
003-R5		
003-R6	R6 We suggest replacing the phrase "any Critical Cyber Asset" with "significant production Critical Cyber Asset". R6.2 Clarification is needed that this requirement doesn't include every change. For example, there should be some allowances for emergency procedures and replacement. R6.3 We suggest replacing the phrase "any change" with "material changes".	Critical Cyber Assets are significant by definition. Requirements 6.2 and 6.3 have been removed.
003-M1		
003-M2		
003-M3		

003-M4		
003-M5		
003-M6		
003-C1,1		
003-C1,2		
003-C1,3		
003-C1,4		
003-C2,1	2.1.1 Level 1 Non-compliance The standard currently does not require a senior manager to be designated within 10 days. Thus, non-compliance should not be based on such a requirement. We suggest dropping this level and letting Level 2 pick up the non-compliance as-is. The standard allows in R2.2 for a 30 day period but this assesses a non-compliance after 10 days. 2.1.3 - There is nothing for an audit team to audit against. We suggest dropping this level.	Levels of noncompliance have been rewritten.
003-C2,2		
003-C2,3		
003-C2,4		

Name	Gary Campbell	
Entity	MAIN	
Ballot:	No	
General Comments		
003-R1	r1.2 This is a very vague and use less statement. I do not think it should be contained in the standard.	The requirement has been clarified.
003-R2		
003-R3		
003-R4		
003-R5		
003-R6		
003-M1	Suggest changing the introductory sentence to the measures to: "The Responsible Entity shall have the following to demonstrate................"	This is basically what the introductory statement says as it applies to each individual standard.
003-M2		
003-M3		
003-M4		
003-M5		
003-M6		
003-C1,1		
003-C1,2		
003-C1,3		
003-C1,4		
003-C2,1	2.1.1 What good does it do to go back in history and look for holes in the designation of a senior manager. It is going to be difficult. You would think that normal replacement of an indiivdual would also mean the taking over of responsibilites. I think that in checking for compliance it would be more benefical to check to ensure that a currently active senior manager is designated. 2.1.2 R1.4 requires that the policy to be reviewed annually. This needs to be corrected. 2.1.3 I did not find a requiremetn which addressed the content of this level of non-compliance, it therefore should be eliminated, unles you are refering to exceptions then this level should say "Exceptions from requirements ...." instead of	Levels of noncompliance have been rewritten.

	Deviations. Additionally, the exception only requires annual review, I did not see the 30 day requirement. 2.1.4 Change " A program ...." to " A Information Protection Program to ....", it makes it clearer.	
003-C2,2	2.2.4 The usage of the wording "critical syber information" should be "critical cyber assets" as stated in the requirement to be consistent and not infur other things.	Levels of noncompliance have been rewritten.
003-C2,3		
003-C2,4	2.4.3 I do not know What I should be looking for. Any level of compliance should clearly define its intent by being specific. Which requirement are we covering.	Levels of noncompliance have been rewritten.

CIP-003 Drafting Team Responses to Comments

Name	Linda Campbell	
Entity	FRCC	
Ballot:	No	
General Comments		
003-R1	R1.2 Please clarify what is meant by the responsible entity verifying that its written policy is "available as needed," by who?	This has been clarified in the standard.
003-R2		
003-R3	R3.1 uses the term "senior management" which is very broad when R.2. requires a specific senior manager. If this should be the senior manager, change the wording. If you wish some other management official to review and approve exceptions previously approved by the designated senior manager, then state at what level of management should have this oversight responsibility.	The standard has been revised fpr clarity.
003-R4	R4.2 "sensitivity" alludes to the Responsible Entity have different levels of protection/classification for Critical Cyber Assets. The requirement should state the the Responsible Entity shall have a written classifcation control policy regarding Critical Cyber Assets.	The standard requires that this information be classified in accordance with its level of sensitivity. It is the responsibility of each entity to determine the best way to accomplish this.
	R4.3 wants to annually assess and document "classification controls." This should be deleted, unless the changes stated above for R4.2 have been incorporated in CIP-003-1.	The requirement has been revised to refer to the assessment and documentation of adherence to its information protection program.
003-R5		
003-R6	R6 Change control… Typically a Change Control process includes formal signoffs but not testing procedures. If it is your intent to have documented testing procedures, then specifically include this in the verbiage and reflect in the measures, such as The Responsible… methodical processes of change control and testing for modifying…... Also provide some guidance in your FAQ's for what the testing procedures should include. R6.1 Clarify by changing to: The responsible entity shall review its processes for managing change to and testing modification or changes to Critical Cyber Assets at least annually. However, if it is only your intent to have a signoff authority, then there is no need to review the "testing process" mentioned in R6.1 above. R6.3 Change Management Procedures typically would identify/list all components of a system that are being changed or added and control their promotion to production. Please clarify what additional information or activity the supporting "configuration management activities" must provide.	R6 has been modified. The change control program must address all relevant environments -- production or non-production -- as defined by Responsible Entity using reasonable business judgment.

CIP-003 Drafting Team Responses to Comments

003-M1	This is not a measurement, a measurement would be that the responsible entity has a	This measures has been clarified to align with the
003-M2	This measurement restates the purpose of the requirement and should only offer what will be measured. This measurement also lack any reference to designated delegate(s). The measurement should be: Maintan documentation of the assignment of, and changes to, the Responsible Entity's senior manager or degelate(s).	The measures have been rewritten to refer back to the requirements.
003-M3	Measurement should read: Documentation of Responsible Entity's approved exceptions, including compensating measures or risk acceptance, and annual reviews.	The measures have been rewritten to refer back to the requirements.
003-M4	Measurement should read: Documentation of Responsible Entity's program to identify, classify, and protect information relating to Critical Assets, including documentation of annual assessments.	The measures have been rewritten to refer back to the requirements.
003-M5	Measurement should read: Documentation of Responsible Entity's written policy for the management of access to information list in R.5 and documentation of annual reviews.	The measures have been rewritten to refer back to the requirements.
003-M6	M6 Make this measure consistent with the final requirements. If no requirements are changed then modify to : The Responsible Entity’s written processes of change control, documented approval authority for testing of modification or changes to Critical Cyber Assets, approved testing results, and documentation of annual reviews.	The measures have been rewritten to refer back to the requirements.
003-C1,1	In the applicability section 4.1.10 and 4.1.11, RRO's and NERC are included. Who has the monitoring responsibility for a RRO or NERC? Add Self-Certification and Audit information to this section. Proposed language would be: 1.1. Complaince Monitoring Responsibility Regional Reliability Organization. 1.1.1. The Compliance Monitor will request a self-certification annually. 1.1.2. The Compliance Monitor will perform an audit at least once every three (3) calendar years.	NERC will monitor the RROs and a third party without vested interest in the outcome will monitor NERC. Self-certification has been added under "Additional Compliance Information."
003-C1,2		
003-C1,3	To complement a audit every three years, the data retention period should be 3 years.	The data retention period matches the requirement. Only the compliance monitor is required to keep records of an audit for 3 years. The Responsible Entity may choose to retain data longer.
003-C1,4		
003-C2,1	D2.1.2 add “or does not address all requirements of NERC CIP-002 through CIP-009 Standards D2.1.3 This should read- Exceptions (rather than Deviations) from written cyber security policy have not been documented…. In addition, there is no requirement or measurement that an exception be documented within thirty days.	2.1.2 was removed and 2.1.3 corrected.

003-C2,2	D2.2. assumes a policy exists. An additional item should be added that a written cyber security polciy exists. This section also assumes that the Responsible Entity is complaint with R4- Information Protection. D2.2.2. If an exception is not document nor aproved by the senior manager or delegate(s), how is the compliance monitor expected to find the exception? D2.2.3 Change to: Access privileges to information associated with Critical Cyber Assets have not been reviewed……	The policy must exist pursuant to R1. If a written policy does not exist, a level 4 violation is incurred. Through interviews and other fact-finding efforts, a compliance monitor may discover evidence of undocumented exceptions. Additionally, should an entity experience an outage due to an undocumented exception, this would be yet another avenue of discovery. This section has been modified.
003-C2,3	The policy must exist pursuant to R1. If a written policy does not exist, a level 4 violation is incurred.	The policy must exist pursuant to R1. If a written policy does not exist, a level 4 violation is incurred.
003-C2,4	D2.4.5 To be consistent with the requirement, change to -Access privileges to information associated with Critical Cyber Assets have not been reviewed in the last calendar year. D2.4.6 Delete, does not match any stated requirement in this standard. Perhaps belongs in CIP-004-1, thought seems adequately covered there already by other non-compliance sentences.	This section has been deleted.

CIP-003 Drafting Team Responses to Comments

Name	Roger Champagne	
Entity	Hydro-Québec TransÉnergie	
Ballot:	No	
General Comments		
003-R1	R1 should be rewritten to "each Entity shall have a Cyber Security Policy that includes the following." NERC Standards should be focused on Reliability not management structure.	Please see responses to Ray A"Brial, Central Hudson Gas & Electric Corp.
003-R2	change R2 to "The Responsible Entity shall assign a senior manager or delegate(s) with responsibility"	
003-R3	Change R3 to "Exceptions - Instances where the Responsible Entity accepts non-conformance with its cyber security policy". The requirement to document non-conformance with an Entity's cyber security policy is sensible, but the requirement for a senior manager to approve all of those non-conformances is not. Some non-conformances may occur for reasons that are understood and knowingly tolerated for valid reasons. One could reasonably require the senior manager concerned to approve these, which effectively signals informed consent. However, there may be instances where a non-conformance occurs which represents an error that is not acceptable to the Entity concerned one which needs correcting rather than approval.	
003-R4	The minimum should not include everything. Remove ", and any related security information". Replace Requirement 4.3 with words from Requirement 5.2	
003-R5	Add R5.1.4 : Every Asset (or list of assets) should have one owner. Rational By experience, one person should be responsible for an asset. If there is a list of persons responsible, no one is responsible!. A list of persons could be designated for authorizing access, but we need only one person responsible of that asset.	
003-R6	R6 should move to CIP007 otherwise the Drafting team to clarify its intent for including it here.	
003-M1		
003-M2		
003-M3		
003-M4		
003-M5		

003-M6 Move to CIP007 since R6 was moved to CIP007

003-C1,1

003-C1,2

003-C1,3

003-C1,4 This is confusing. We believe this refers to non-conformance with the Entity's cyber security policy.

003-C2,1 Compliance statement 2.1.1 imposes a requirement that is not identified in the requirements section. Specifically, 2.1.1 effectively imposes a requirement that the gap in designating a senior management representative be less than 10 days, which is not specified in the requirements section. Ten days was never specified before this.

Requirement R1.4 requires annual review of the cyber security policy. This is not consistent with compliance statement 2.1.2 which suggests that an entity that reviews its policy every three years would be fully compliant.

Compliance statement 2.1.3 imposes a requirement that is not identified in the requirements section.

003-C2,2

003-C2,3

003-C2,4 Compliance statement 2.4.3 should be revised to more clearly refer to a program for the identification and classification of information about Critical Cyber Assets.

CIP-003 Drafting Team Responses to Comments

Name	Larry Conrad	
Entity	Cinergy	
Ballot:	No	
General Comments	These standards include numerous and extensive documentation and review requirements. Standardize reviews to an annual requirement, with updates required within 90 days of the change occurring.	The update and retention periods reflect industry consensus.
003-R1		
003-R2	Comment relates to consistency between Section D (non compliance) and R2. D.2.1.1: Level 1 non compliance is stated if a senior manager “was not designated for 10 or more calendar days…” The corresponding requirement R2.2. indicates that the designated senior manager must be documented within 30 calendar days of the effective date. If the requirement is that the senior manager must be documented within "__" number of days, then there should not be compliance violations at any level for a time period less than the requirement states. In general annual reviews are required, with updates required within 90 days of the change occurring. Several required timeframes are presently shorter than this and should be increased so that all timeframes throughout the standard are consistent and reasonable, and to make compliance more manageable: B.R2.2 Documentation of the senior manager leading CIP adherence must be updated within 30 days of the effective date of the change. 90-day update should be acceptable.	This level of non-compliance has been revised to address the requirements in R2. The update and retention periods reflect industry consensus.
003-R3		
003-R4		
003-R5		
003-R6		
003-M1		
003-M2		
003-M3		
003-M4		
003-M5		
003-M6		
003-C1,1		

CIP-003 Drafting Team Responses to Comments

003-C1,2

003-C1,3

003-C1,4

003-C2,1

003-C2,2

003-C2,3

003-C2,4

CIP-003 Drafting Team Responses to Comments

Name	Larry Conrad	
Entity	ECAR Critical Infrastructure Protection Panel	
Ballot:	No	
General Comments	We would like to see something in the FAQ's for designating a temporary Senior Manager Responsible (R2). In the compliance portion of the standard, only 10 days is give to name a Senior Manager responsible, it will likely take more time than that (and probably more than 30 days) to name the responsible person when there is a staff change.	This level of non-compliance has been revised to address the requirements in R2
003-R1		
003-R2	R2.2 We feel this is in conflict with Compliance section 2.1.1. The requirement states that changes to senior management responsible must be within 30 days, but in the compliance section it is a level 1 violation if it not done in 10 days.	This requirement has been revised.
003-R3		
003-R4		
003-R5		
003-R6		
003-M1		
003-M2		
003-M3		
003-M4		
003-M5		
003-M6		
003-C1,1		
003-C1,2		
003-C1,3		
003-C1,4		

CIP-003 Drafting Team Responses to Comments

003-C2,1

003-C2,2

003-C2,3

003-C2,4

CIP-003 Drafting Team Responses to Comments

Name	Theodore Creedon, P.E.	
Entity	Creedon Engineering	
Ballot:	Yes	
General Comments	Does not recognize the extensive engineering required to implement this standard.	These requirements represent a consensus of the industry, as gauged by comments the drafting team received. They are a set of minimum requirements that must be complied with to protect Critical Cyber Assets. Responsible Entities may exceed the minimum requirements if they deem it appropriate to do so.
003-R1		
003-R2	Change "manager" to "engineering manager". Needs to be a PE or equivalent. The technical difficulty of implementing this standard required engineering not (financial) management.	The Responsible Entity retains the flexibility to determine the appropriate expertise for its cyber security program leadership.
003-R3		
003-R4		
003-R5		
003-R6		
003-M1		
003-M2		
003-M3		
003-M4		
003-M5		
003-M6		
003-C1,1		
003-C1,2		
003-C1,3		
003-C1,4		
003-C2,1		

CIP-003 Drafting Team Responses to Comments

003-C2,2

003-C2,3

003-C2,4

CIP-003 Drafting Team Responses to Comments

Name	Joel De Granda
Entity	Florida Power and Light
Ballot:	Yes

General Comments

003-R1

003-R2

003-R3

003-R4

003-R5

003-R6

003-M1

003-M2

003-M3

003-M4

003-M5

003-M6

003-C1,1

003-C1,2

003-C1,3

003-C1,4

003-C2,1

003-C2,2

003-C2,3

003-C2,4

CIP-003 Drafting Team Responses to Comments

Name	Richard Engelbrecht	
Entity	RGE	
Ballot:	No	
General Comments		
003-R1	R1 should be rewritten to "each Entity shall have a Cyber Security Policy that includes the following." NERC Standards should be focused on Reliability not management structure.	Please see responses to Ray A'Brial, Central Hudson Gas & Electric Corp.
003-R2	change R2 to "The Responsible Entity shall assign a senior manager or delegate(s) with responsibility"	
003-R3	Change R3 to "Exceptions - Instances where the Responsible Entity accepts non-conformance with its cyber security policy". The requirement to document non-conformance with an Entity’s cyber security policy is sensible, but the requirement for a senior manager to approve all of those non-conformances is not. Some non-conformances may occur for reasons that are understood and knowingly tolerated for valid reasons. One could reasonably require the senior manager concerned to approve these, which effectively signals informed consent. However, there may be instances where a non-conformance occurs which represents an error that is not acceptable to the Entity concerned one which needs correcting rather than approval.	
003-R4	The minimum should not include everything. Remove ", and any related security information". Replace Requirement 4.3 with words from Requirement 5.2	
003-R5	Remove R5 because it overlaps Requirement 4 in CIP004 and Requirement 6.1 in CIP007. This overlap is confusing. It is not clear how Requirement 4 in CIP003 is different from this Requirement.	
003-R6	R6 should move to CIP007 otherwise the Drafting team to clarify its intent for including it here.	
003-M1		
003-M2		
003-M3		
003-M4		
003-M5	Remove M5 since R5 was removed	
003-M6	Move to CIP007 since R6 was moved to CIP007	
003-C1,1		

CIP-003 Drafting Team Responses to Comments

003-C1,2

003-C1,3

003-C1,4 This is confusing. We believe this refers to non-conformance with the Entity's cyber security policy.

003-C2,1 Compliance statement 2.1.1 imposes a requirement that is not identified in the requirements section. Specifically, 2.1.1 effectively imposes a requirement that the gap in designating a senior management representative be less than 10 days, which is not specified in the requirements section. Ten days was never specified before this.

Requirement R1.4 requires annual review of the cyber security policy. This is not consistent with compliance statement 2.1.2 which suggests that an entity that reviews its policy every three years would be fully compliant.

Compliance statement 2.1.3 imposes a requirement that is not identified in the requirements section.

Remove 2.2.3 since M5 was removed.

003-C2,2

003-C2,3

003-C2,4 Compliance statement 2.4.3 should be revised to more clearly refer to a program for the identification and classification of information about Critical Cyber Assets.

2.4.5 and 2.4.6 should be removed since they depend on M5, which we removed

CIP-003 Drafting Team Responses to Comments

Name	Ken Fell	
Entity	New York ISO	
Ballot:	No	
General Comments		
003-R1	R1 should be rewritten to "each Entity shall have a Cyber Security Policy that includes the following." NERC Standards should be focused on Reliability not management structure.	Please see responses to Ray A'Brial, Central Hudson Gas & Electric Corp.
003-R2	change R2 to "The Responsible Entity shall assign a senior manager or delegate(s) with responsibility"	
003-R3	Change R3 to "Exceptions - Instances where the Responsible Entity accepts non-conformance with its cyber security policy". The requirement to document non-conformance with an Entity's cyber security policy is sensible, but the requirement for a senior manager to approve all of those non-conformances is not. Some non-conformances may occur for reasons that are understood and knowingly tolerated for valid reasons. One could reasonably require the senior manager concerned to approve these, which effectively signals informed consent. However, there may be instances where a non-conformance occurs which represents an error that is not acceptable to the Entity concerned one which needs correcting rather than approval.	
003-R4	The minimum should not include everything. Remove ", and any related security information". Replace Requirement 4.3 with words from Requirement 5.2	
003-R5	Remove R5 because it overlaps Requirement 4 in CIP004 and Requirement 6.1 in CIP007. This overlap is confusing. It is not clear how Requirement 4 in CIP003 is different from this Requirement.	
003-R6	R6 should move to CIP007 otherwise the Drafting team to clarify its intent for including it here.	
003-M1		
003-M2		
003-M3		
003-M4		
003-M5	Remove M5 since R5 was removed	
003-M6	Move to CIP007 since R6 was moved to CIP007	
003-C1,1		

CIP-003 Drafting Team Responses to Comments

003-C1,2

003-C1,3

003-C1,4 This is confusing. We believe this refers to non-conformance with the Entity's cyber security policy.

003-C2,1 Compliance statement 2.1.1 imposes a requirement that is not identified in the requirements section. Specifically, 2.1.1 effectively imposes a requirement that the gap in designating a senior management representative be less than 10 days, which is not specified in the requirements section. Ten days was never specified before this.

Requirement R1.4 requires annual review of the cyber security policy. This is not consistent with compliance statement 2.1.2 which suggests that an entity that reviews its policy every three years would be fully compliant.

Compliance statement 2.1.3 imposes a requirement that is not identified in the requirements section.

Remove 2.2.3 since M5 was removed.

003-C2,2

003-C2,3

003-C2,4 Compliance statement 2.4.3 should be revised to more clearly refer to a program for the identification and classification of information about Critical Cyber Assets.

2.4.5 and 2.4.6 should be removed since they depend on M5, which we removed

CIP-003 Drafting Team Responses to Comments

Name	Francis Flynn	
Entity	National Grid USA	
Ballot:	No	
General Comments		
003-R1	R1 should be rewritten to "each Entity shall have a Cyber Security Policy that includes the following." NERC Standards should be focused on Reliability not management structure.	Please see responses to Ray A'Brial, Central Hudson Gas & Electric Corp.
003-R2	change R2 to "The Responsible Entity shall assign a senior manager or delegate(s) with responsibility"	
003-R3	Change R3 to "Exceptions - Instances where the Responsible Entity accepts non-conformance with its cyber security policy". The requirement to document non-conformance with an Entity's cyber security policy is sensible, but the requirement for a senior manager to approve all of those non-conformances is not. Some non-conformances may occur for reasons that are understood and knowingly tolerated for valid reasons. One could reasonably require the senior manager concerned to approve these, which effectively signals informed consent. However, there may be instances where a non-conformance occurs which represents an error that is not acceptable to the Entity concerned one which needs correcting rather than approval.	
003-R4	The minimum should not include everything. Remove ", and any related security information". Replace Requirement 4.3 with words from Requirement 5.2	
003-R5	Remove R5 because it overlaps Requirement 4 in CIP004 and Requirement 6.1 in CIP007. This overlap is confusing. It is not clear how Requirement 4 in CIP003 is different from this Requirement.	
003-R6	R6 should move to CIP007 otherwise the Drafting team to clarify its intent for including it here.	
003-M1		
003-M2		
003-M3		
003-M4		
003-M5	Remove M5 since R5 was removed	
003-M6	Move to CIP007 since R6 was moved to CIP007	
003-C1,1		

003-C1,2

003-C1,3

003-C1,4 This is confusing. We believe this refers to non-conformance with the Entity's cyber security policy.

003-C2,1 Compliance statement 2.1.1 imposes a requirement that is not identified in the requirements section. Specifically, 2.1.1 effectively imposes a requirement that the gap in designating a senior management representative be less than 10 days, which is not specified in the requirements section. Ten days was never specified before this.

Requirement R1.4 requires annual review of the cyber security policy. This is not consistent with compliance statement 2.1.2 which suggests that an entity that reviews its policy every three years would be fully compliant.

Compliance statement 2.1.3 imposes a requirement that is not identified in the requirements section.

Remove 2.2.3 since M5 was removed.

003-C2,2

003-C2,3

003-C2,4 Compliance statement 2.4.3 should be revised to more clearly refer to a program for the identification and classification of information about Critical Cyber Assets.

2.4.5 and 2.4.6 should be removed since they depend on M5, which we removed

CIP-003 Drafting Team Responses to Comments

Name	Greg Fraser	
Entity	Manitoba Hydro	
Ballot:	No	
General Comments	Labeling for Part A is missing.	Labeling has been addressed
	Introduction 4.2.3 should read the same as in CIP-009-1 which is: "Responsible Entities that, in compliance with Standard CIP-002, identify that they have no Critical Cyber Assets.	This has been corrected.
	CIP-005 includes Non-Critical Cyber Assets in R1.4 and Cyber Assets in R1.5 which need to be managed as Critical Cyber Assets including documentation (lists), access controls, etc. CIP-003 should make it clear that these additional Cyber Assets must also be managed as Critical Cyber Assets, if they can affect the security of Critical Cyber Assets.	CIP-005, CIP-006, and CIP-007 include references back to CIP-003 for this purpose.
003-R1	In R1.3 add delegates "…relationships and processes including delegates…".	This language has been removed.
	R1.3 may be more appropriate under R2 Leadership rather R1 Policy.	The requirements in R1 have been revised.
	The Requirement in R1.4 that the cyber security policy be reviewed annually does not align with the compliance requirement in Level 1 Non-Compliance 2.1.2, which indicates a three year periodicity.	This has been corrected.
003-R2	R2.3 contains two different concepts "designated delegates" and "policy exceptions". The "policy exceptions" concept should be moved into R3 Exceptions. Then R2.3 could be changed to introduce the concept of designated delegate for all items including changes, not just policy exceptions, etc.	R2.3 highlights one of the general duties included in R2. R3.1 specifies the window within which documentation of exceptions must be completed. R3.3 relates to annual review of all exceptions.
003-R3	R3 does not indicate how long an entity has to document an exemption, but Level 1 Non-Compliance, 2.1.3, indicates that an entity only has thirty calendar days. This 30 day requirement should be worked into R3 so these align.	This has been corrected.
	R3.2 change "or" to "and" as both compensating measures and risk acceptance should be included.	While it is true that the implementation of a compensating measure may also include a certain degree of risk acceptance, this may not always be the case. Hence the inclusion of the word "or" rather than "and".
003-R4	In R4.1 add Critical Cyber Asset inventories in addition to Critical Asset inventories as identified in CIP-002-1.	This has been corrected.
	In R4.3 remove the words "at least" as they are redundant.	Consistent with verbiage used in other CIP standards, the verbiage allows the Responsible Entities to choose more frequent assessment periods.
	In R4.3 change the words "assess and document" to "review".	Assessing the adherence to this requirement is quite

		different from documenting the results.
003-R5	R5 should be revised to add “Critical Cyber Assets and” prior to the words “information associated with”. Access Control should apply to both the asset and asset information.	Access to Critical Cyber Assets is covered in CIP-005.
003-R6	Consider changing heading to "Change Control & Testing" since the sub-requirements include testing or alternately explain that change control includes testing control.	Heading has been changed to “Change Control and Configuration Management”.
	Backup procedures should be required during testing. This requirement may be more appropriate in one of the another cyber security standards	Testing is covered in CIP-007.
	R6.2 sign-off should be required for all parts of change management and not just the testing portion.	R6 has been modified. It now requires Responsible Entities to establish and document a process of change control and configuration management.
003-M1		
003-M2	M2 does not adequately cover all items in Requirement R2.	The measures have been rewritten to refer back to the requirements.
003-M3	Remove the word "or".	The measures have been rewritten to refer back to the requirements.
003-M4	M4 does not address all items in Requirement R4. A "written and approved program" is not specifically included in R4.	The measures have been rewritten to refer back to the requirements.
003-M5	Change to "…access to asset information…".	The measures have been rewritten to refer back to the requirements.
003-M6	Remove "and assessment" as this is a part of the requirements.	The measures have been rewritten to refer back to the requirements.
003-C1,1		
003-C1,2		
003-C1,3		
003-C1,4		
003-C2,1	In 2.1.2 change three calendar years to one calendar year match R1. This noncompliance item would seem to be more approporiate in level 2.	The levels of noncompliance have been rewritten.
003-C2,2	2.2.3 does not line up with R5.1.3 as authorizing personnel.	The levels of noncompliance have been rewritten.
	2.24 is redundant with 2.4.5.	
003-C2,3		
003-C2,4	2.4.5 could be clearer as "Authorizing personnel have not been…".	The levels of noncompliance have been rewritten.
	2.4.6 access revocations/changes not in the requirements of this standard.	

CIP-003 Drafting Team Responses to Comments

Name	Jerry Freese	
Entity	American Electric Power	
Ballot:	No	
General Comments	Based on the expanded scope set forth in CIP-002 R1 for the Critical Assets and the subsequently expanded scope of the Critical Cyber Assets and the Electronic Security Perimeter, it would be impractical and infeasible to meet the obligations set forth in this requirement.	CIP-002 has been changed.
003-R1		
003-R2		
003-R3		
003-R4		
003-R5		
003-R6	As an internal matter, our PCIS database would be the ideal tool for most efficiently documenting our compliance (this has worked very well to satisfy NERC P&C maintenance compliance audits). This would include documenting our installed base of station cyber security sensitive assets (e.g. equipment types, models, nameplate info, firmware/software version, serial #'s etc) , and tracking associated security task/work status and "changes". It is also ideal for generating canned reports that summarize this activity. However, to achieve this would involve some programming and augmentation of PCIS.....The budgeting process for 2006 approved IT projects was completed in early June. Therefore, if PCIS programming changes need to occur in 2006, we would need to work around the customary/planned process.	The Implementation Plan is intended to address this issue.
003-M1		
003-M2		
003-M3		
003-M4		
003-M5		
003-M6		
003-C1,1		
003-C1,2		
003-C1,3		

CIP-003 Drafting Team Responses to Comments

003-C1,4

003-C2,1

003-C2,2

003-C2,3

003-C2,4

CIP-003 Drafting Team Responses to Comments

Name	Edwin C. Goff III
Entity	Progress Energy
Ballot:	No

General Comments		
003-R1		
003-R2		
003-R3		
003-R4		
003-R5	The requirement should be changed to indicate that the RE shall maintain a process for authorizing access to critical assets: The process should take into consideration the need for both physical and cyber access controls to ensure only personnel who have been authorized and trained have access to critical assets. Access privileges should be reviewed at least annually to ensure access is appropriate and correspond to the entity's needs.	Physical and electronic access controls are covered in other CIP standards. The requirement here is to protect information associated with Critical Cyber Assets. While this may include physical and/or electronic security, it is not part of this requirement.
003-R6	States "Responsible entity shall implement an approval authority responsible for sign-off on testing results prior to a system being promoted to operate in in a production environment." Suggest this be modified to allow an approval process (rather than authority) such that if would be acceptable if at least two individuals within the workgroup close to the process actually verify and attest to successful testing prior to promoting to production. This would allow flexibility and efficiency within organizations to have a second set of eyes close to the work verify that proper pre-production testing had been completed rather than implementing a separate approval authority that would add unnecessary overhead.	R6 has been modified. It now requires Responsible Entities to establish and document a process of change control and configuration management.
003-M1		
003-M2		
003-M3		
003-M4		
003-M5		
003-M6		
003-C1,1		
003-C1,2		

CIP-003 Drafting Team Responses to Comments

003-C1,3

003-C1,4

003-C2,1

003-C2,2

003-C2,3

003-C2,4

CIP-003 Drafting Team Responses to Comments

Name	Kenneth Goldsmith	
Entity	Alliant Energy	
Ballot:	No	
General Comments		
003-R1		
003-R2	This requirement (or R1.3) shoudl have language added that clarifies that management responsibility in various areas of cyber security can be delegated within the organization as defined in hte responsible entity's cyber security policy. While the need for a single senior manager to be designated as having overall responsibility is understandable, it should be clear that all other aspects of control and accountability can be delegated as necessary, and as they are defined, by each organization.	The designated senior manager is the person responsible overall for the implementation and adherence to CIP-002 through CIP-009. How this manager goes about ensuring the implementation and adherence to these standards is within the scope of his or her responsibilities. If the senior manager wishes to delegate some responsibilities in order to accomplish the work, there is no requirement prohibiting this action. The senior manager would be responsible for any implementation and adherence actions by the delegates.
003-R3		
003-R4		
003-R5		
003-R6		
003-M1		
003-M2		
003-M3		
003-M4		
003-M5		
003-M6		
003-C1,1		
003-C1,2		
003-C1,3		
003-C1,4		

CIP-003 Drafting Team Responses to Comments

003-C2,1

003-C2,2

003-C2,3

003-C2,4

CIP-003 Drafting Team Responses to Comments

Name	Kathleen Goodman
Entity	ISO New England Inc
Ballot:	No

General Comments	We believe that CIP002 through CIP009 go beyond the intended scope of the original SAR for 1300. The final SAR for 1300, dated March 8, 2004, clearly states that the U/A 1200 is the basis for development of a permanent standard to replace it. The intent of both U/A 1200 and SAR 1300 is to establish a minimum set of cyber security best practices as a standard baseline for general cyber protection of a reliable BES. References to organizational relationships and decision-making processes are outside of the scope of SAR 1300. Within the intent of a minimum baseline, consistent across responsible entities, the focus should remain on the Critical Cyber Assets themselves.	The SAR for 1300 included the following statement: "This cyber security standard shall primarily focus on electronic systems, which include hardware, software, data, related communications networks, control systems as they impact electric system operations, and personnel." This statement includes process control systems, distributed control systems, or electric systems installed in generating stations, switching stations and substations. Therefore, the drafting team does not believe it has extended the scope of the SAR. CIP-002--CIP-009 provide a minimum set of requirements that must be complied with rather than a set of best practices. Reference to organzational relationships and decision-making processes have been removed.
003-R1	Remove the words that say "...defines a structure of relationships and decision-making processes that identify and..." R1.2 - replace "written" with "documented." Regarding comments above, remove R1.3.	See response, above.
003-R2		
003-R3		
003-R4		
003-R5	Remove "...information associated with...".	R5 hs been modified.
003-R6	Remove the word "any" in R6.3.	R6 has been modified and the subrequirements removed.
003-M1	Replace "written" with "documented." Remove the word "relationships."	The measures have been reworded to refer back to the requirements.
003-M2	Replace "written" with "documented."	The measures have been reworded to refer back to the requirements.
003-M3	Replace "written" with "documented."	The measures have been reworded to refer back to the requirements.
003-M4	Replace "written" with "documented."	The measures have been reworded to refer back to the requirements.
003-M5	Replace "written" with "documented."	The measures have been reworded to refer back to the

		requirements.
003-M6	Replace "written" with "documented." Remove the word "assessment" as it is open to too much interpretation.	The measures have been reworded to refer back to the requirements.
003-C1,1		
003-C1,2		
003-C1,3	It is not clear when you mean documents, records, or data. These are three distinct items and should not be referenced interchangeably. Please clarify.	This section has been revised for clarity.
003-C1,4		
003-C2,1	2.1.1 Change to "designated within thirty." 2.1.2 Change to "last calendar year." Change to "requirements of cyber."	This level of non-compliance has been revised to address the requirements in R2. This level of non-compliance has been removed. This language no longer exists in this section of the standard.
003-C2,2		
003-C2,3	The wording has been modified.	The wording has been modified.
003-C2,4		

CIP-003 Drafting Team Responses to Comments

Name	Tim Hattaway
Entity	Alabama Electric Cooperative
Ballot:	Yes

General Comments

003-R1

003-R2

003-R3

003-R4

003-R5

003-R6

003-M1

003-M2

003-M3

003-M4

003-M5

003-M6

003-C1,1

003-C1,2

003-C1,3

003-C1,4

003-C2,1

003-C2,2

003-C2,3

003-C2,4

CIP-003 Drafting Team Responses to Comments

Name	Jerry Heeren	
Entity	MEAG Power	
Ballot:	No	
General Comments	This section needs to address jointly owned assets. See R5.	Responsibility for jointly owned assets would have to be negotiated between the owners of those assets. It is not the intent of this standard to address business agreements between entities.
003-R1		
003-R2		
003-R3		
003-R4		
003-R5	A jointly own asset should require all entities in the relationship to be responsible for the maintenance of the personnel list for the asset.	See response above.
003-R6		
003-M1		
003-M2		
003-M3		
003-M4		
003-M5		
003-M6		
003-C1,1		
003-C1,2		
003-C1,3		
003-C1,4		
003-C2,1		
003-C2,2		
003-C2,3		
003-C2,4		

CIP-003 Drafting Team Responses to Comments

Name	Peter Henderson	
Entity	Independent Electricity System Operator (IESO)	
Ballot:	No	
General Comments	The requirement to document non-conformance with an Entity's cyber security policy is sensible, but the requirement for a senior manager to approve all of those non-conformances is not. Some non-conformances may occur for reasons that are understood and knowingly tolerated for valid reasons. One could reasonably require the senior manager concerned to approve these, which effectively signals informed consent. However, there may be instances where a non-conformance occurs which represents an error that is not acceptable to the Entity concerned one which needs correcting rather than approval. Consider the wording, "Instances where the Responsible Entity accepts non-conformance with its cyber security policy….." .	The language of the requirement has been modified to address delegation of the authorization of exceptions. It is expected that security problems will be addressed expeditiously. If a Responsible Entity chooses to leave a security problem unresolved which causes a violation of the Responsible Entity's cyber security policies, than an exception, meeting the requirements of CIP-003, R3 must be written and duly authorized.
003-R1	R1 should be rewritten to "each Entity shall have a Cyber Security Policy that includes the following." NERC Standards should be focused on Reliability not management structure.	Part of any security program that addresses the reliability of the electric grid is having a strong management understanding of the issues involved. To that end, the drafting team feels that any good Cyber Security policy should include statements that indicate that management is in support of the policy and generally indicates how this support is structured. Generally, corporate policies have statements in them indicating that the senior management officials endorse the policy and expect all employees to follow them.
003-R2	Change R2 to "The Responsible Entity shall assign a senior manager or delegate(s) with responsibility"	This requirement is similar to Sarbanes-Oxley requirements. One senior manager needs to be responsible for ensuring that the requirements of these cyber security standards are being followed.
003-R3		
003-R4	1. R5 and R4 should be combined. Both talk about requirements to protect information about Critical Cyber Assets. 2. In R4.3, it is unclear what is meant by the phrase, "cyber security protection controls". This could be taken as a reference to the sum-total of controls in place to ensure compliance with CIP-002 through CIP-009. If this is actually intended, the requirement to assess and document these controls annually appears to overlap many similar requirements throughout the standards (eg. the requirements in R1.3, R5.2, R5.3, and R6.1 of CIP-003, R3 and R4, of CIP-005, R7 of CIP-006, and R9 of CIP-007) 3. The minimum should not include everything. Remove ", and any related security information".	1. R4 addresses the identification and classification of information associated with Critical Cyber Assets. R5 addresses the requirement for controls for managing access to information associated with Critical Cyber Assets. These are separate requirements and have been kept separate for clarity. 2. This language no longer exists in the current version of this standard. 3. Changed to "..security configuration information of cyber security assets.

003-R5	Requirements 5.1, 5.1.1, 5.1.2, and 5.1.3 are about managing access to the assets themselves, yet they appear as sub-bullets of a requirement to manage access to information about Critical Cyber Assets. This is confusing, particularly as there is no measure that relates to the management of access to the assets themselves.	This requirement has been clarified to address access to information associated with Critical Cyber Assets.
003-R6	1. R6.2 appears to require that testing be performed prior to promoting systems to production. It is unclear what the purpose and scope of that testing needs to be, and where those dimensions are documented. If this is a reference to testing required in CIP-007, this should be noted, or the reference to testing deleted in favour of a more thorough treatment in CIP-007. 2. In R6.3, it is unclear what is meant by the qualifier “supporting” when referring to configuration management activities. 3. R6.3 is redundant given the text of R6, and overlaps with the requirements of R6.2.	1. Testing requirements have been moved to CIP-007 2. These would be activities designed to identify, control, and document changes pursuant to the Responsible Entity’s change control processes. 3. R6 has been reworded and the subrequirements removed.
003-M1		
003-M2		
003-M3		
003-M4	Measures M4 and M5 should be reviewed in light of comment 1 on R4 & R5 above.	M4 and M5 have been revised to be in line with requirements.
003-M5	1. Measures M4 and M5 should be reviewed in light of comment 1 on R4 & R5 above. 2. M5 refers to a policy for management of access to information. There is no	See response above.
003-M6	Measure M6 should be reviewed in light of comments on R6 above.	See response above.
003-C1,1		
003-C1,2		
003-C1,3		
003-C1,4	Section 1.4 under “Compliance” is somewhat unclear. The text appears to suggest that a Responsible Entity that does not fulfill one or more of the Standard’s requirements should actually claim that it is fully compliant with the Standard if it has a properly documented exception to those requirements approved by the designated senior manager at the time of compliance reporting. Is this the intent?	You cannot write an exception to a NERC Standard. You may grant exceptions to your internal cyber security policy that implement these requirements. Duly authorized exceptions will not result in noncompliance.
003-C2,1	1. Requirement R 2.2 requires that changes to the designated senior manager must be documented within 30 days of the effective date. Compliance statement 2.1.1, however, states that an entity that fails to do so within 10 days is in non-compliance. This inconsistency should be resolved.	This level of non-compliance has been revised to address the requirements in R2.

	2. Compliance statement 2.1.1 imposes a requirement that is not identified in the requirements section. Specifically, 2.1.1 effectively imposes a requirement that the gap in designating a senior management representative be less than 10 days, which is not specified in the requirements section. 3. Requirement R1.4 requires annual review of the cyber security policy. This is not consistent with compliance statement 2.1.2 which suggests that an entity that reviews its policy every three years would be fully compliant. 4. Compliance statement 2.1.3 imposes a requirement that is not identified in the requirements section. corresponding requirement (R5 requires the establishment of a program).	
003-C2,2	1. Compliance statement 2.2.3 should refer to access privileges to information associated with Critical Cyber Assets to more clearly correspond to R5.2 and to avoid imposing a requirement to review access privileges to the Critical Cyber Assets themselves that is not identified in the Requirements section.	Levels of noncompliance have been rewritten.
003-C2,3	Levels of noncompliance have been rewritten.	Levels of noncompliance have been rewritten.
003-C2,4	1. Compliance statement 2.4.3 should be revised to more clearly refer to a program for the identification and classification of information about Critical Cyber Assets. 2. Compliance statement 2.4.5 appears to duplicate 2.2.3 but at a different level of non-compliance. 3. Compliance statement 2.4.6 imposes new requirements not specified in the Requirements section specifically to document access revocations and changes. The requirements only specify the need to confirm that access privileges that prevail at the time of review are appropriate, without reference to maintaining a history of how those privileges came about.	Levels of noncompliance have been rewritten.

CIP-003 Drafting Team Responses to Comments

Name	E. Nick Henery	
Entity	SMUD	
Ballot:	Yes	
General Comments	The Drafting Team will need to go through the Standard and assign responsibility to each function from the functional model like the Version 0 STD. For this Standard to enforceable the generic use of Responsible Entity is the same as the generic use of Control Area. Even if the Standard lists the different functions it leaves open the possibility of misinterpretation as to which function is truly responsible.	The Responsible Entities are clearly enumerated in the standard Section A, item 4.
003-R1		
003-R2		
003-R3		
003-R4		
003-R5		
003-R6		
003-M1		
003-M2		
003-M3		
003-M4		
003-M5		
003-M6		
003-C1,1		
003-C1,2		
003-C1,3		
003-C1,4		
003-C2,1		
003-C2,2		
003-C2,3		

003-C2,4

CIP-003 Drafting Team Responses to Comments

Name	Jack Hobbick	
Entity	Consumers Energy	
Ballot:	No	
General Comments	Consumers Energy has also submitted comments via the ECAR CIPP.	Please see responses to Larry Conrad, ECAR CIPP.
003-R1		
003-R2		
003-R3		
003-R4		
003-R5		
003-R6		
003-M1		
003-M2		
003-M3		
003-M4		
003-M5		
003-M6		
003-C1,1		
003-C1,2		
003-C1,3		
003-C1,4		
003-C2,1		
003-C2,2		
003-C2,3		
003-C2,4		

CIP-003 Drafting Team Responses to Comments

Name	Richard Kafka
Entity	Pepco Holdings, Inc.
Ballot:	No

General Comments		
003-R1	Does the phrase "structure of relationships" indicate that detailed organization charts are required? If yes, should they be included in the overall policy section, since policies do not change frequently?	This language has been removed from this standard.
003-R2		
003-R3	Must every emergency count as an exception that must be documented? Can certain predictable emergencies by provided for through policies? R.3.1 It is not clear whether this applies to any exception even after it is over (for instance, to assist in reviewing the entity's general application of exceptions), or only to exceptions that have lasted some period of time (and if so, then to what period).	R1.1 has been revised to address emergency situations.
003-R4		
003-R5		
003-R6	Please clarify "modifying". For example does it include relay setting changes?	Modifications to the environment do not include normal, daily operations. Change control and configuration management processes typically address a documented method for handling changes to hardware/software upgrades or vendor-pushed patches and the like.
003-M1		
003-M2		
003-M3		
003-M4		
003-M5		
003-M6		
003-C1,1		
003-C1,2		
003-C1,3		
003-C1,4		

CIP-003 Drafting Team Responses to Comments

003-C2,1	Requirements are listed in 2.1.1 and 2.2.1 (i.e. 10 days) that are not in requirement R2.	The levels of non-compliance have been rewritten.
003-C2,2		
003-C2,3		
003-C2,4	No apparent compliance for R6 or M6.	The levels of non-compliance have been rewritten.

CIP-003 Drafting Team Responses to Comments

Name	Tony Kroskey	
Entity	Brazos Electric Power Cooperative	
Ballot:	No	
General Comments	Subsection 4.2, should remove word "entities".	The word entities has been removed.
003-R1	R1.1, suggest changing word "address" to "comply with requirements". R1.2, available to who? R1.3, suggest changing text "this program" to "implementation of its cyber security policy".	The Responsible Entity's cyber security policy should address each of the requirements of the CIP-002 through CIP-009 to ensure compliance. R1.2 has been clarified. This has been revised.
003-R2		
003-R3		
003-R4		
003-R5		
003-R6		
003-M1		
003-M2		
003-M3		
003-M4		
003-M5		
003-M6		
003-C1,1		
003-C1,2		
003-C1,3		
003-C1,4		
003-C2,1		
003-C2,2		

003-C2,3

003-C2,4

Name	Carol Krysevig	
Entity	Allegheny Energy Supply Co. LLC	
Ballot:	No	
General Comments	D1.3.1 Revise sentence to state 'The Responsible Entity shall keep records of all reviews and assessments (including changes, when applicable) from the previous full calendar year.' D2.1.1 Add 'or changes to the senior manager' after 'A senior manager'. Change 'was' to 'were' at beginning of sentence. D2.1.1 and 2.1.3 These sections identify specific time periods that trigger levels of non-compliance that are more stringent than what the requirements specify. They should agree. D2.2.3 Add 'to the information related to Critical Cyber Assets' after 'Access privileges' at the beginning of the sentence. D2.2.4 Add 'asset' after 'critical cyber'. D2.3.1 Add 'or changes to the senior manager' after 'A senior manager'. Change 'was' to 'were' at beginning of sentence. D2.3.2 Add 'information related to' before 'Critical Cyber Assets'. The related requirement (R5.2) is somewhat vague; clarify. D2.3.3 Add 'information related to' before 'Critical Cyber Assets'. D2.3.4 The related requirement (R6) is somewhat vague; clarify. D2.4.4 How is this different from 2.4.2 this would be part of the cyber security policy. Possibly remove 2.4.4. D2.4.5 Add 'to the information related to Critical Cyber Assets' after 'Access authorizations'. D2.4.6 The related requirement (R5.3) is vague; clarify	The levels of noncompliance have been rewritten.
003-R1	R1.1. Can a broad policy statement that the Responsible Entity's cyber security policy shall comply with the NERC CIP-002 through CIP-009 Standards suffice or does the Entity's policy have to address specific items in the Standards? R1.2. - 'The Responsible Entity shall verify that its written cyber security policy is available as needed.' Available to whom, or for what? R1.3 What 'program' is this referencing? Should 'program' be changed to 'policy'? R1.4 - 'The Responsible Entity's cyber security policy shall be reviewed and approved annually.' Reviewed and approved by whom? The designated senior manager?	R1.1 Revised the wording to specify that the cyber security policy addresses the requirements in CIP-002 through CIP-009. The Responsible Entity retains flexibiity in how it chooses to write its policy. R1.2 has been revised to state that the cyber security policy is readily available to all personnel who have access to or are responsible for Critical Cyber Assets. R1.3 has been removed. Draft 3, R1.4 has been renumbered to R1.3 and revised for clarity.
003-R2		
003-R3		
003-R4	R4.1 - This could be a tremendous amount of information for a power station. Suggest at a minimum that 'floor plans' and 'equipment layouts' be removed or limited to assets defined	R4.1 is a minumum list of sensitive information associated with Critical Cyber Assets that must be protected. It

	under CIP-002-1, R1.1.1. and R1.1.2. R4.1 - Our preference is to remove R4.1 from the standard and add to the FAQ as examples of documents that may need protected. The requirement as stated is too burdensome. R4.2 should be modified to state 'The Responsible Entity shall classify and protect….'	respresents information that should not be released into the public domain if at all possible.
003-R5	R5.1.1 through R5.1.3- Is the intent of these items to document access to Critical Asset information or electronic/physical access to Critical Assets? Based on R5. it is the information only. Either revise by adding 'information' where applicable or move these items under CIP-005-1 and CIP-006-1. Also applies in the Levels of Noncompliance Section (2.2.3, 2.2.4, 2.3.3, 2.4.5., and 2.4.6.)	This has been revised to specify access to information related to Critical Cyber Assets.
003-R6		
003-M1		
003-M2	Add '(if applicable)' after 'and changes to'	All changes to the leadership as required in R2 must be documented.
003-M3	Add 'documentation supporting' before 'annual reviews.'	Measures have been rewritten to refer back to requirements.
003-M4	Clarification is needed as to whom should be approving program for the identification, classification and protection of information associated with Critical Cyber Assets. Requirement R4 does not specifically state approval of program is required.	Measures have been rewritten to refer back to requirements.
003-M5	Clarification is needed as to who should be approving program for the management of access to information. Requirement R5 does not specifically state approval of program is required. Also add 'associated with Critical Cyber Assets' after 'access to information' and revise the last portion of the sentence to state 'documentation supporting annuals reviews of the list of designated personnel, access privileges and process for controlling access privileges'.	Measures have been rewritten to refer back to requirements.
003-M6	Clarification is needed as to whom should be approving the processes of change control and configuration management, documented controls for testing and assessment of hardware and software, and documentation of annual reviews. Requirement R6 does not specifically state approvals of processes are required.	Measures have been rewritten to refer back to requirements.
003-C1,1		
003-C1,2		
003-C1,3		
003-C1,4		
003-C2,1		
003-C2,2		
003-C2,3		

003-C2,4

CIP-003 Drafting Team Responses to Comments

Name	John Lim
Entity	Con Edison
Ballot:	No

General Comments	CIP-003 should specifically require that Responsible Entities have a policy on information about critical assets in transit or in the custody of third parties.	This is covered in general in R5. Protection of information is the responsibility of the entity to which the information belongs.
003-R1		
003-R2		
003-R3	Change R3 to "Exceptions - Instances where the Responsible Entity accepts non-conformance with its cyber security policy". The requirement to document non-conformance with an Entity's cyber security policy is sensible, but the requirement for a senior manager to approve all of those non-conformances is not. Some non-conformances may occur for reasons that are understood and knowingly tolerated for valid reasons. One could reasonably require the senior manager concerned to approve these, which effectively signals informed consent. However, there may be instances where a non-conformance occurs which represents an error that is not acceptable to the Entity concerned one which needs correcting rather than approval.	The language of the standard states that the approval of exceptions to the policy can be approved by a delegate or delegates approved by the senior manager.
003-R4	R4.1 The minimum should not include everything. Remove ", and any related security information". Replace Requirement 4.3 with words from Requirement 5.2	Changed to "security configuration information of cyber security assets." Requirement 4.3 deals with the classification of information related to Critical Cyber Assets. Requirement 5.2 deals specifically with the ability of personnel to access the information. The classification of sensitive information and the access restrictions to the information are two separate requirements.
003-R5	Remove R5 because it overlaps Requirement 4 in CIP004 and Requirement 6.1 in CIP007. This overlap is confusing. It is not clear how Requirement 4 in CIP003 is different from this Requirement.	CIP-004 addresses the phsyical and logical access to Critical Cyber Assets. CIP-003 deals with restricting access to protected information regarding Critical Cyber Assets. These two are not in conflict. CIP-007 requirement 6.1 deals with user and system accounts and is not in conflict with CIP-003.
003-R6		
003-M1		
003-M2		
003-M3		

CIP-003 Drafting Team Responses to Comments

003-M4		
003-M5	Remove M5 since R5 was removed.	Please see response above.
003-M6		
003-C1,1		
003-C1,2		
003-C1,3		
003-C1,4	This is confusing. We believe this refers to non-conformance with the Entity's cyber security policy. It is already stated in requirement R3.	You are correct. This section has been reworded for clarity.
003-C2,1	Requirement R1.4 requires annual review of the cyber security policy. This is not consistent with compliance statement 2.1.2 which suggests that an entity that reviews its policy every three years would be fully compliant. Remove 2.2.3 since M5 was removed.	Levels of noncompliance have been rewritten.
003-C2,2		
003-C2,3	Levels of noncompliance have been rewritten.	Levels of noncompliance have been rewritten.
003-C2,4	Compliance statement 2.4.3 should be revised to more clearly refer to a program for the identification and classification of information about Critical Cyber Assets. 2.4.5 and 2.4.6 should be removed since they depend on M5, which we removed	The program for the identification and classification of information aboutCritical Cyber Assets referenced in 2.4.2 is intended to address the program defined on R4.

CIP-003 Drafting Team Responses to Comments

Name	Deborah Linke	
Entity	Bureau of Reclamation	
Ballot:	No	
General Comments	There are several areas which should be clarified including who is to review and approve the entity's cyber security policy, and how delegation of these responsibilities is to be accomplished.	The policy review and delegation of responsibilities is the responsibility of each entity. It is not the intent of this standard to dictate business processes.
	The word “classification” regarding information has some connotations that are probably not the intent. The crux of the issue is to identify the information that needs to be protected on a need to know basis.	Identifying the information that needs to be protected on a “need to know basis” is only one step. Classifying the information provides a second level of protection that serves as not only a reminder of the security level of the information but also provides personnel a mechanism for identifying protected information that helps protect against accidental dissemination.
003-R1		
003-R2		
003-R3		
003-R4		
003-R5	Section R5 is a bit confusing. We believe the intent is to limit access to systems, system diagrams, documentation, etc, to those authorized. As written, it would imply that physical access is also covered, which could be problematic and which is covered elsewhere in the standard.	R5 requires limiting logical and physical access to information associated with Critical Cyber Assets. This is different from limiting physical access to the Critical Cyber Assets themselves.
003-R6		
003-M1		
003-M2		
003-M3		
003-M4		
003-M5		
003-M6		
003-C1,1		
003-C1,2		

CIP-003 Drafting Team Responses to Comments

003-C1,3

003-C1,4

003-C2,1

003-C2,2

003-C2,3

003-C2,4

CIP-003 Drafting Team Responses to Comments

Name	Greg Mason	
Entity	Dynegy Generation	
Ballot:	No	
General Comments		
003-R1		
003-R2		
003-R3	Section R3 and Section D1.4 in CIP-003 and CIP-007 provide for "Exceptions" when the "Responsible Entity cannot conform to its cyber security policy.. "The standard also provides for the documentation and approval of any such exceptions with compensating measures or risk acceptance. Please revise the wording to clarify the intent of the wording "..cannot conform..".For example, are these exceptions oriented toward interim periods before longer lead time remediation improvements can be implemented?Is simply accepting,documenting and appropriately approving non compliance with a provision of the standard acceptable?	All exceptions must be approved and documented per the Responsible Entity's documented exception process.
003-R4		
003-R5		
003-R6		
003-M1		
003-M2		
003-M3		
003-M4		
003-M5		
003-M6		
003-C1,1		
003-C1,2		
003-C1,3		
003-C1,4		
003-C2,1		

CIP-003 Drafting Team Responses to Comments

003-C2,2

003-C2,3

003-C2,4

CIP-003 Drafting Team Responses to Comments

Name	Paul McClay	
Entity	Tampa Electric	
Ballot:	No	
General Comments		
003-R1		
003-R2		
003-R3		
003-R4	R4.1 A great deal of information covered in this requirement may either be a document of public record (i.e. floorplans/blueprints) or released to government agencies or other entities as part of disaster or other computer planning activities (i.e. configurations for upgrades, new purchases, etc.). For equipment already purchased and installed, we have no opportunity to control documents (already released) as multi-year contract terms have already been agreed to. How is an organization to secure material that falls into these categories?	The Responsible Entity is responsible to protect the information that is covered by this requirement. Responsible Entities that cannot meet the requirements of its cyber security policies must have duly authorized exceptions. The standard does not require you to recover information that is already released or required to be released to the public.
003-R5	R5.3 The subject of 5.3 is not all access privileges. To clarify this requirement, change to: The Responsible Entity shall annually review and update the process for controlling access privileges to information associated to Critical Cyber Assets.	This section has been revised.
003-R6	Change control… We feel that the word “any” within the phrase “for modifying or replacing any Critical Cyber Asset hardware or software” is too broad. Technically this could apply to changing of a NIC card, monitor, keyboard, printer driver, or another change that has little or no impact on the operation of this asset. We feel that this should be changed to “for the significant modification or replacement of Critical Cyber Asset hardware or software” and "significant" left to the entity’s interpretation. This same comment applies to “any changes” in R6.3. Typically a Change Control process includes formal signoffs, but not testing procedures. If it is your intent to have documented testing procedures, then specifically include this in the verbiage and reflect in the measures, such as The Responsible… methodical processes of change control and testing for modifying…... Also provide some guidance in your FAQ’s for what the testing procedures should include. R6.1 Clarify by changing to: The responsible entity shall review its processes for managing change to and testing modification or changes to Critical Cyber Assets at least annually. However, if it is only your intent to have a signoff authority, then there is no need to review the “testing process” mentioned in R6.1 above. R6.3 Change Management Procedures typically would identify/list all components of a	R6 has been revised and its subrequirements removed. Supporting configuration management activities are those which monitor what is being done by the vendor and works closely with the vendor to ensure that a) nothing breaks and b) implemented security controls are not disabled.

	system that are being changed or added and control their promotion to production. Please clarify what additional information or activity the supporting “configuration management activities” must provide.	
003-M1		
003-M2		
003-M3		
003-M4		
003-M5		
003-M6	Make this measure consistent with the final requirements. If no requirements are changed then modify to : The Responsible Entity’s written and approved processes of change control, documented approval authority for testing of modification or changes to Critical Cyber Assets, approved testing results, and documentation of annual reviews.	The measures have been reworded to refer back to the requirements.
003-C1,1		
003-C1,2		
003-C1,3		
003-C1,4		
003-C2,1	D2.1.2 add “or does not address all requirements of NERC CIP-002 through CIP-009 Standards D2.1.3 This should read- Exceptions (rather than Deviations) from written cyber security policy have not been documented….	The levels of noncompliance have been rewritten.
003-C2,2	D2.2.3 Change to: Access privileges to information associated with Critical Cyber Assets have not been reviewed……	The levels of noncompliance have been rewritten.
003-C2,3	The levels of noncompliance have been rewritten.	The levels of noncompliance have been rewritten.
003-C2,4	D2.4.5 To be consistent with the requirement, change to -Access privileges to information associated with Critical Cyber Assets have not been reviewed in the last calendar year. D2.4.6 Delete, does not match any stated requirement in this standard. Perhaps belongs in CIP-004-1, thought seems adequately covered there already by other non-compliance sentences.	The levels of noncompliance have been rewritten.

CIP-003 Drafting Team Responses to Comments

Name	David McCoy	
Entity	Great Plains Energy/Kansas City Power & Light	
Ballot:	No	
General Comments		
003-R1		
003-R2	Here it says changes in the designated senior manager must be documented within thirty days. Noncompliance provision 2.1.1. says entities can be out of compliance if senior managers are not designated within ten days. If you change senior managers then it should be clear whether you have ten or thirty days to do so. I would recommend it be 30 days.	The level of non-compliance has been removed.
003-R3		
003-R4		
003-R5		
003-R6		
003-M1		
003-M2		
003-M3		
003-M4		
003-M5		
003-M6	Every other measure has a non compliance provision that addresses it but this one. It seems that this measure should also have a corresponding non compliance provision.	The levels of noncompliance have been rewritten.
003-C1,1		
003-C1,2		
003-C1,3		
003-C1,4		
003-C2,1	See comment on R.2	Please see response at R2.
003-C2,2		

CIP-003 Drafting Team Responses to Comments

003-C2,3

003-C2,4

CIP-003 Drafting Team Responses to Comments

Name	William McEvoy	
Entity	Northeast Utilities	
Ballot:	No	
General Comments		
003-R1	R1 should be rewritten to "each Entity shall have a Cyber Security Policy that includes the following." NERC Standards should be focused on Reliability not management structure.	Please see responses to Ray A'Brial, Central Hudson Gas & Electric Corp.
003-R2	change R2 to "The Responsible Entity shall assign a senior manager or delegate(s) with responsibility"	
003-R3	Change R3 to "Exceptions - Instances where the Responsible Entity accepts non-conformance with its cyber security policy". The requirement to document non-conformance with an Entity's cyber security policy is sensible, but the requirement for a senior manager to approve all of those non-conformances is not. Some non-conformances may occur for reasons that are understood and knowingly tolerated for valid reasons. One could reasonably require the senior manager concerned to approve these, which effectively signals informed consent. However, there may be instances where a non-conformance occurs which represents an error that is not acceptable to the Entity concerned one which needs correcting rather than approval.	
003-R4	The minimum should not include everything. Remove ", and any related security information". Replace Requirement 4.3 with words from Requirement 5.2	
003-R5	Remove R5 because it overlaps Requirement 4 in CIP004 and Requirement 6.1 in CIP007. This overlap is confusing. It is not clear how Requirement 4 in CIP003 is different from this Requirement.	
003-R6	R6 should move to CIP007.	
003-M1		
003-M2		
003-M3		
003-M4		
003-M5	Remove M5 since R5 was removed	
003-M6	Move to CIP007 since R6 was moved to CIP007	
003-C1,1		

CIP-003 Drafting Team Responses to Comments

003-C1,2

003-C1,3

003-C1,4 This is confusing. We believe this refers to non-conformance with the Entity's cyber security policy.

003-C2,1 Compliance statement 2.1.1 imposes a requirement that is not identified in the requirements section. Specifically, 2.1.1 effectively imposes a requirement that the gap in designating a senior management representative be less than 10 days, which is not specified in the requirements section. Ten days was never specified before this.

Requirement R1.4 requires annual review of the cyber security policy. This is not consistent with compliance statement 2.1.2 which suggests that an entity that reviews its policy every three years would be fully compliant.

Compliance statement 2.1.3 imposes a requirement that is not identified in the requirements section.

Remove 2.2.3 since M5 was removed.

003-C2,2

003-C2,3

003-C2,4 Compliance statement 2.4.3 should be revised to more clearly refer to a program for the identification and classification of information about Critical Cyber Assets.

2.4.5 and 2.4.6 should be removed since they depend on M5, which we removed

CIP-003 Drafting Team Responses to Comments

Name	Patrick Miller	
Entity	PacifiCorp	
Ballot:	No	
General Comments		
003-R1		
003-R2		
003-R3		
003-R4	For section R4.3, there are too many requirements in the verbiage to represent a single, stand-alone item. Please break this out into multiple standards.	R4 has been revised for greater clarity.
003-R5	For R5, the term "Access Control" is somewhat misleading, from a Security Lexicon perspective. Consider using "Access Management" or other alternative language. Additionally, for R5.1.2, consider including email as one of the identification points. For section R5.2, there are too many requirements in the verbiage to represent a single, stand-alone item. Please break this out into multiple standards.	The title explains the intent-- controlling access to information. It is the responsibility of each entity to identify what information is associated with Critical Cyber Assets and where that information may reside. R5 has been revised for greater clarity.
003-R6		
003-M1		
003-M2		
003-M3		
003-M4		
003-M5		
003-M6		
003-C1,1		
003-C1,2		
003-C1,3		
003-C1,4		

CIP-003 Drafting Team Responses to Comments

003-C2,1

003-C2,2

003-C2,3

003-C2,4

CIP-003 Drafting Team Responses to Comments

Name	Don Miller	
Entity	First Energy Corp	
Ballot:	No	
General Comments		
003-R1		
003-R2		
003-R3		
003-R4	Information Protection you require entities to identify, classify and protect their information, classification is an enormous task for any major corporation be specific on what to classify, also under R 4.1 you have added a catch all statement to protect "any related security information". This is to general of a statement, put bounds around the statement to make it more manageable.	The identification and classification of information associated with Critical Cyber Assets is for each entity to determine. It is not the intent of this standard to dictate the methodology for identifying or classifying information as it relates to each Responsible Entity’s Critical Cyber Assets. This statement has been removed from R4.1.
003-R5		
003-R6		
003-M1		
003-M2		
003-M3		
003-M4		
003-M5		
003-M6		
003-C1,1		
003-C1,2		
003-C1,3		
003-C1,4		
003-C2,1		

CIP-003 Drafting Team Responses to Comments

003-C2,2

003-C2,3

003-C2,4

CIP-003 Drafting Team Responses to Comments

Name	Jeff Mitchell
Entity	ECAR
Ballot:	Yes
General Comments	N/A
003-R1	
003-R2	
003-R3	
003-R4	
003-R5	
003-R6	
003-M1	
003-M2	
003-M3	
003-M4	
003-M5	
003-M6	
003-C1,1	
003-C1,2	
003-C1,3	
003-C1,4	
003-C2,1	
003-C2,2	
003-C2,3	
003-C2,4	

CIP-003 Drafting Team Responses to Comments

Name	Scott Mix	
Entity	KEMA, Inc	
Ballot:	No	
General Comments		
003-R1		
003-R2		
003-R3		
003-R4		
003-R5	Requirement R5.2 deals with the list of authorized users, not the authorization and approval process. CIP-004 R4 deals with this topic. I suggest that this requirement be folded into CIP-004 R4.1.	CIP-004.R4.1 addresses access to Critical Cyber Assets. CIP-003.R5.2 addresses access to information associated with Critical Cyber Assets. This information does not necessarily reside within the physical or electronic security perimeter protecting Critical Cyber Assets.
003-R6		
003-M1		
003-M2		
003-M3		
003-M4		
003-M5		
003-M6		
003-C1,1		
003-C1,2		
003-C1,3		
003-C1,4		
003-C2,1		
003-C2,2		
003-C2,3		
003-C2,4		

CIP-003 Drafting Team Responses to Comments

Name Darrick Moe

Entity WAPA

Ballot: No

General Comments		
003-R1	R2 (or R1.3) should have language added that clarifies that management responsibility in various areas of cyber security can be delegated within the organization as defined in the responsible entity's cyber security policy. While the need for a single senior manager to be designated as having overall responsibility is understandable, it should be clear that all other aspects of control and accountability can be delegated as necessary, and as they define, by each organization. "The Senior Manager may delegate any of these responsibilities as desired and defined" could be added at the end of R2 (after "CIP-009 Standards") to achieve this. In R1.3, the word "continually" in the phrase "management is continually engaged" should be changed to something more measurable. The Requirement in R1.4 that the cyber security policy be reviewed annually does not align with the compliance requirement in Level 1 Non-Compliance, 2.1.2, which indicates a three year periodicity.	The standard stipulates the designation of a senior manager with overall responsibility to lead and mange the implementation of and adherence to CIP-002 through CIP-009. How that manager delegates responsibilities is solely up to the Responsible Entity. R1.3 has been removed. The inconsistency in R1.4 (renumbered to R1.3) has been resolved.
003-R2		
003-R3	R3 does not indicate how long an entity has to document an exemption, but Level 1 Non-Compliance, 2.1.3, indicates that an entity only has thirty calendar days. This 30 day requirement should be worked into R3 so these align.	This inconsistency has been resolved.
003-R4	FAQ #3 associated with CIP-003-1 implies that US Government entities, such as the Power Marketing Administrations, would use the classification scheme of "Top Secret, Secret, Classified, or Unclassified" and goes on to suggest a parallel with "Confidential, Sensitive, Nonpublic, and Public". The implied tie between these two schemes should be eliminated. Cyber information for Federal entities that is not "Public" may still not be "Classified, Secret, or Top Secret", as established by Federal standards for these classifications. It is not necessary to establish requirements to implement a classification scheme at all; to mandate one, results in unnecessary complication. In R4.2, the word "classify" should be changed to "identify and protect". R4.3 should be modified to require only the annual review of an entity's identification and protection program, eliminating the reference to classification. R4 should be modified by deleting the word "classify".	The FAQ is merely showing, by way of example, some existing classification schemes. Responsible Entities are encouraged to develop a classification scheme that works for them.
003-R5	R5 should be revised to add "Critical Cyber Assets and" prior to the words "information associated with", to clarify that R5 is not specific only to the Assets, but also to information.	R4 addresses an information protection program and R5 addresses access to protected information.

003-R6

003-M1

003-M2

003-M3

003-M4

003-M5

003-M6

003-C1,1

003-C1,2

003-C1,3

003-C1,4

003-C2,1

003-C2,2

003-C2,3

003-C2,4

CIP-003 Drafting Team Responses to Comments

Name	Selby Mohr
Entity	Sacramento Municipal Utility District
Ballot:	Yes

General Comments

003-R1

003-R2

003-R3

003-R4

003-R5

003-R6

003-M1

003-M2

003-M3

003-M4

003-M5

003-M6

003-C1,1

003-C1,2

003-C1,3

003-C1,4

003-C2,1

003-C2,2

003-C2,3

003-C2,4

CIP-003 Drafting Team Responses to Comments

Name	Kurt Muehlbauer	
Entity	Exelon	
Ballot:	No	
General Comments	The documentation and processes around the responsible entitys tasks are too prescriptive. The industry needs to be extremely careful to avoid the creation of purely documentation-based non-compliances. With increasing legal requirements for compliance, and the associated penalties for noncompliance, noncompliance should be reserved for real security issues. It is simply too easy to make a mistake in documentation in light of the constantly evolving cyber environment. Each entity should develop its own processes in support of the requirements, and these processes should be required to contain provisions for periodic review and approval applicable to each requirement. The processes should also be required to produce reasonable documentation to demonstrate compliance. However, it is not necessary to specify the details of the documentation or review periods. The above approach can be met by removing references to documentation from the requirements section. Then, in the measures section require each entity to reasonably document programs and processes that support the security requirements and to produce reasonable documentation required to demonstrate compliance to the security requirements. Please refer to our overall comments on defining reasonable. If the above approach is taken, it will be possible to delete many of the sub-bullet points under each requirement (because the details will be specified by each entity in their program or process, as applicable). This will also ensure that documentation and excessive low-value administrative tasks are removed from the requirements.	The Drafting Team has reviewed the standards and removed prescription where possible. The prescriptiveness that remains is necessary to provide the clarity requested by a majority of commenters. The documentation required by these standards allow Responsible Entities to demonstrate that the policies, processes, and procedures that they have implemented consistently comply with the requirements of these standards.
003-R1	R1 Structure of relationships and decision-making processes should not be required to be in the policy itself. Keep the org chart separate from the policies. R2 defines the company leader who is accountable for compliance. Delete R1.3 and R1.4. Please see the general comments to this standard for our rationale. In place of these statements, we recommend adding a general measure in the measures section to the affect, Each entity shall have processes for maintaining their policy, which shall include provisions for periodic reviews and approvals.	The statements requiring entities to define a structure of relationships and decision-making processes has been removed from the standard. Please refer to response to general comments above.
003-R2	R2.1 Remove name, phone, and address. Only title and date should be required. Delete R2.1 and R2.2. Please see the general comments to this standard for our rationale. In place of this statement, we recommend adding a general measure in the measures section to the affect, Each entity shall have processes for maintaining the documentation of the senior responsible manager, which shall include provisions for periodic reviews and approvals. Delete R2.3, as it is redundant with R3.	The contact information is necessary to know who is responsible for leading and managing the entity's implementation of and adherence to these standards. This should be business-level information, not personal. Refer to response to general comments. These sections have been revised to eliminate redundancy.

CIP-003 Drafting Team Responses to Comments

003-R3	Delete 3.1. Simply require periodic review and approval according to the entity s own policies and procedures. Combine 3.2 and 3.3.	Each entity may implement greater security measures than those required by this standard. The time periods imposed by this standard represent an industry consensus. 3.2 and 3.3 represent separate activities and remain separate requirements.
003-R4	Require each entity to implement a program that controls and protects information, but leave the specifics of the program to each entity. This can be accomplished by keeping the first sentence of R4.1 and adding, implement a program to… after shall. Then remove the second sentence in R4.1, because these specified documents are all included previously under, information related to Critical Cyber Assets… Please delete R4.2, as this is redundant with R4, a program to identify, classify, and protect… Delete R4.3. Please see the general comments to this standard for our rationale. In place of this statement, we recommend adding a general measure in the measures section to the affect, Each entity shall have processes for maintaining the information protection program, which shall include provisions for periodic reviews and approvals.	R4.1 includes a minimum list. A Responsible Entity can choose to include to protect other information as it deems appropriate using reasonable business judgment. The statement in R4.1 has been removed. 4.1 specifies types of information to be protected. 4.2 addresses the level of protection that may be applicable to the information mentioned in 4.1. 4.2 has been revised to be more specific. 4.3 Refer to response to general comments.
003-R5	R5 and R5.1 Clarify the intent of this requirement. The first sentence talks about access to information associated with Critical Cyber Assets , but the rest of the requirement addresses access to the critical cyber assets themselves. Suggest rewording R5 to include the information and the critical cyber assets themselves. Implement an access authorization program for managing access to information associated with critical cyber assets and the critical cyber assets themselves. Delete R5.1.1 It is implied in R5.1. Delete R5.1.2 It is redundant with R5.1 and the contact details should be consistent with each entity s access program. Delete R5.1.3 and R5.3. Please see the general comments to this standard for our rationale. In place of this statement, we recommend adding a general measure in the measures section to the affect, Each entity shall have processes for maintaining the program for managing access to information associated with critical cyber assets, which shall include provisions for periodic reviews and approvals. Modify R5.2 as follows: The access management program shall require periodic review of access privileges.	These sections have been revised for greater clarity and consistency. R5.1.1 has been revised. R5.1.2 has been revised. Identifying the personnel responsible for authorizing access to protected information is critical. The ability to assign responsibility for access to protected information allows entities to exert a greater level of control. Entities may implement controls beyond the basic set of requirements in this standard. Refer to response to general comments. R5.2 An annual review is consistent with time frames used in other CIP standards and represents industry consensus.
003-R6	Reword R6, to, shall establish and implement a program for change control that addresses CCA hardware and software. Delete 6.1-6.3. These are too prescriptive in dictating the process. Each entity should establish an acceptable process.	R6 has been revised.

CIP-003 Drafting Team Responses to Comments

003-M1 Refer to general, overall comments submitted on CIP-002 through CIP-009 regarding revision of the measures and compliance specification.

003-M2 Refer to general, overall comments submitted on CIP-002 through CIP-009 regarding revision of the measures and compliance specification.

003-M3 Refer to general, overall comments submitted on CIP-002 through CIP-009 regarding revision of the measures and compliance specification.

003-M4 Refer to general, overall comments submitted on CIP-002 through CIP-009 regarding revision of the measures and compliance specification.

003-M5 Refer to general, overall comments submitted on CIP-002 through CIP-009 regarding revision of the measures and compliance specification.

003-M6 Refer to general, overall comments submitted on CIP-002 through CIP-009 regarding revision of the measures and compliance specification.

003-C1,1 Refer to general, overall comments submitted on CIP-002 through CIP-009 regarding revision of the measures and compliance specification.

003-C1,2 Refer to general, overall comments submitted on CIP-002 through CIP-009 regarding revision of the measures and compliance specification.

003-C1,3 Refer to general, overall comments submitted on CIP-002 through CIP-009 regarding revision of the measures and compliance specification.

003-C1,4 Refer to general, overall comments submitted on CIP-002 through CIP-009 regarding revision of the measures and compliance specification.

003-C2,1 Refer to general, overall comments submitted on CIP-002 through CIP-009 regarding revision of the measures and compliance specification.

003-C2,2 Refer to general, overall comments submitted on CIP-002 through CIP-009 regarding revision of the measures and compliance specification.

003-C2,3

003-C2,4 Refer to general, overall comments submitted on CIP-002 through CIP-009 regarding revision of the measures and compliance specification.

CIP-003 Drafting Team Responses to Comments

Name	Jeffrey Mueller	
Entity	PSEG Companies	
Ballot:	No	
General Comments	The PSEG Companies have reviewed and share the concerns expressed in the Comments of PJM and EEI. Accordingly, the PSEG Companies support the comments of PJM and EEI, and request that the concerns expressed in those comments be properly addressed in the next version of the draft standard.	Please see responses to Laurence W. Brown, Edison Electric Institute.
003-R1		
003-R2		
003-R3		
003-R4		
003-R5		
003-R6		
003-M1		
003-M2		
003-M3		
003-M4		
003-M5		
003-M6		
003-C1,1		
003-C1,2		
003-C1,3		
003-C1,4		
003-C2,1		
003-C2,2		
003-C2,3		
003-C2,4		

CIP-003 Drafting Team Responses to Comments

Name	Mitchell Needham
Entity	Tennessee Valley Authority
Ballot:	Yes
General Comments	
003-R1	
003-R2	
003-R3	
003-R4	
003-R5	
003-R6	
003-M1	
003-M2	
003-M3	
003-M4	
003-M5	
003-M6	
003-C1,1	
003-C1,2	
003-C1,3	
003-C1,4	
003-C2,1	
003-C2,2	
003-C2,3	
003-C2,4	

CIP-003 Drafting Team Responses to Comments

Name	Dave Norton	
Entity	Entergy Transmission	
Ballot:	No	
General Comments		
003-R1		
003-R2		
003-R3		
003-R4	R4.1: “Information Protection The Responsible Entity shall identify and protect information relating to Critical Cyber Assets, regardless of media type.” The requirement goes on to identify “at a minimum” the various types of *documentary* information that should be protected, such as floor plans, network topologies, etc. Did the drafting team consciously intend that documentary information is the only information that requires protection? Computer RAM is a media type, so what about real time, “live” data and information about critical assets that’s being processed or transmitted? Information is an asset not just hardware - and this asset is essentially relevant to reliable operation of critical electric infrastructure assets, so therefore shouldn’t critical asset “data in process” also be subject to the same information protection requirements as documentation?	R4.1 includes a minimum list. A Responsible Entity can choose to include to protect other information as it deems appropriate using reasonable business judgment.
003-R5		
003-R6	R6.3: Is use of the word “report” intended, or should it read “record”?	This requirement has been removed.
003-M1		
003-M2		
003-M3		
003-M4	M4: Is it “written and approved program”, or, should it be “written and approved program plan” or “… program summary description”?	The measures have been reworded to refer back to the requirements.
003-M5		
003-M6		
003-C1,1		
003-C1,2		
003-C1,3		

CIP-003 Drafting Team Responses to Comments

003-C1,4		
003-C2,1	C2.1: Where are the violations of M.1 and M.4 covered?	Levels of noncompliance have been rewritten. M1 and M4 violations are level 4 noncompliance.
003-C2,2		
003-C2,3		
003-C2,4		

CIP-003 Drafting Team Responses to Comments

Name	Doug Orlofske
Entity	Wisconsin Public Power Inc
Ballot:	Yes

General Comments

003-R1

003-R2

003-R3

003-R4

003-R5

003-R6

003-M1

003-M2

003-M3

003-M4

003-M5

003-M6

003-C1,1

003-C1,2

003-C1,3

003-C1,4

003-C2,1

003-C2,2

003-C2,3

003-C2,4

CIP-003 Drafting Team Responses to Comments

Name	Kevin Perry	
Entity	Southwest Power Pool	
Ballot:	No	
General Comments		
003-R1	R1.4: Approved by whom? The designated senior manager (Requirement R2) is recommended as a clarification.	The requirement has been clarified.
003-R2	Please clarify "Senior Manager". Is this a company executive, the manager of security, or someone else? In all likelihood, the Senior Manager is probably not going to be the person responsible for leading and managing the implementation of the CIP standards. That will typically be delegated to one or more functional managers, whether the security manager, SCADA systems manager, or someone else. This requirement should be clarified to refer to an individual charged with overall compliance to the CIP standards.	The assignment of a "senior manager" is at the discretion of the Responsible Entity. Typically this would be someone in a higher position of responsibility than a line supervisor. The requirement has been clarified.
003-R3	R3: Delegation of approval for non-conformance should not be delegated.	It is up to Responsible Entities to define policies, exception handling, and delegation authority.
003-R4		
003-R5		
003-R6	Change control, while an important business function, is not a security issue. Change management affects the reliability and availability of the managed system. It does not contribute to the security of the affected system. Other requirements of the CIP standards deal with security-related changes, such as system patching. The prescription for implementing a rigorous change management process should be removed from this standard.	Changes to a secure environment can affect security controls that are currently in place. A change control program can assist in mitigating some of these risks by not only documenting the changes but by keeping all involved parties informed.
003-M1	Who is the approval authority? Is it the senior manager designated in R2?	Measures have been rewritten to refer back to the requirements.
003-M2		
003-M3		
003-M4	Who is the approval authority? Is it the senior manager designated in R2?	Measures have been rewritten to refer back to the requirements.
003-M5	Who is the approval authority? Is it the senior manager designated in R2?	Measures have been rewritten to refer back to the requirements.
003-M6	Subject to the comment for R6, this measure should be removed. Who is the approval authority? Is it the senior manager designated in R2?	Measures have been rewritten to refer back to the requirements.

CIP-003 Drafting Team Responses to Comments

003-C1,1		
003-C1,2		
003-C1,3		
003-C1,4	Exception approval should not be delegated.	It is up to Responsible Entities to define policies, exception handling, and delegation authority.
003-C2,1		
003-C2,2		
003-C2,3		
003-C2,4		

CIP-003 Drafting Team Responses to Comments

Name	Tom Pruitt	
Entity	Duke Power Company	
Ballot:	Yes	
General Comments	A.4.1 -- Given the critical role of the PSE, why are these standards not applicable to that entity? A.4.2.2 -- Appears to be inconsistent with definition of "Cyber Asset". A.5 -- This should reference the proposed Implementation Plan. Alternatively, the compliance implementation plan should be referenced in the compliance sections for all of CIP002 thru CIP 009.	The standards reflect the Standard Authorization Request (SAR), which excluded PSEs. The drafting team must respect the scope of the SAR and not extend it during standards development. The SAR reflects industry consensus on the scope of the standard to be developed. The SAR specifically excluded communication links. Although reviewed and commented upon by the industry, the Implementation Plan is not part of the standard and cannot be referenced therein.
003-R1	R1.4 -- Approval should only be required if the policy is changed. The reviewing body sign-off should be sufficient to document the review process.	A review and approval, even if the policies have not changed, should be signed by the senior manager as defined in R2. Where the policy is not changed, senior management approval is not expected to be burdensome.
003-R2	R2.2 -- Replace "Changes to" … to "A change in"...	
003-R3		
003-R4	R4 -- There is no requirement to back up protected information related to Critical Cyber Assets (and no protection required for backup media)? Why not?	The standard indicates that information associated with Critical Cyber Assets, regardless of media type, shall be protected. This statement would include backup media since the backup media would contain information associated with Critical Cyber Assets.
003-R5	R5.1.2 -- This list needs to be revised within some shorter timeframe than yearly (as indicated in R5.1.3) if any of the designated personnel change.	The standard specifies "at least an annual review." Responsible Entities may go beyond the minimum requirements as they deem appropriate.
003-R6		
003-M1		
003-M2		
003-M3		
003-M4		
003-M5		

CIP-003 Drafting Team Responses to Comments

003-M6

003-C1,1

003-C1,2

003-C1,3

003-C1,4

003-C2,1

003-C2,2

003-C2,3

003-C2,4

CIP-003 Drafting Team Responses to Comments

Name	Duane Radzwion
Entity	Consumers Energy
Ballot:	Yes
General Comments	
003-R1	
003-R2	
003-R3	
003-R4	
003-R5	
003-R6	
003-M1	
003-M2	
003-M3	
003-M4	
003-M5	
003-M6	
003-C1,1	
003-C1,2	
003-C1,3	
003-C1,4	
003-C2,1	
003-C2,2	
003-C2,3	
003-C2,4	

CIP-003 Drafting Team Responses to Comments

Name	Howard Rulf	
Entity	We Energies	
Ballot:	No	
General Comments		
003-R1		
003-R2		
003-R3	Due to the lack of user account administration security and general system security in the plant control systems, many exceptions will be documented per the CIP requirements until the vendor supplied systems implement security functionality and the systems can feasibly be upgraded. Most deal with the CIP-007: Cyber Security -Systems Security Management	Only exceptions to the Responsible Entity's cyber security policy are allowed. Exceptions to NERC Standards are not allowed. Therefore, it is important for each entity, when documenting its cyber security policies, to structure them accordingly so that limitations of systems due to technological constraints may be properly addressed. Please see the FAQ on technical feasibility.
003-R4		
003-R5		
003-R6		
003-M1		
003-M2		
003-M3		
003-M4		
003-M5		
003-M6		
003-C1,1		
003-C1,2		
003-C1,3		
003-C1,4		
003-C2,1		
003-C2,2		

CIP-003 Drafting Team Responses to Comments

003-C2,3

003-C2,4

CIP-003 Drafting Team Responses to Comments

Name	Randy Schimka	
Entity	San Diego Gas and Electric Co.	
Ballot:	No	
General Comments		
003-R1	R1.2 suggested change: "The Responsible Entity shall have a written cyber security policy and make it available to employees."	This requirement has been revised to address this issue.
003-R2		
003-R3		
003-R4	R4.1 suggested change: Add "Critical Asset system passwords" to the list of protected items in this section.	R4.1 includes a minimum list. A Responsible Entity can choose to include to protect other information as it deems appropriate using reasonable business judgment.
003-R5		
003-R6		
003-M1		
003-M2		
003-M3		
003-M4		
003-M5		
003-M6		
003-C1,1		
003-C1,2		
003-C1,3		
003-C1,4		
003-C2,1		
003-C2,2		
003-C2,3		
003-C2,4		

CIP-003 Drafting Team Responses to Comments

Name	Lyman Shaffer	
Entity	PG&E	
Ballot:	Yes	
General Comments		
003-R1	R.1.4 requires an annual approval of the security policy. Given that these probably won't change much, we would like to suggest an annual review and a biannual formal approval by the responsible officer.	A review and approval, even if the policies have not changed, should be signed by the senior manager as defined in R2. Where the policy is not changed, senior management approval is not expected to be burdensome.
003-R2		
003-R3	R.3.1 uses two terms ("senior management" and "senior manager" somewhat interchangeably. To most companies, senior management implies senior officer level which is where we believe this is intended to rest. Senior manager implies someone below that officer level which is not appropriate.	The requirements have been revised and "senior manager" is now used consistently. This was intended to mean someone in a higher position of responsibility than a line supervisor, however, the assignment of a "senior manager" is at the discretion of the Responsible Entity.
003-R4	R.4.1 the standard uses the term "regardless of media type." this m,ay be too broad as there are documents such as system diagrams that are used widely in paper form but shouldn't be covered wthin the scoipe of this standard	Even printed system diagrams could be compromised. It is each entity's responsibility to protect information related to Critical Cyber Assets regardless of the media in which it is presented.
003-R5		
003-R6		
003-M1		
003-M2		
003-M3		
003-M4		
003-M5		
003-M6		
003-C1,1		
003-C1,2		
003-C1,3		

CIP-003 Drafting Team Responses to Comments

003-C1,4

003-C2,1

003-C2,2

003-C2,3

003-C2,4

CIP-003 Drafting Team Responses to Comments

Name	Neil Shockey	
Entity	Southern California Edison	
Ballot:	No	
General Comments		
003-R1		
003-R2	Change R2.2 to read: Changes to the designated senior manager must be documented in the Cyber Security Policy within 90 calendar days of the effective date.	30 calendar days represents industry consensus.
003-R3		
003-R4		
003-R5		
003-R6		
003-M1		
003-M2		
003-M3		
003-M4		
003-M5		
003-M6		
003-C1,1		
003-C1,2		
003-C1,3		
003-C1,4		
003-C2,1		
003-C2,2		
003-C2,3		
003-C2,4		

CIP-003 Drafting Team Responses to Comments

Name	William Smith	
Entity	Allegheny Power	
Ballot:	No	
General Comments		
003-R1		
003-R2		
003-R3		
003-R4	R4.1 should be removed from the standard and add to the FAQ as examples of documents that may need protected. The requirement as stated is too burdensome. R4.2 should be modified to state "The Responsible Entity shall classify and protect…."	R4.1 includes a minimum list. A Responsible Entity can choose to include to protect other information as it deems appropriate using reasonable business judgment. 4.1 specifies types of information to be protected. 4.2 addresses the level of protection that may be applicable to the information identified in 4.1.
003-R5		
003-R6		
003-M1		
003-M2	Add "(if applicable)" after "and changes to"	Measures have been rewritten to refer back to the requirements.
003-M3	Add "documentation supporting" before "annual reviews."	Measures have been rewritten to refer back to the requirements.
003-M4		
003-M5		
003-M6		
003-C1,1		
003-C1,2		
003-C1,3		
003-C1,4		
003-C2,1	Identified specific time periods that trigger levels of non-compliance that are more stringent than what the requirements specify. They should agree.	The levels of non-compliance has been rewritten.

003-C2,2		
003-C2,3	The levels of non-compliance has been rewritten.	The levels of non-compliance has been rewritten.
003-C2,4		

CIP-003 Drafting Team Responses to Comments

Name	Paul Sorenson
Entity	Open Access Technology International
Ballot:	Yes

General Comments

003-R1

003-R2

003-R3

003-R4

003-R5

003-R6

003-M1

003-M2

003-M3

003-M4

003-M5

003-M6

003-C1,1

003-C1,2

003-C1,3

003-C1,4

003-C2,1

003-C2,2

003-C2,3

003-C2,4

CIP-003 Drafting Team Responses to Comments

Name	Robert Strauss	
Entity	NYSEG	
Ballot:	No	
General Comments		
003-R1	R1 should be rewritten to "each Entity shall have a Cyber Security Policy that includes the following." NERC Standards should be focused on Reliability not management structure.	Please see responses to Ray A'Brial, Central Hudson Gas & Electric Corp.
003-R2	change R2 to "The Responsible Entity shall assign a senior manager or delegate(s) with responsibility	
003-R3	Change R3 to "Exceptions - Instances where the Responsible Entity accepts non-conformance with its cyber security policy". The requirement to document non-conformance with an Entity's cyber security policy is sensible, but the requirement for a senior manager to approve all of those non-conformances is not. Some non-conformances may occur for reasons that are understood and knowingly tolerated for valid reasons. One could reasonably require the senior manager concerned to approve these, which effectively signals informed consent. However, there may be instances where a non-conformance occurs which represents an error that is not acceptable to the Entity concerned one which needs correcting rather than approval.	
003-R4	The minimum should not include everything. Remove ", and any related security information". Replace Requirement 4.3 with words from Requirement 5.2	
003-R5	Remove R5 because it overlaps Requirement 4 in CIP004 and Requirement 6.1 in CIP007. This overlap is confusing. It is not clear how Requirement 4 in CIP003 is different from this Requirement	
003-R6	R6 should move to CIP007 otherwise the Drafting team to clarify its intent for including it here.	
003-M1		
003-M2		
003-M3		
003-M4		
003-M5	Remove M5 since R5 was removed	
003-M6	Move to CIP007 since R6 was moved to CIP007	
003-C1,1		

003-C1,2	
003-C1,3	
003-C1,4	This is confusing. We believe this refers to non-conformance with the Entity's cyber security policy.
003-C2,1	Compliance statement 2.1.1 imposes a requirement that is not identified in the requirements section. Specifically, 2.1.1 effectively imposes a requirement that the gap in designating a senior management representative be less than 10 days, which is not specified in the requirements section. Ten days was never specified before this. Requirement R1.4 requires annual review of the cyber security policy. This is not consistent with compliance statement 2.1.2 which suggests that an entity that reviews its policy every three years would be fully compliant. Compliance statement 2.1.3 imposes a requirement that is not identified in the requirements section. Remove 2.2.3 since M5 was removed.
003-C2,2	
003-C2,3	
003-C2,4	Compliance statement 2.4.3 should be revised to more clearly refer to a program for the identification and classification of information about Critical Cyber Assets. 2.4.5 and 2.4.6 should be removed since they depend on M5, which we removed

CIP-003 Drafting Team Responses to Comments

Name	Karl Tammar
Entity	IRC
Ballot:	No

General Comments

1.The requirement to document non-conformance with an Entity’s cyber security policy is sensible, but the requirement for a senior manager to approve all of those non-conformances is not. Some non-conformances may occur for reasons that are understood and knowingly tolerated for valid reasons. One could reasonably require the senior manager concerned to approve these, which effectively signals informed consent. However, there may be instances where a non-conformance occurs which represents an error that is not acceptable to the Entity concerned one which needs correcting rather than approval. Consider the wording, “Instances where the Responsible Entity accepts non-conformance with its cyber security policy…..” .

2. R5 and R4 should be combined. Both talk about requirements to protect information about Critical Cyber Assets.

3. In R4.3, it is unclear what is meant by the phrase, “cyber security protection controls”. This could be taken as a reference to the sum-total of controls in place to ensure compliance with CIP-002 through CIP-009. If this is actually intended, the requirement to assess and document these controls annually appears to overlap many similar requirements throughout the standards (eg. the requirements in R1.3, R5.2, R5.3, and R6.1 of CIP-003, R3 and R4, of CIP-005, R7 of CIP-006, and R9 of CIP-007)

4. Requirements 5.1, 5.1.1, 5.1.2, and 5.1.3 are about managing access to the assets themselves, yet they appear as sub-bullets of a requirement to manage access to information about Critical Cyber Assets. This is confusing, particularly as there is no measure that relates to the management of access to the assets themselves.

5. Measures M4 and M5 should be reviewed in light of comment 2 above.

6. M5 refers to a policy for management of access to information. There is no corresponding requirement (R5 requires the establishment of a program).

7. R6.2 appears to require that testing be performed prior to promoting systems to production. It is unclear what the purpose and scope of that testing needs to be, and where those dimensions are documented. If this is a reference to testing required in CIP-007, this should be noted, or the reference to testing deleted in favour of a more thorough treatment in CIP-007.

8. In R6.3, it is unclear what is meant by the qualifier “supporting” when referring to configuration management activities.

9. R6.3 is redundant given the text of R6, and overlaps with the requirements of R6.2.

Please see responses to Peter Henderson, Independent Electricity System Operator (IESO).

10. Section 1.4 under “Compliance” is somewhat unclear. The text appears to suggest that a Responsible Entity that does not fulfill one or more of the Standard’s requirements should actually claim that it is fully compliant with the Standard if it has a properly documented exception to those requirements approved by the designated senior manager at the time of compliance reporting. Is this the intent?

11. Requirement R 2.2 requires that changes to the designated senior manager must be documented within 30 days of the effective date. Compliance statement 2.1.1, however, states that an entity that fails to do so within 10 days is in non-compliance. This inconsistency should be resolved.

12. Compliance statement 2.1.1 imposes a requirement that is not identified in the requirements section. Specifically, 2.1.1 effectively imposes a requirement that the gap in designating a senior management representative be less than 10 days, which is not specified in the requirements section.

13. Requirement R1.4 requires annual review of the cyber security policy. This is not consistent with compliance statement 2.1.2 which suggests that an entity that reviews its policy every three years would be fully compliant.

14. Compliance statement 2.1.3 imposes a requirement that is not identified in the requirements section.

15. Compliance statement 2.2.3 should refer to access privileges to information associated with Critical Cyber Assets to more clearly correspond to R5.2 and to avoid imposing a requirement to review access privileges to the Critical Cyber Assets themselves that is not identified in the Requirements section.

16. Compliance statement 2.3.2 imposes a requirement that is not identified in the Requirements section. The compliance statement refers to access to the Critical Cyber Assets themselves, whereas the requirements refer to access to information about the assets.

17. Furthermore, compliance statement 2.3.2 imposes a new requirement that the roles and responsibilies of personnel with access to the assets must be documented (requiring a mapping of role/responsibility to access privilege), whereas the Requirements section asks only that access privileges correspond to roles and responsibilities (which is a looser requirement needing far less documentation and simpler business processes).

18. Failure to document the roles and responsibilties of personnel with access to Critical Cyber Assets (compl

CIP-003 Drafting Team Responses to Comments

003-R1

003-R2

003-R3

003-R4

003-R5

003-R6

003-M1

003-M2

003-M3

003-M4

003-M5

003-M6

003-C1,1

003-C1,2

003-C1,3

003-C1,4

003-C2,1

003-C2,2

003-C2,3

003-C2,4

CIP-003 Drafting Team Responses to Comments

Name	Todd Thompson	
Entity	PJM Interconnection	
Ballot:	No	
General Comments	The requirement to document non-conformance with an Entity's cyber security policy is sensible, but the requirement for a senior manager to approve all of those non-conformances is not. Some non-conformances may occur for reasons that are understood and knowingly tolerated for valid reasons. One could reasonably require the senior manager concerned to approve these, which effectively signals informed consent. However, there may be instances where a non-conformance occurs which represents an error that is not acceptable to the Entity concerned one which needs correcting rather than approval. Consider the wording, "Instances where the Responsible Entity accepts non-conformance with its cyber security policy…..".	Please see responses to Peter Henderson, Independent Electricity System Operator (IESO).
003-R1		
003-R2		
003-R3		
003-R4	R5 and R4 should be combined. Both talk about requirements to protect information about Critical Cyber Assets. In R4.3, it is unclear what is meant by the phrase, "cyber security protection controls". This could be taken as a reference to the sum-total of controls in place to ensure compliance with CIP-002 through CIP-009. If this is actually intended, the requirement to assess and document these controls annually appears to overlap many similar requirements throughout the standards (eg. the requirements in R1.3, R5.2, R5.3, and R6.1 of CIP-003, R3 and R4, of CIP-005, R7 of CIP-006, and R9 of CIP-007)	
003-R5	R5 and R4 should be combined. Both talk about requirements to protect information about Critical Cyber Assets. Requirements 5.1, 5.1.1, 5.1.2, and 5.1.3 are about managing access to the assets themselves, yet they appear as sub-bullets of a requirement to manage access to information about Critical Cyber Assets. This is confusing, particularly as there is no measure that relates to the management of access to the assets themselves.	
003-R6	R6.2 appears to require that testing be performed prior to promoting systems to production. It is unclear what the purpose and scope of that testing needs to be, and where those dimensions are documented. If this is a reference to testing required in CIP-007, this should be noted, or the reference to testing deleted in favour of a more thorough treatment in CIP-007. In R6.3, it is unclear what is meant by the qualifier "supporting" when referring to configuration management activities.	

R6.3 is redundant given the text of R6, and overlaps with the requirements of R6.2.

003-M1

003-M2

003-M3

003-M4

003-M5 Measures M4 and M5 should be reviewed in light of comment R4 and R5.

M5 refers to a policy for management of access to information. There is no corresponding requirement (R5 requires the establishment of a program).

003-M6

003-C1,1

003-C1,2

003-C1,3

003-C1,4 Section 1.4 under "Compliance" is somewhat unclear. The text appears to suggest that a Responsible Entity that does not fulfill one or more of the Standard's requirements should actually claim that it is fully compliant with the Standard if it has a properly documented exception to those requirements approved by the designated senior manager at the time of compliance reporting. Is this the intent?

003-C2,1 Requirement R 2.2 requires that changes to the designated senior manager must be documented within 30 days of the effective date. Compliance statement 2.1.1, however, states that an entity that fails to do so within 10 days is in non-compliance. This inconsistency should be resolved.

Compliance statement 2.1.1 imposes a requirement that is not identified in the requirements section. Specifically, 2.1.1 effectively imposes a requirement that the gap in designating a senior management representative be less than 10 days, which is not specified in the requirements section.

Requirement R1.4 requires annual review of the cyber security policy. This is not consistent with compliance statement 2.1.2 which suggests that an entity that reviews its policy every three years would be fully compliant.

Compliance statement 2.1.3 imposes a requirement that is not identified in the requirements section.

003-C2,2 Compliance statement 2.2.3 should refer to access privileges to information associated with Critical Cyber Assets to more clearly correspond to R5.2 and to avoid imposing a requirement to review access privileges to the Critical Cyber Assets themselves that is not identified in the Requirements section.

003-C2,3

003-C2,4 Compliance statement 2.4.3 should be revised to more clearly refer to a program for the identification and classification of information about Critical Cyber Assets.

Compliance statement 2.4.5 appears to duplicate 2.2.3 but at a different level of non-compliance

Compliance statement 2.4.6 imposes new requirements not specified in the Requirements section specifically to document access revocations and changes. The requirements only specify the need to confirm that access privileges that prevail at the time of review are appropriate, without reference to maintaining a history of how those privileges came about.

CIP-003 Drafting Team Responses to Comments

Name	Steven Townsend	
Entity	Consumers Energy Co.	
Ballot:	No	
General Comments	Consumers Energy has also submitted comments via the ECAR CIPP.	Please see reponses to Larry Conrad, ECAR CIPP.
003-R1		
003-R2		
003-R3		
003-R4		
003-R5		
003-R6		
003-M1		
003-M2		
003-M3		
003-M4		
003-M5		
003-M6		
003-C1,1		
003-C1,2		
003-C1,3		
003-C1,4		
003-C2,1		
003-C2,2		
003-C2,3		
003-C2,4		

CIP-003 Drafting Team Responses to Comments

Name	Martin Trence
Entity	Xcel Energy - Northen States Power (NSP)
Ballot:	Yes
General Comments	
003-R1	
003-R2	
003-R3	
003-R4	
003-R5	
003-R6	
003-M1	
003-M2	
003-M3	
003-M4	
003-M5	
003-M6	
003-C1,1	
003-C1,2	
003-C1,3	
003-C1,4	
003-C2,1	
003-C2,2	
003-C2,3	
003-C2,4	

CIP-003 Drafting Team Responses to Comments

Name	Rick Vermeers
Entity	Avistacorp
Ballot:	Yes
General Comments	
003-R1	
003-R2	
003-R3	
003-R4	
003-R5	
003-R6	
003-M1	
003-M2	
003-M3	
003-M4	
003-M5	
003-M6	
003-C1,1	
003-C1,2	
003-C1,3	
003-C1,4	
003-C2,1	
003-C2,2	
003-C2,3	
003-C2,4	

CIP-003 Drafting Team Responses to Comments

Name	Robert C. Webb	
Entity	Instrumentation, Systems and Automation Society	
Ballot:	No	
General Comments	1. Who is ISA and Why is ISA commenting on CIP-002 through CIP-009?	Regarding comment #2a, the exclusionary language concerning generation assets has been removed with the exception of nuclear generation which is excluded by the SAR. Because distribution assets are not considered part of the Bulk Electric System, these resources remain excluded as well. Regarding comment #2b, much of the prescriptive language on how certain security measures should be applied has been removed. For example, the requirement for port scans in CIP 005, R4.2 has been replaced by a requirement to review only ports and services required for operations are enabled. In addition, the Drafting Team has removed most references to "how" security measures should be applied throughout the Standards unless it is required for compliance purposes. Regarding comment #2c, language has been added to reflect the fact that some security solutions that are available today were not available when some legacy systems were designed and put into service. CIP-003, CIP- 004, CIP-005, and CIP-006 contain language addressing exceptions to their policies that may be required to deal with legacy systems and facilities where modern security solutions are not technically possible. In these cases, the Responsible Entities must identify and document the exception and describe the mitigating steps they are taking to secure the assets in lieu of the modern solution. Regarding the comments #3, #4, and #5 related to scope, the Standard reflects the Standard Authorization Request which excluded distribution, nuclear generation, and telecommunication infrastructure. The Drafting Team cannot exceed the scope of the SAR. A SAR reflects the industry consensus on the scope of any particular standard to be developed. Once SAR has been approved for standards drafting, the scope cannot be changed.

		The NERC Reliability Standards process would require new SARs to address these scope issues.
003-R1	Insert a new R1.2 The Responsible Entity's cyber security policy shall specifically address critical cyber assets used for monitoring and control, load and frequency control, emergency actions, contingency analysis, special protection systems, power plant control, substation control, and real-time information exchange as used by the Critical Assets defined in CIP-002. Insert a new R1.3 The Responsible Entity's cyber security policy relationships shall include, at a minimum, those organizational elements responsible for the design, operation, and maintenance of the subject Cyber Assets.	CIP-003 addresses Critical Cyber Assets as identified by the Responsible Entity pursuant to CIP-002. Defining organizational relationships is beyond the scope of this standard.
003-R2		
003-R3		
003-R4		
003-R5		
003-R6		
003-M1		
003-M2	Insert measures corresponding to the two new requirements identified above.	See responses above.
003-M3		
003-M4		
003-M5		
003-M6		
003-C1,1		
003-C1,2		
003-C1,3		
003-C1,4		
003-C2,1		
003-C2,2		
003-C2,3		
003-C2,4	2.4.2 Insert level 4 non-compliance corresponding to the new requirement for control systems policy identified above (new R1.2.), and for organizational participation (new R1.3).	See responses above.

CIP-003 Drafting Team Responses to Comments

Name	Laurent Webber	
Entity	Western Area Power Administration	
Ballot:	No	
General Comments		
003-R1	R1.4: Who is to review and approve the entity's cyber security policy? The requirement should be, "The senior manager responsible for leading and managing the entities implementation and adherence to the NERC CIP-002 through CIP-009 Standards shall review and approve the entity's cyber security policy."	R1 has been clarified to address this concern.
003-R2	Add this sentence, “The senior manager may delegate any of these responsibilities as desired and defined.”	This requirement is similar to Sarbanes-Oxley requirements. One senior manager needs to be responsible for ensuring that the requirements of these cyber security standards are being followed.
003-R3		
003-R4	R4: Identification and protection of information is adequate. The requirement to "classify" information implies that all information, regardless of context, be listed and classified as to type (i.e. public, confidential, etc.). Remove the word "classify" from R4. R4.2: This requirement is repetitive and unnecessary. Remove R4.2 because R4.1 clearly defines the requirement to identify and protect information. R4.3: Change the word "classification" to "protection".	R4.1 sets forth the types of information to be protected. R4.2 requires the classification of the information identified in R4.1 according to its sensitivity.
003-R5	R5: R5 seems to require managing access to information rather than to the Critical Cyber Assets themselves. Change "access to information" to "access to Critical Cyber Assets and information" R5.1.1: Remove the words "physical access". It will be impossible to meet this requirement if physical access is included. Switchmen from other entities are one example of what will make it impossible to implement.	CIP-003 addresses access to protected information regarding Critical Cyber Assets. CIP-004 addresses access to Critical Cyber Assets. R5.1 addresses logical or physical access to protected information regarding Critical Cyber Assets.
003-R6		
003-M1		
003-M2		
003-M3		
003-M4	Remove the word “classification” (see R4 comments above).	Measures have been reword to refer back to requirements. See response to R4 above.
003-M5		

003-M6	Does this imply that we have to keep all the testing documents?	Testing and related document retention is now covered in CIP-007.
003-C1,1		
003-C1,2		
003-C1,3		
003-C1,4		
003-C2,1	Compliance 2.1.4: Remove the word “classify” (see R4 comments above).	
003-C2,2		
003-C2,3		
003-C2,4		

CIP-003 Drafting Team Responses to Comments

Name	Michal Zeithammel
Entity	Brascan Power
Ballot:	Yes

General Comments

003-R1

003-R2

003-R3

003-R4

003-R5

003-R6

003-M1

003-M2

003-M3

003-M4

003-M5

003-M6

003-C1,1

003-C1,2

003-C1,3

003-C1,4

003-C2,1

003-C2,2

003-C2,3

003-C2,4

CIP-003 Drafting Team Responses to Comments

Name	Guy Zito	
Entity	NPCC	
Ballot:	No	
General Comments		
003-R1	R1 should be rewritten to "each Entity shall have a Cyber Security Policy that includes the following." NERC Standards should be focused on Reliability not management structure.	Please see responses to Ray A'Brial, Central Hudson Gas & Electric Corp.
003-R2	change R2 to "The Responsible Entity shall assign a senior manager or delegate(s) with responsibility"	
003-R3	Change R3 to "Exceptions - Instances where the Responsible Entity accepts non-conformance with its cyber security policy". The requirement to document non-conformance with an Entity's cyber security policy is sensible, but the requirement for a senior manager to approve all of those non-conformances is not. Some non-conformances may occur for reasons that are understood and knowingly tolerated for valid reasons. One could reasonably require the senior manager concerned to approve these, which effectively signals informed consent. However, there may be instances where a non-conformance occurs which represents an error that is not acceptable to the Entity concerned one which needs correcting rather than approval.	
003-R4	The minimum should not include everything. Remove ", and any related security information". Replace Requirement 4.3 with words from Requirement 5.2	
003-R5	Remove R5 because it overlaps Requirement 4 in CIP004 and Requirement 6.1 in CIP007. This overlap is confusing. It is not clear how Requirement 4 in CIP003 is different from this Requirement.	
003-R6	R6 should move to CIP007 otherwise the Drafting team to clarify its intent for including it here.	
003-M1		
003-M2		
003-M3		
003-M4		
003-M5	Remove M5 since R5 was removed	
003-M6	Move to CIP007 since R6 was moved to CIP007	
003-C1,1		

003-C1,2

003-C1,3

003-C1,4 This is confusing. We believe this refers to non-conformance with the Entity's cyber security policy.

003-C2,1 Compliance statement 2.1.1 imposes a requirement that is not identified in the requirements section. Specifically, 2.1.1 effectively imposes a requirement that the gap in designating a senior management representative be less than 10 days, which is not specified in the requirements section. Ten days was never specified before this.

Requirement R1.4 requires annual review of the cyber security policy. This is not consistent with compliance statement 2.1.2 which suggests that an entity that reviews its policy every three years would be fully compliant.

Compliance statement 2.1.3 imposes a requirement that is not identified in the requirements section.

Remove 2.2.3 since M5 was removed.

003-C2,2

003-C2,3

003-C2,4 Compliance statement 2.4.3 should be revised to more clearly refer to a program for the identification and classification of information about Critical Cyber Assets.

2.4.5 and 2.4.6 should be removed since they depend on M5, which we removed

CIP-004 Drafting Team Responses to Comments

Name	Raymond A'Brial
Entity	Central Hudson Gas & Electric Corp
Ready to Ballot:	No

General Comments	Change the purpose to "This standard requires that personnel having access to Critical Cyber Assets, including contractors and service vendors, have a higher level of personnel risk assessment, training and security awareness than personnel not provided access."	The purpose has been modified.
	Comment - access could be electronic, physical or both.	Access applies to either physical access, cyber access, or both.
	This Standard's compliance is too prescriptive. This Standard has 4 Requirements and 4 Measures. The first three Compliance Levels have at least 5 clauses.	The levels of noncompliance have been rewritten.
004-R1		
004-R2	R2.1 should be reworded to state "All personnel having access to Critical Cyber Assets shall have received cyber security training appropriate to their role."	The requirement has been clarified.
004-R3	Remove R3.1 since it is covered by R3.2.	R3.1 and R3.2 have been combined.
	Suggest that the correct order of these sections is R3 (risk assessment), R2 (training), R4 (access), and R1 (awareness).	
	Change the old R3.2.2 from five years to ten years to be consistent with with Federal security clearance.	Changed to 7 years to align with the retention period in the Fair Credit Reporting Act.
004-R4	R4.1 requires a quarterly review. This is too prescriptive and does not match M4. We recommend an annual review and signed by the person authorizing.	Changed to quarterly records in both sections for consistency. Frequent cross-checks of these records is critical to the success of the process -- mitigating potential unauthorized access to Critical Cyber Assets.
	Add R4.3 Unauthorized personnel must be escorted by authorized personnel	CIP-006 addresses this issue.
004-M1	Reorder to stay consistent with R1 - R4	Measures have been reworded to refer back to the requirements.
004-M2		
004-M3		
004-M4		
004-C1,1		
004-C1,2		
004-C1,3		

004-C1,4		
004-C2,1	Update 2.1.1 to remain consistent with R4.1 and M4. Failed to perform the annual review. Failure to document the personnel risk assessment gives rise to both Level 1 non-compliance (2.1.3) and Level 3 non-compliance (2.3.3). This is confusing and should be resolved.	Levels of noncompliance have been rewritten.
004-C2,2	Remove 2.2.1 since it is covered by the updated 2.1.1. Failure of the Training program to address two or more required items gives rise to non-compliance at Level 2 (2.2.3) and Level 3 (2.3.4). This is confusing and should be resolved.	Levels of noncompliance have been rewritten.
004-C2,3		
004-C2,4	Eliminate 2.3.7 since it is covered by 2.1.3.	Levels of noncompliance have been rewritten.

CIP-004 Drafting Team Responses to Comments

Name	Ori Artman	
Entity	Teltone	
Ready to Ballot:	Yes	
General Comments		
004-R1		
004-R2		
004-R3		
004-R4	7 days for change of status access OK 24 for personnel who is let go for cause - is this a sliding 24 hours from time of letting go? How about adding an instant shutdown of access for extreme cases?	24 hours upon termination is the minimum requirement. Responsible Entities may go beyond the minimum if they deemed it appropriate to do so.
004-M1		
004-M2		
004-M3		
004-M4		
004-C1,1		
004-C1,2		
004-C1,3		
004-C1,4		
004-C2,1		
004-C2,2		
004-C2,3		
004-C2,4		

CIP-004 Drafting Team Responses to Comments

Name	Steve Badgett
Entity	Riverside Public Utilitities
Ready to Ballot:	Yes

General Comments

004-R1

004-R2

004-R3

004-R4

004-M1

004-M2

004-M3

004-M4

004-C1,1

004-C1,2

004-C1,3

004-C1,4

004-C2,1

004-C2,2

004-C2,3

004-C2,4

CIP-004 Drafting Team Responses to Comments

Name	Terry Baker
Entity	Platte River Power Authority
Ready to Ballot:	Yes

General Comments

004-R1

004-R2

004-R3

004-R4

004-M1

004-M2

004-M3

004-M4

004-C1,1

004-C1,2

004-C1,3

004-C1,4

004-C2,1

004-C2,2

004-C2,3

004-C2,4

CIP-004 Drafting Team Responses to Comments

Name	Terry Bilke
Entity	Midwest ISO
Ready to Ballot:	No

General Comments

004-R1

004-R2

004-R3

004-R4

004-M1

004-M2

004-M3

004-M4

004-C1,1

004-C1,2

004-C1,3

004-C1,4

004-C2,1

004-C2,2

004-C2,3

004-C2,4

CIP-004 Drafting Team Responses to Comments

Name	Pat Bourassa	
Entity	Wisconsin Public Service Corporation	
Ready to Ballot:	No	
General Comments	What about emergency waivers? Storms and other disasters may require personnel from other utilities to access critical assets for restoration. This access may be unescorted. This section should note this special case.	Responsible Entities must include provisions for emergencies in their cyber security policies. Please refer to CIP-003, R1.1.
004-R1		
004-R2		
004-R3	R3.2.2 Change language to allow background investigations to be performed in a manner consistent with organizational policy and not necessarily every five years. Random selections or with cause should be considered. It appears as if there is only one level of background checks. In order to save dollars for the utilities, does it make more sense to have a lower level of background check performed for grandathered" employees?	The timeline has been changed to 7 years to align with the retention period in the Fair Credit Reporting Act. The level of checks is at the discretion of Responsible Entities, with the minimum defined as criminal check and identity verification. Personnel represent a significant vulnerability and periodic reassessment is useful in uncovering potentially serious problems that may otherwise be undiscovered or unobserved.
004-R4		
004-M1		
004-M2		
004-M3		
004-M4		
004-C1,1		
004-C1,2		
004-C1,3		
004-C1,4		
004-C2,1		
004-C2,2		
004-C2,3		
004-C2,4		

CIP-004 Drafting Team Responses to Comments

Name	Laurence W. Brown	
Entity	Edison Electric Institute	
Ready to Ballot:	No	
General Comments	There is no reference to exceptions in this Standard, though it is to be expected that the need for such exceptions will occur, particularly for natural disasters and law enforcement situations.	Responsible Entities must include provisions for emergencies in their cyber security policies. Please refer to CIP-003, R1.1.
004-R1		
004-R2		
004-R3	R3.1 and the opening paragraph of R3.2 appear to be the same. If they are intended to address different issues, then they must be clarified. Suggested Alternative Wording: "R3.1. The Responsible Entity shall, consistent with the Responsible Entity’s >< human resources requirements> in accordance with federal, state, provincial, and local laws, and subject to existing collective bargaining unit agreements<, subject all personnel having access to Critical Cyber Assets, including contractors and service vendors, to a documented personnel risk assessment process prior to granting authorized access to Critical Cyber Assets. "R3.2. >A reasonable< personnel risk assessment >program shall include the following elements:<" R3.1 – Also, the phrase "authorized access" could include escorted physical access in addition to "escorted" or monitored electronic access. If not, this should be clarified. R3.2.3 – The final phrase starting with the word "including" is unclear. It should be clarified that vendors and at least some contractors will conduct their own Personnel Risk Assessments, but will do so pursuant to standards set by the appropriate Responsible Entity.	These requirements have been combined.
004-R4	R4.1 – It is unclear how this will be applied to contractors and vendors, how their compliance will be monitored, and especially how it will be audited.	Requirement has been modified for clarity.
004-M1		
004-M2	It is unclear whether training is to be prior to any unescorted or unmonitored access, or if with certain period after such access (such as 90 calendar days). If so, then such restriction must be explicitly stated in the Requirement (such as at R2.1).	Measures have been rewritten to refer back to requirements. The requirements states that training is required within 90 days of access authorization.
004-M3		
004-M4		
004-C1,1		

CIP-004 Drafting Team Responses to Comments

004-C1,2		
004-C1,3		
004-C1,4		
004-C2,1	The phrase "not applied consistently" is unclear. Given that various methods of awareness training are permitted, it appears to refer to some time period or among different personnel, but neither is stated in the applicable Requirement. Suggested Alternative Wording: "2.1.5 Awareness program exists, but >is< not >conducted< within the minimum required period><."	Levels of noncompliance have been rewritten.
004-C2,2		
004-C2,3	C2.3.6 appears to be vastly over-reaching the authority of NERC or the Regions. Any audit would require access to confidential personnel records, and would involve judgements that no audit staff is trained, qualified, or authorized to make. If at all necessary, this should reference a prior, public, legally binding finding or other determination of behavior inconsistent with applicable requirement. Further, if such a determination has been made, this would appear to warrant moving the severity of the noncompliance to Level 4.	Levels of noncompliance have been rewritten.
004-C2,4	SEE C2.3.6, above.	Levels of noncompliance have been rewritten.

CIP-004 Drafting Team Responses to Comments

Name	Peter Burke	
Entity	American Transmission Company	
Ready to Ballot:	No	
General Comments	American Transmission Company concurs with the comments submitted separately by the Edison Electric Institute and by the Midwest Reliability Organization.	Please see responses to Laurence W. Brown, Edison Electric Institute.
004-R1		
004-R2	American Transmission Company concurs with the comments submitted separately by the Midwest Reliability Organization.	
004-R3	American Transmission Company concurs with the comments submitted separately by the Edison Electric Institute and by the Midwest Reliability Organization.	
004-R4	American Transmission Company concurs with the comments submitted separately by the Edison Electric Institute.	
004-M1		
004-M2	American Transmission Company concurs with the comments submitted separately by the Edison Electric Institute.	
004-M3		
004-M4		
004-C1,1		
004-C1,2		
004-C1,3		
004-C1,4		
004-C2,1	American Transmission Company concurs with the comments submitted separately by the Edison Electric Institute and by the Midwest Reliability Organization.	
004-C2,2	American Transmission Company concurs with the comments submitted separately by the Midwest Reliability Organization.	
004-C2,3	American Transmission Company concurs with the comments submitted separately by the Edison Electric Institute and by the Midwest Reliability Organization.	
004-C2,4	American Transmission Company concurs with the comments submitted separately by the Edison Electric Institute.	

CIP-004 Drafting Team Responses to Comments

Name	Marc Butts	
Entity	Southern Company	
Ready to Ballot:	No	
General Comments	Overall - The language seems to preclude the ability to contractually obligate vendors and contractors. The language consistently states that the responsible entity must maintain the records of other's employees.	This requirement has been clarified. Refer to FAQs.
004-R1		
004-R2		
004-R3	R3 - This requirement could potentially delay emergency system restoration when mutual aid resources are being used. An exemption for emergencies should be included. Normal fitness for duty and supervisory observation should be adequate in addressing continual personnel risk assessments	Responsible Entities must include provisions for emergencies in their cyber security policies. Please refer to CIP-003, R1.1.
	R3.2 - We suggest changing the phrase "being granted access to" to "being granted authorized access to".	R3.1 and R3.2 have been combined and this issue addressed.
	R3.2 - We suggest that the drafting team include the provision that persons "granted authorized access" may escort persons "without authorized access".	CIP-006 addresses this issue
004-R4	4.1 - When a vendor changes personnel, how would you know and how would you audit it? There needs to be a way to initiate a waiver during times of storms when outside personnel come in to work. Should the responsible entity be held in non-compliance if a vendor promotes, transfers, or terminates a field service rep that has access to these assets if the change is not made in 7 days? For its own employees, yes, but for vendor employees?	Responsible Entities should have processes in place with vendors to notify the Responsible Entity of personnel changes, if those personnel have access to Critical Cyber Assets. Furthermore, Responsible Entities must include provisions for emergencies in their cyber security policies. Please refer to CIP-003, R1.1.
	4.1 - In this section the word "lists" is used. In 4.1.1 - the word "list" is used. It is preferred to use "lists" so that entities with multiple companies would not be required to have just one list. Making this consistent throughout the standards will help.	Changed to “lists”.
	4.1 – We suggest replacing the phrase "or any change in the access rights of such personnel" to "or additions or deletions of access rights of such personnel".	Additions and deletions are changes.
	4.2 – We suggest replacing "within seven calendar days" to "within 14 calendar days" to allow for normal change in job responsibilities when some overlap is necessary.	7 days represents industry consensus.
004-M1		
004-M2		
004-M3		
004-M4		

CIP-004 Drafting Team Responses to Comments

004-C1,1		
004-C1,2		
004-C1,3		
004-C1,4		
004-C2,1	2.1.5 - The current language is vague and unclear. We suggest deleting the phrases "but not applied consistently or" and "of quarterly reinforcement" from this requirement.	Levels of noncompliance have been rewritten.
004-C2,2		
004-C2,3	2.3.6 Level 3 noncompliance - how is this measured or audited? NERC or regional audit teams should not have access to this type of information. Should this be deleted entirely?	Levels of noncompliance have been rewritten.
004-C2,4		

CIP-004 Drafting Team Responses to Comments

Name	Gary Campbell	
Entity	MAIN	
Ready to Ballot:	No	
General Comments	Need to address item below.	
004-R1		
004-R2		
004-R3		
004-R4	In reading CIP-003-1 R5. I wonder how this is requirement is not coverd there. It should not be in both places unless there is a very specific difference which can be clearly defined.	CIP-003 addresses the management of the process, while CIP-004 addresses the personnel subject to personnel risk assessment.
004-M1		
004-M2		
004-M3		
004-M4		
004-C1,1		
004-C1,2		
004-C1,3		
004-C1,4		
004-C2,1	2.1.5 "but not consistentlt appplied" should be deleted. This is very vague and hard to consistently measure. Reword to state " Awareness program exists but reinforced on a quarterly basis"	Levels of noncompliance have been rewritten.
004-C2,2	2.2.3 Delete "or more" , as written I could be both Level 2 and 3 non-compliant. 2.2.5 Delete "but is not consistently applied" be more specific	Levels of noncompliance have been rewritten.
004-C2,3	2.3.4 Delete "or more" , as written I could be both Level 2 and 3 non-compliant. 2.3.6 I do not think this is an easily measurable item and is probably out of the scope of this standard.	Levels of noncompliance have been rewritten.
004-C2,4	2.4.3 What does "NO cocumentation exist" mean? All required documemtation does not exist? If that is the case do you think there will be many entities that doe not have any documentation? It needs to be specific and try to achive some level of compliance and the regions should always be working to achive full compliance and therefore want the standards to try and help in that effort.	Levels of noncompliance have been rewritten.

CIP-004 Drafting Team Responses to Comments

Name	Linda Campbell	
Entity	FRCC	
Ready to Ballot:	No	
General Comments		
004-R1		
004-R2	R2.1 What does "access" to Critical Cyber Asset actually mean? For example, do service personnel that support HVAC equipment require training? We suggest that vendors or service personnel who need such access for more than 30 days receive training. Sample wording: "This program will ensure that all personnel having authorized access to Critical Cyber Assets, including contractors and service vendors requiring access for more than 30 days are trained."	Authorized access has been clarified. Untrained personnel with authorized cyber or authorized unescorted physical access to Critical Cyber Assets represent a significant vulnerability. Please refer to FAQs.
	The standards draft team should create an R2.2.5 "Security and Cyber Security incident reporting" to maintain consistency within the standards.	Cyber Security Incident Reporting is covered in CIP 008.
004-R3	Is a personnel risk assessment necessary for service contractors who need access for short limited time (less than 30 days)? This assessment is not practical for short term vendors.	Unassessed personnel who have authorized access to Critical Cyber Assets represent a significant vulnerability. Industry consensus supports this position. Please refer to FAQs.
	R3.2.1 The five year criminal check is to what depth; local law enforcement, state law enforcement, all 50 states law enforcement, FBI, Interpol, last 5 year residences and neighboring states?	The requirement defines the minimum and states "Responsible Entities may conduct more detailed reviews...."
	R3.2.2 We believe the "every five years" criteris will be ectremely costly and is unneccessary. However, if it remains it should be phased in over a longer time period for implementation than in the current plan. Proposed wording for the R3.2.2 would be: R3.2.2. The Responsible Entity shall update personnel risk assessments at the following intervals: 1. Seventh year of employment 2. Fifteenth year of employment 3. Every eighth year after the fiftheenth year of employment 4. For casue.	Changed to every 7 years.
	R3.2.3 The FAQ indicates that the responsible entity must only ensure (via audit) that background screening is performed for third parties, in which case the responsible entity would not have those records. Many of our vendors have already indicated they will perform background checks, but will not provide records about their employees to us. However, the Requirement R3.2.3 indicates the Responsible Entity will document the results. The requirements should specifically address third parties, not leave this to the FAQ's. Suggest changing R3.2.3 to address only employees and change wording from "having authorized access" to "having or requesting authorized access"	Access to the results of the personnel risk assessment are not needed for documentation by the Responsible Entity. The Responsible Entity must ensure that personnel risk assessments for service vendors and contractors are conducted pursuant to the requirements of the standard.Please see the FAQs.
		See response above.

	Add R3.2.4 The Responsible Entity shall contractually obligate vendors to perform the background checking of contract and service-vendor personnel with access to Critical Cyber Assets. If an Audit requirement is included, then guidance on what the audit must include should be provided, i.e. is a statistical sampling enough, what constitutes the documentation of an audit, etc.	
004-R4		
004-M1	Delete duplicate "program" wording.	Done.
004-M2		
004-M3		
004-M4		
004-C1,1	In the applicability section 4.1.10 and 4.1.11, RRO's and NERC are included. Who has the monitoring responsibility for a RRO or NERC?	NERC will monitor the RROs and a third party without vested interest in the outcome will monitor NERC.
	Add Self-Certification and Audit information to this section. Proposed language would be: 1.1. Complaince Monitoring Responsibility Regional Reliability Organization. 1.1.1. The Compliance Monitor will request a self-certification annually. 1.1.2. The Compliance Monitor will perform an audit at least once every three (3) calendar years.	Self-certification has been added under "Additional Compliance Information."
004-C1,2		
004-C1,3	D1.3.1 Retention requirements seem excessive. What is the rationale for keeping 3 years past end of employment? One year past "having approved access to critical cyber assets" seem more than enough. Once updated, can previous personnel risk assessment records be destroyed? Would suggest changing to "… shall keep personnel risk assessment documents in accordance with the company's policy for retaining such employee records."	Data retention has been changed to "in accordance with federal, state, provincial, and local laws."
004-C1,4		
004-C2,1	D2. It would be more consistent if the items under levels of non-compliance were listed in the same order as the requirements or measures as they are in the other standards.	Levels of noncompliance have been rewritten.
	D2. The threshold of non-compliance levels should address the size of a corporation. The non-compliances of a company that has 5 instances of terminations not begin handled within 24 hours for cause when only 10 personnel have access to critical cyber assets versus a company that has 5 instances of terminations not begin handled within 24 hours for cause where 1,000 personnel have access is significantly different. Perhaps some percentage could be used instead of a number.	
	D2.1.2, D2.2.2, D2.3.2 The requirement is to revoke access within 24 hours (and appropriately so), not to update the access control list within 24 hours. All of these compliance statements should be changed to "…. in which access to critical cyber assets was not revoked within 24 hours….."	

	D2.2.1 "Access control document: is not referenced in this standard. If you are referring to list of personnel with access, copy verbiage of D2.1.1 and change the time period to 6-12 months. D2.3.6 "Adverse employment actions" and "hiring or retention of employees" are not mentioned in any requirement of this standard. This compliance level should be deleted or reworded to match a requirement. D2.3.7 Delete the word "update" or change to "Updated"	
004-C2,2		
004-C2,3	Level 3 assumes that an Awareness program exists.	Levels of noncompliance have been rewritten.
004-C2,4	Level 4 assumes that an Awareness program and Access lists exist. D2.4.3. Should be changed, it could be interpreted that if even one document exists, the non-compliance level would be level 3, and not level 4.	Levels of noncompliance have been rewritten.

Name	Roger Champagne	
Entity	Hydro-Québec TransÉnergie	
Ready to Ballot:	No	
General Comments	Change the purpose to "This standard requires that personnel having access to Critical Cyber Assets, including contractors and service vendors, have a higher level of personnel risk assessment, training and security awareness than personnel not provided access." Comment - access could be electronic, physical or both. This Standard's compliance is too prescriptive. This Standard has 4 Requirements and 4 Measures. The first three Compliance Levels have at least 5 clauses.	Please see response to Ray A'Brial, Central Hudson Gas & Electric Corp.
004-R1		
004-R2	R2.1 should be reworded to state "All personnel having access to Critical Cyber Assets shall have received cyber security training appropriate to their role."	
004-R3	We suggest the Drafting team combine and clarify R3.1 with/to R3.2. Suggest that the correct order of these sections is R3 (risk assessment), R2 (training), R4 (access), and R1 (awareness). Change the old R3.2.2 from five years to ten years to be consistent with with Federal security clearance.	
004-R4	R4.1 requires a quarterly review. This is too prescriptive and does not match M4. We recommend an annual review and signed by the person authorizing. Add R4.3 Unauthorized personnel must be escorted by authorized personnel	
004-M1	Reorder to stay consistent with R1 - R4	
004-M2		
004-M3		
004-M4		
004-C1,1		
004-C1,2		
004-C1,3		
004-C1,4		

CIP-004 Drafting Team Responses to Comments

004-C2,1 Update 2.1.1 to remain consistent with R4.1 and M4. Change the words from "for more than three months but less than six months;

to

annually.

Failure to document the personnel risk assessment gives rise to both Level 1 non-compliance (2.1.3) and Level 3 non-compliance (2.3.3). This is confusing and should be resolved.

004-C2,2 Remove 2.2.1 since it is covered by the updated 2.1.1.

Failure of the Training program to address two or more required items gives rise to non-compliance at Level 2 (2.2.3) and Level 3 (2.3.4). This is confusing and should be resolved.

004-C2,3 Eliminate 2.3.7 since it is covered by 2.1.3.

004-C2,4

Name	Larry Conrad
Entity	Cinergy
Ready to Ballot:	No

General Comments

004-R1	Cyber Security Awareness reinforcement is required quarterly, in addition to the annual training requirements of R2. The quarterly awareness reinforcement is redundant and excessive and should be eliminated.	An awareness program and an annual training program are uniquely different. These differences are reflected in the requirements.
004-R2	R2.1 Change this sentence to read: "This program will ensure that all personnel having un-escorted authorized access to Critical Cyber assets, including contractors and service vendors are trained." We expect that all access will be authorized, but that training will be required if the access is un-escorted.	R2 has been modified for clarity.
	CIP 004-1, R2.3: Add that where contractual agreements specify training, training documentation may be kept by the vendor or contractor.	The requirement does not preclude such arrangements. Vendors and service providers must be trained in accordance with R2.2.
004-R3	This section describes a personnel risk assessment. Remove the words "…and five year criminal check…" from requirement R.3.2.1.	The requirement has been renumbered to R3.1 and refers to a 7-year criminal check.
	Sections R3.1 and 3.2 are nearly redundant. The group thought perhaps the writers' point in R3.1 is that the Responsible Entity must conduct the personnel risk assessment and the writer's point in R3.2 is that the Responsible Entity must document that the personnel risk assessment was done. If this is the case, then the language needs to be clear. Un-necessary redundancies should also be combined.	R3.1 and R3.2 have been combined.
004-R4	These standards include numerous and extensive documentation and review requirements. In general annual reviews are required, with updates required within 90 days of the change occurring. Several required timeframes are presently shorter than this and should be increased so that all timeframes throughout the standard are consistent and reasonable, and to make compliance more manageable:	The timeframes have been reviewed and standardized where appropriate. Frequency of reviews and updates represent industry consensus.
	CIP-004- R4.1 – List of authorized personnel with access to Critical Cyber Assets must be reviewed at least quarterly, and updated within 7 days of a change of personnel or access rights. These timeframes are much too short to be practical for remote substations. At substations, changes may require replacing keys or changing locks. Annual review and update within 30 days for normal change of status should be acceptable for routine personnel changes for substation personnel.	This requirement is to update the lists.
	CIP-004- R4.2 – Physical and electronic access to Critical Cyber Assets must be revoked within 24 hours for termination with cause and within 7 days for personnel who have a change of status where they are no longer allowed access to Critical Cyber Assets. These timeframes are much too short to be practical for remote substations. At substations, changes may require replacing keys or changing locks. Timeframes of 7 days for termination	Personnel with unauthorized "unescorted" physical and cyber access to Critical Cyber Assets represent a significant vulnerability to the Critical Cyber Asset. Industry consensus supports these timeframes.

	with cause and 30 days for change of status would be more reasonable for substation personnel.	
004-M1		
004-M2		
004-M3		
004-M4		
004-C1,1		
004-C1,2		
004-C1,3	Data Retention The requirement that the responsible entity retain the personnel risk assessment documents for the duration of employee employment plus 3 years is too long. Change the data retention requirement to be 3 years data retention.	Data retention has been changed.
004-C1,4		
004-C2,1	Levels of non-compliance 2.1.2 and 2.2.2 and 2.3.2 One (1) instance in which access control list was not updated within the timing requirements creates a Level 1 non-compliance event. We believe this is too harsh. We recommend that the Level 1 violation for 1 instance should be removed. We recommend moving the Level 2 violation identified in 2.2.2 (more than 1 but not more than 5 instances) from Level 2 to Level 1. We also recommend moving the Level 3 violation identified in 2.3.2 (more than 5 instances) from Level 3 to Level 2 violation.	Levels of noncompliance have been rewritten.
004-C2,2	Compliance 2.2.1 "Access control documents(s)…have not been updated or reviewed…" Please specify what documents. Does this mean the list of personnel with account control rights? If so, please specify.	Levels of noncompliance have been rewritten.
004-C2,3		
004-C2,4		

CIP-004 Drafting Team Responses to Comments

Name	Larry Conrad	
Entity	ECAR Critical Infrastructure Protection Panel	
Ready to Ballot:	No	
General Comments		
004-R1		
004-R2		
004-R3	Sections R3.1 and R3.2 are nearly redundant. The group thought perhaps the writer's point in R3.1 is that the Responsible Entity must conduct the personnel risk assessment and writer's point in R3.2 is that the Responsible Entity must document that the personnel risk assessment was done. If this is the case, the language needs to be clear. Un-necessary redundancies should also be combined. R3.2.1 - This section describes a personnel risk assessment. Remove the words "…and five year criminal check…" from requirement R3.2.1. Criminal check is not part of a normal personnel risk assessment and the reference to it needs to be removed.	Please see responses to Larry Conrad, Cinergy.
004-R4	CIP-004-1, .R4.1 – List of authorized personnel with access to Critical Cyber Assets must be reviewed at least quarterly, and updated within 7 days of a change of personnel or access rights. These timeframes are too short to be practical for remote substations. At substations, changes may require replacing keys or changing locks. Annual review and update within 30 days for normal change of status should be acceptable for routine personnel changes for substation personnel. CIP-004-1, .R4.2 – Physical and electronic access to Critical Cyber Assets must be revoked within 24 hours for termination with cause and within 7 days for personnel who have a change of status where they are no longer allowed access to Critical Cyber Assets. At substations, changes may require replacing keys or changing locks. Timeframes of 7 days for termination with cause and 30 days for change of status would be more reasonable for substation personnel.	
004-M1		
004-M2		
004-M3		
004-M4		

CIP-004 Drafting Team Responses to Comments

004-C1,1

004-C1,2

004-C1,3 1.3.1. Data Retention
The requirement that the responsible entity retain the personnel risk assessment documents for the duration of employee employment plus 3 years is too long. We recommend changing the data retention requirement to be 3 years data retention.

004-C1,4

004-C2,1 C2.1.2 - One (1) instance in which access control list was not updated within the timing requirements creates a Level 1 non-compliance event. We believe this is too harsh. We recommend that the Level 1 violation for 1 instance should be removed.

004-C2,2 C2.2.2 - We recommend moving the Level 2 violation identified in 2.2.2 (more than 1 but not

more than 5 instances) from Level 2 to Level 1.

004-C2,3 C2.3.2 - We recommend moving the Level 2 violation identified in 2.3.2 (more than 5 instances) from Level 3 to Level 2.

004-C2,4

CIP-004 Drafting Team Responses to Comments

Name	Theodore Creedon, P.E.	
Entity	Creedon Engineering	
Ready to Ballot:	No	
General Comments		
004-R1		
004-R2		
004-R3	Duplication of effort for vendors and service contractors working for different utilities. There needs to be an acceptable standard common to all utilities.	Contractors and service vendors must satisfy the requirements of each Responsible Entity. Mandating contractual arrangements is beyond the scope of this standard.
004-R4		
004-M1		
004-M2		
004-M3		
004-M4		
004-C1,1		
004-C1,2		
004-C1,3		
004-C1,4		
004-C2,1		
004-C2,2		
004-C2,3		
004-C2,4		

CIP-004 Drafting Team Responses to Comments

Name	Joel De Granda	
Entity	Florida Power and Light	
Ready to Ballot:	No	
General Comments		
004-R1		
004-R2	R2.1 What does "access" to Critical Cyber Asset actually mean? For example, do service personnel that support HVAC equipment require training? We suggest that vendors or service personnel who need such access for more than 30 days receive training. Sample working: "This program will ensure that all personnel having authorized access to Critical Cyber Assets, including contractors and service vendors requiring access for more than 30 days are trained."	Please see response to Linda Campbell, FRCC.
004-R3	Is a personnel risk assessment necessary for service contractors who need access for short limited time (less than 30 days)? This assessment is not practical for short term vendors.	
004-R4		
004-M1		
004-M2		
004-M3		
004-M4		
004-C1,1		
004-C1,2		
004-C1,3		
004-C1,4		
004-C2,1		
004-C2,2		
004-C2,3		
004-C2,4		

CIP-004 Drafting Team Responses to Comments

Name	Richard Engelbrecht	
Entity	RGE	
Ready to Ballot:	No	
General Comments	Change the purpose to "This standard requires that personnel having access to Critical Cyber Assets, including contractors and service vendors, have a higher level of personnel risk assessment, training and security awareness than personnel not provided access." Comment - access could be electronic, physical or both. This Standard's compliance is too prescriptive. This Standard has 4 Requirements and 4 Measures. The first three Compliance Levels have at least 5 clauses.	Please see responses to Ray A'Brial, Central Hudson Gas & Electric Corp.
004-R1		
004-R2	R2.1 should be reworded to state "All personnel having access to Critical Cyber Assets shall have received cyber security training appropriate to their role."	
004-R3	NPCC Participating Members suggest the Drafting team combine and clarify R3.1 with/to R3.2. Suggest that the correct order of these sections is R3 (risk assessment), R2 (training), R4 (access), and R1 (awareness). Change the old R3.2.2 from five years to ten years to be consistent with with Federal security clearance.	
004-R4	R4.1 requires a quarterly review. This is too prescriptive and does not match M4. We recommend an annual review and signed by the person authorizing. Add R4.3 Unauthorized personnel must be escorted by authorized personnel	
004-M1	Reorder to stay consistent with R1 - R4	
004-M2		
004-M3		
004-M4		
004-C1,1		
004-C1,2		
004-C1,3		
004-C1,4		

CIP-004 Drafting Team Responses to Comments

004-C2,1 Update 2.1.1 to remain consistent with R4.1 and M4. Change the words from "for more than three months but less than six months;

to

annually.

Failure to document the personnel risk assessment gives rise to both Level 1 non-compliance (2.1.3) and Level 3 non-compliance (2.3.3). This is confusing and should be resolved.

004-C2,2 Remove 2.2.1 since it is covered by the updated 2.1.1.

Failure of the Training program to address two or more required items gives rise to non-compliance at Level 2 (2.2.3) and Level 3 (2.3.4). This is confusing and should be resolved.

004-C2,3

004-C2,4 Eliminate 2.3.7 since it is covered by 2.1.3.

CIP-004 Drafting Team Responses to Comments

Name	Ken Fell	
Entity	New York ISO	
Ready to Ballot:	No	
General Comments	Change the purpose to "This standard requires that personnel having access to Critical Cyber Assets, including contractors and service vendors, have a higher level of personnel risk assessment, training and security awareness than personnel not provided access." Comment - access could be electronic, physical or both. This Standard's compliance is too prescriptive. This Standard has 4 Requirements and 4 Measures. The first three Compliance Levels have at least 5 clauses.	Please see responses to Ray A'Brial, Central Hudson Gas & Electric Corp.
004-R1		
004-R2	R2.1 should be reworded to state "All personnel having access to Critical Cyber Assets shall have received cyber security training appropriate to their role."	
004-R3	We suggest the Drafting team combine and clarify R3.1 with/to R3.2. Suggest that the correct order of these sections is R3 (risk assessment), R2 (training), R4 (access), and R1 (awareness). Change the old R3.2.2 from five years to ten years to be consistent with with Federal security clearance.	
004-R4	R4.1 requires a quarterly review. This is too prescriptive and does not match M4. We recommend an annual review and signed by the person authorizing. Add R4.3 Unauthorized personnel must be escorted by authorized personnel	
004-M1	Reorder to stay consistent with R1 - R4	
004-M2		
004-M3		
004-M4		
004-C1,1		
004-C1,2		
004-C1,3		
004-C1,4		

004-C2,1

Update 2.1.1 to remain consistent with R4.1 and M4. Change the words from "for more than three months but less than six months;

to

annually.

Failure to document the personnel risk assessment gives rise to both Level 1 non-compliance (2.1.3) and Level 3 non-compliance (2.3.3). This is confusing and should be resolved.

004-C2,2

Remove 2.2.1 since it is covered by the updated 2.1.1.

Failure of the Training program to address two or more required items gives rise to non-compliance at Level 2 (2.2.3) and Level 3 (2.3.4). This is confusing and should be resolved.

004-C2,3

004-C2,4

Eliminate 2.3.7 since it is covered by 2.1.3.

CIP-004 Drafting Team Responses to Comments

Name	Francis Flynn	
Entity	National Grid USA	
Ready to Ballot:	No	
General Comments	Change the purpose to "This standard requires that personnel having access to Critical Cyber Assets, including contractors and service vendors, have a higher level of personnel risk assessment, training and security awareness than personnel not provided access." Comment - access could be electronic, physical or both. This Standard's compliance is too prescriptive. This Standard has 4 Requirements and 4 Measures. The first three Compliance Levels have at least 5 clauses.	Please see responses to Ray A'Brial, Central Hudson Gas & Electric Corp.
004-R1		
004-R2	R2.1 should be reworded to state "All personnel having access to Critical Cyber Assets shall have received cyber security training appropriate to their role."	
004-R3	NPCC Participating Members suggest the Drafting team combine and clarify R3.1 with/to R3.2. Suggest that the correct order of these sections is R3 (risk assessment), R2 (training), R4 (access), and R1 (awareness). Change the old R3.2.2 from five years to ten years to be consistent with with Federal security clearance.	
004-R4	R4.1 requires a quarterly review. This is too prescriptive and does not match M4. We recommend an annual review and signed by the person authorizing. Add R4.3 Unauthorized personnel must be escorted by authorized personnel	
004-M1	Reorder to stay consistent with R1 - R4	
004-M2		
004-M3		
004-M4		
004-C1,1		
004-C1,2		
004-C1,3		
004-C1,4		

CIP-004 Drafting Team Responses to Comments

004-C2,1 Update 2.1.1 to remain consistent with R4.1 and M4. Change the words from "for more than three months but less than six months;

to

annually.

Failure to document the personnel risk assessment gives rise to both Level 1 non-compliance (2.1.3) and Level 3 non-compliance (2.3.3). This is confusing and should be resolved.

004-C2,2 Remove 2.2.1 since it is covered by the updated 2.1.1.

Failure of the Training program to address two or more required items gives rise to non-compliance at Level 2 (2.2.3) and Level 3 (2.3.4). This is confusing and should be resolved.

004-C2,3

004-C2,4 Eliminate 2.3.7 since it is covered by 2.1.3.

CIP-004 Drafting Team Responses to Comments

Name	Greg Fraser	
Entity	Manitoba Hydro	
Ready to Ballot:	No	
General Comments	Introduction 4.2.3 should read the same as in CIP-009-1 which is: "Responsible Entities that, in compliance with Standard CIP-002, identify that they have no Critical Cyber Assets."	Introduction has been changed.
004-R1		
004-R2	Suggested wording "…service vendors are appropriately trained."	Requirement has been clarified.
004-R3	R3.1 & R3.2 are mostly redundant and could be combined in one requirement.	These requirements have been combined.
004-R4	R4.1 suggest reversing order quarterly review or within seven days and perhaps including in two separate requirements or at least two sentences.	The requirement has been clarified.
	The requirement deals with authorized access what about other's perhaps adding "…all others must be escorted".	The requirements states “authorized cyber or authorized unescorted physical access. It is reasonable to assume all others must be escorted or otherwise supervised.
	R4.2 the examples should perhaps be split up by "for cause" and "change of status".	R4.2 has been clarified.
004-M1	Delete 2nd word "program".	Done.
004-M2	Remove 2nd "Responsible Entity".	Done.
004-M3	Measures have been rewritten to refer back to the requirements.	Measures have been rewritten to refer back to the requirements.
004-M4		
004-C1,1		
004-C1,2		
004-C1,3		
004-C1,4		
004-C2,1		
004-C2,2		
004-C2,3		
004-C2,4		

CIP-004 Drafting Team Responses to Comments

Name	Jerry Freese	
Entity	American Electric Power	
Ready to Ballot:	No	
General Comments	Based on the expanded scope set forth in CIP-002 R1 for the Critical Assets and the subsequently expanded scope of the Critical Cyber Assets and the Electronic Security Perimeter, it would be impractical and infeasible to meet the obligations set forth in this requirement.	The scope of CIP-002 R1 has been changed.
004-R1		
004-R2		
004-R3		
004-R4		
004-M1		
004-M2		
004-M3		
004-M4		
004-C1,1		
004-C1,2		
004-C1,3		
004-C1,4		
004-C2,1		
004-C2,2		
004-C2,3		
004-C2,4		

CIP-004 Drafting Team Responses to Comments

Name	Edwin C. Goff III	
Entity	Progress Energy	
Ready to Ballot:	No	
General Comments		
004-R1	Recommend security awareness training to be bi-annual versus quarterly.	An awareness program is an effective way to reinforce sound cyber security practices and procedures. Awareness is less rigorous than training and quarterly reinforcement should not be burdensome, especially in light of the benefit.
004-R2	Would personnel that are outside of System Control Centers that have VIEW-ONLY display access of EMS generation and transmission data for informational purposes only be required to participate in Cyber Security training program? These personnel do not have direct interactive access to System Control Center "critical cyber assets", they access VIEW-ONLY displays from PC's that receive copies of EMS data. However in that they have visual access to bulk electric information would they be required to participate in the Cyber Security programs?	Per requirement, users of the remote display screens would not need training. However, Responsible Entities may go beyond these minimum requirements if they deem it appropriate to do so.
	Recommend initial cyber security training per R2, then refresher training every other year, unless major changes in the program necessitate re-training.	Annual training represents industry consensus.
004-R3	Recommend the 5 year Criminal History check and SSN verification be performed during the hiring process or prior to granting access to the cyber asset and should waive the requirement for existing personnel. Behavior observation programs or other programs that detect aberrant behavior should be used in lieu of additional checks on a 5 year cycle. These factors should drive the need to update the risk assessment (for cause, after a conviction, or after any other incident is evaluated, etc.)	The requirement has been changed 7 years for the update of personal risk assessments. Personnel represent a significant vulnerability and periodic reassessment is useful in uncovering potentially serious problems that may not otherwise be discovered. Please refer to FAQs for grandfathering of existing staff.
004-R4	4.1 requires quarterly reviews of "the list" of all authorized personnel - and an update within 7 days if changes in access or access rights are noted or within 24 hours if the reasons are for-cause. This will be very hard to administer especially with contractors who may have only infrequent access to the asset. All contractual agreements with our vendors will need to be revised to reflect written notification of personnel changes. The RE can respond to requests within these time frames, but a process like this relies heavily on supervisors and contractors to notify appropriate personnel and normally leaves many opportunities for improvement.	24 hours for cause represents industry consensus. Responsible Entities should have processes in place with vendors to notify the Responsible Entity of personnel changes, if those personnel have access to Critical Cyber Assets.
004-M1		
004-M2		
004-M3		
004-M4		

CIP-004 Drafting Team Responses to Comments

004-C1,1		
004-C1,2		
004-C1,3	1.3.1 Documentation retention should not exceed 5 years - Evidence that the check was performed could be provided thru a database or other tracking tool that documents that personnel with access to critical assets have undergone screening), but the old hardcopy records should not have to be maintained longer than 5 years.	Data retention has been changed.
004-C1,4		
004-C2,1	2.1.2 -- This indicates a non-compliance when access and the access control list is not updated in 24 hours. It is unclear whether "Access control list" this is referring to the "document" which lists all authorized personnel or if this is referring to the actual "electronic access control list". If the access control list is referring to updating the "document", this is in conflict with requirements R4.1. Although it is reasonable to expect that physical & electronic access has been revoked or updated in 24 hours, it is not reasonable to expect administrative records to be updated within a day. Additionally, if contract or service provider personnel was terminated internally by the Contractor, they may not provide notice to the utility within 24-hours of the termination. Suggest editing item 2.1.2 to delete the reference to update the access control list within 24-hours as follows: 2.1.2 One instance of personnel termination (employee, contractor or service provider) in which access was not updated within 24 hours for cause or upon notification by contractor that personnel had been terminated; or the access control list document was not updated within seven calendar days of any personnel change.	Levels of noncompliance have been rewritten.
004-C2,2		
004-C2,3		
004-C2,4		

CIP-004 Drafting Team Responses to Comments

Name	Kenneth Goldsmith	
Entity	Alliant Energy	
Ready to Ballot:	No	
General Comments		
004-R1		
004-R2	R2.2.4 requires that all the personnel that have access to critical cyber assets be trained on the procedures used to recover those assets following an incident. Thyis requirement is too broad, as it apparently includes all people that use these assets in addition to the IT people that would largely be responsible for restoring them. The requirement should be that all individuals "that have a role in restoration procedures" be trained in those roles.	R2 has been clarified.
004-R3	R3.2.2 appears to require that existing employees go through a background screening, including criminal records check, at least every 5 years. This should be eliminated as a requirement and left to companies corporte policies relating to it. R3.2.2 should be rewritten to indicate: "The Responsible Entity shall document a procedure defining the process to be used to update personnel risk assessments, and shall be able to demonstrate that the procedure is being followed." Responsible Entities should also be given the option of grandfathering existing employees, as they see fit.	The requirement has been changed to 7 years for the update of personal risk assessments to align with the retention period in the Fair Credit Reporting Act. Personnel represent a significant vulnerability and periodic reassessment is useful in uncovering potentially serious problems that may not otherwise be discovered. Please refer to FAQs for grandfathering of existing staff.
004-R4		
004-M1		
004-M2		
004-M3		
004-M4		
004-C1,1		
004-C1,2		
004-C1,3		
004-C1,4		
004-C2,1		
004-C2,2		
004-C2,3		
004-C2,4		

CIP-004 Drafting Team Responses to Comments

Name	Kathleen Goodman	
Entity	ISO New England Inc	
Ready to Ballot:	No	
General Comments		
004-R1		
004-R2	R2.2.4 Such training sould be able to be limited to those who have a designated role in inicident management and recovery.	The requirement has been clarified.
004-R3	R3.2.1 & R3.2.2 should be changed to ten years to be consistent with federal government requirements for security clearances.	The requirement was changed to 7 years to align with the Fair Credit Reporting Act.
004-R4	R4.1 should be changed to "annually."	Frequent cross-checks of these records is critical to mitigating potential unauthorized access to Critical Cyber Assets.
	R4.2 should be changed to "revoke physical and electronic access through the perimeters with...".	R4.2 has been clarified.
004-M1		
004-M2		
004-M3		
004-M4		
004-C1,1		
004-C1,2		
004-C1,3	It is not clear when you mean documents, records, or data. These are three distinct items and should not be referenced interchangeably. Please clarify.	The Drafting Team has revised the standards for consistency. Please see FAQs.
004-C1,4		
004-C2,1		
004-C2,2		
004-C2,3	2.3.6 We do not understand what is meant by an "adverse employment action." Please calrify.	This term has been removed.
004-C2,4		

CIP-004 Drafting Team Responses to Comments

Name	Tim Hattaway
Entity	Alabama Electric Cooperative
Ready to Ballot:	Yes

General Comments

004-R1

004-R2

004-R3

004-R4

004-M1

004-M2

004-M3

004-M4

004-C1,1

004-C1,2

004-C1,3

004-C1,4

004-C2,1

004-C2,2

004-C2,3

004-C2,4

CIP-004 Drafting Team Responses to Comments

Name	Jerry Heeren
Entity	MEAG Power
Ready to Ballot:	Yes

General Comments

004-R1

004-R2

004-R3

004-R4

004-M1

004-M2

004-M3

004-M4

004-C1,1

004-C1,2

004-C1,3

004-C1,4

004-C2,1

004-C2,2

004-C2,3

004-C2,4

Name	Peter Henderson	
Entity	Independent Electricity System Operator (IESO)	
Ready to Ballot:	No	
General Comments	Change the purpose to "This standard requires that personnel having access to Critical Cyber Assets, including contractors and service vendors, have a higher level of personnel risk assessment, training and security awareness than personnel not provided access." Comment - access could be electronic, physical or both.	The purpose has been clarified. Agreed.
004-R1		
004-R2	R2.1 should be reworded to state "All personnel having access to Critical Cyber Assets shall have received cyber security training or shall be escorted by personnel who have had such training."	The requirement has been clarified.
004-R3	1. The text of R3.1 and R3.2 overlap somewhat. The two requirements should be combined into one statement and the remaining sections re-numbered. 2. R3.1 and R3.2 should be reworded to be applicable only to personnel, vendors and contractors who are granted unescorted access to Critical Cyber Assets.	R3.1 and R3.2 have been combined. R3 has been clarified to "personnel having authorized cyber or authorized unescorted physical access."
004-R4	1. R4 requires quarterly review of access lists, where as M4 suggests that annual review is sufficient. The discrepancy should be resolved. 2. Add R4.3 Unauthorized personnel must be escorted by authorized personnel.	Measures have been reworded to refer back to requirements. CIP-006 addresses this issue.
004-M1	Reorder to stay consistent with R1 - R4	Measures have been reworded to refer back to requirements.
004-M2		
004-M3		
004-M4		
004-C1,1		
004-C1,2		
004-C1,3		
004-C1,4		
004-C2,1	1. Update 2.1.1 to remain consistent with R4.1 and M4. Change the words from "for more than three months but less than six months; to	Levels of noncompliance have been rewritten.

	annually. 2. Failure to document the personnel risk assessment gives rise to both Level 1 non-compliance (2.1.3) and Level 3 non-compliance (2.3.3). This is confusing and should be resolved. 3. If documentation of the personnel risk assessment program reveals that the program fails to require risk assessment updates every 5 years, a Responsible Entity could legitimately claim non-compliance at Level 1 (2.1.3) whereas 2.3.7 characterizes this as Level 3 non-compliance. This is confusing and should be resolved.	
004-C2,2	1. Remove 2.2.1 since it is covered by the updated 2.1.1. 2. Failure of the Training program to address two or more required items gives rise to non-compliance at Level 2 (2.2.3) and Level 3 (2.3.4). This is confusing and should be resolved.	Levels of noncompliance have been rewritten.
004-C2,3	1. Failure to document the personnel risk assessment gives rise to both Level 1 non-compliance (2.1.3) and Level 3 non-compliance (2.3.3). This is confusing and should be resolved. 2. Failure of the Training program to address two or more required items gives rise to non-compliance at Level 2 (2.2.3) and Level 3 (2.3.4). This is confusing and should be resolved. 3. If documentation of the personnel risk assessment program reveals that the program fails to require risk assessment updates every 5 years, a Responsible Entity could legitimately claim non-compliance at Level 1 (2.1.3) whereas 2.3.7 characterizes this as Level 3 non-compliance. This is confusing and should be resolved.	Levels of noncompliance have been rewritten.
004-C2,4	Eliminate 2.3.7 since it is covered by 2.1.3.	Levels of noncompliance have been rewritten.

CIP-004 Drafting Team Responses to Comments

Name	E. Nick Henery	
Entity	SMUD	
Ready to Ballot:	Yes	
General Comments	The Drafting Team will need to go through the Standard and assign responsibility to each function from the functional model like the Version 0 STD. For this Standard to enforceable the generic use of Responsible Entity is the same as the generic use of Control Area. Even if the Standard lists the different functions it leaves open the possibility of misinterpretation as to which function is truly responsible.	The Responsible Entities are clearly enumerated in the standard Section A, item 4.
004-R1		
004-R2		
004-R3		
004-R4		
004-M1		
004-M2		
004-M3		
004-M4		
004-C1,1		
004-C1,2		
004-C1,3		
004-C1,4		
004-C2,1		
004-C2,2		
004-C2,3		
004-C2,4		

CIP-004 Drafting Team Responses to Comments

Name	Jack Hobbick	
Entity	Consumers Energy	
Ready to Ballot:	No	
General Comments	Consumers Energy has also submitted comments via the ECAR CIPP.	Please see response to Larry Conrad, ECAR CIPP.
004-R1		
004-R2		
004-R3		
004-R4		
004-M1		
004-M2		
004-M3		
004-M4		
004-C1,1		
004-C1,2		
004-C1,3		
004-C1,4		
004-C2,1		
004-C2,2		
004-C2,3		
004-C2,4		

CIP-004 Drafting Team Responses to Comments

Name	Richard Kafka	
Entity	Pepco Holdings, Inc.	
Ready to Ballot:	No	
General Comments	There is no reference to exceptions in this Standard, though it is to be expected that the need for such exceptions will occur for recovery/emergency waivers (e.g. natural disasters such as hurricanes, weather, flooding) and law enforcement, fire, & EPS personnel. - There is a need for NERC to develop waivers or include verbage to mitigate compliance and audit issue every time there is an emergency.	CIP-003 R1.1 addresses emergency situations. Responsible Entities may write exceptions to their cyber security policies, as shown in the Additional Compliance section of each standard.
004-R1	R2.1. Is training required prior to access? Within 90 days of receiving access?	The requirement calls for training within 90 calendar days of being granted access.
004-R2	R2.2.4 is reporting of incidents included?	Reporting is covered in training because reporting is a requirement of a Responsible Entity's Cyber Security Program. Please see CIP-008.
004-R3	R3.1 and the opening paragraph of R3.2 appear to be the same. If they are intended to address different issues, then they must be clarified. R3.1 – Also, the phrase "authorized access" could include escorted physical access in addition to "escorted" or monitored electronic access. If not, this should be clarified. R3.2.3 – The final phrase starting with the word "including" is unclear. It should be clarified that vendors and at least some contractors will conduct their own Personnel Risk Assessments, but will do so pursuant to standards set by the appropriate Responsible Entity. "Conduct" versus "ensures has been conducted".	R3.1 and R3.2 have been combined. R3 has been clarified to address this issue. R3.3 has been clarified to address this issue.
004-R4	R4.1 – It is unclear how this will be applied to contractors and vendors, how their compliance will be monitored, and especially how it will be audited.	R4.1 has been clarified to address this issue.
004-M1		
004-M2	It is unclear whether training is to be prior to any unescorted or unmonitored access, or if within certain period after such access (such as 90 calendar days). If so, then such restriction must be explicitly stated in the Requirement (such as at R2.1).	Measures have been reworded to refer back to requirements. Please see response at R1 above.
004-M3		
004-M4		
004-C1,1		
004-C1,2		
004-C1,3		
004-C1,4		
004-C2,1	2.1.5 not applied consistently? The phrase "not applied consistently" is unclear. Given that	The levels of noncompliance have been rewritten.

	various methods of awareness training are permitted, it appears to refer to some time period or among different personnel, but neither is stated in the applicable Requirement.	
004-C2,2		
004-C2,3	C2.3.6 appears to be vastly over-reaching the authority of NERC or the Regions. How would this be audited? Any audit would require access to confidential personnel records, and would involve judgements that no audit staff is trained, qualified, or authorized to make. If at all necessary, this should reference a prior, public, legally binding finding or other determination of behavior inconsistent with applicable requirement. Further, if such a determination has been made, this would appear to warrant moving the severity of the noncompliance to Level 4.	The levels of noncompliance have been rewritten.
004-C2,4		

CIP-004 Drafting Team Responses to Comments

Name	Tony Kroskey
Entity	Brazos Electric Power Cooperative
Ready to Ballot:	No

General Comments	Subsection 4.2, remove word "entities".	Done.
004-R1		
004-R2		
004-R3	R3.1, R3.2 and R3.2.3 all seem to be repeating the same requirement, this is confusing.	Requirements 3.1 and 3.2 have been combined.
004-R4	R4. and R4.1, suggest changing the text "all authorized personnel with access" to "all personnel with authorized access".	Revised to clarify.
004-M1	Correct typo "program program".	Done.
004-M2	Suggest changing the text "authorized personnel who have access" to "personnel who have authorized access".	Measures have been reworded to refer back to requirements.
004-M3		
004-M4		
004-C1,1		
004-C1,2		
004-C1,3		
004-C1,4		
004-C2,1		
004-C2,2		
004-C2,3		
004-C2,4		

CIP-004 Drafting Team Responses to Comments

Name	Carol Krysevig	
Entity	Allegheny Energy Supply Co. LLC	
Ready to Ballot:	No	
General Comments	The Purpose shouldn't be that those having access to critical cyber assets have a higher level of risk assessment, training, security awareness than those who don't; it should be that those having access to critical assets have the appropriate level of risk assessment etc.	The purpose has been revised.
	D2.1.1 – Remove 'list' after 'access control rights'. D2.1.1 and Levels of Non-Compliance 2.1.2 relate to Requirement R4 – we are suggesting R4 be relocated to other CIP standards (electronic and physical security). These two Levels of Non-Compliance should be moved along with R4. D2.1.3 – Change 'program' to 'process' throughout sentence. D2.1.5 – Clarification needed on 'not applied consistently'. Somewhat vague in meaning. D2.2.1 and Levels of Non-Compliance 2.2.2 relate to Requirement R4 – we are suggesting R4 be relocated to other CIP standards (electronic and physical security). These two Levels of Non-Compliance should be moved along with R4. D2.2.5 – Change 'program' to 'process' and clarification needed on 'not consistently applied'. Somewhat vague in meaning. D2.3.1 and Levels of Non-Compliance 2.3.2 relate to Requirement R4 – we are suggesting R4 be relocated to other CIP 'standards (electronic and physical security)'. These two Levels of Non-Compliance should be moved along with R4. D2.3.3 – Change 'program' to 'process'. D2.3.6. - This section mentions 'adverse employment actions.' However, we didn't see this mentioned anywhere in the requirements sections. We also question the appropriateness of a NERC sanction for human relations type of violation. Recommend deleting this level of noncompliance. D2.3.7 – Change the word 'Update' to 'Updated'. D2.4.2 – Change 'program' to 'process'. D2.4.3 – Specify exactly what documentation NERC is looking for.	Levels of noncompliance have been rewritten. R4 addresses personnel, the subject of CIP-004.
004-R1	R1 - Awareness – how will the quarterly requirement be applied to 'contractors and service vendors' that may or may not receive this type of training due to their short duration on site?	It is up to the Responsible Entity to determine how to meet the requirements. As an example, the Responsible Entity may choose to rely on procedures incorporated into the Responsible Entity's contract with the vendor.
004-R2	R2.1 should be modified to reflect that training requirements are to be commensurate with the individual's level of access. It should be modified to say, 'This program will ensure that all personnel having access to Critical Cyber Assets, including contractors and vendors, are trained commensurate with their level of access.' R2.2.4. - Why is this in the training section? Do all users, or just pertinent users, need to know how to recover after an incident?	This requirement has been clarified.
004-R3		

CIP-004 Drafting Team Responses to Comments

004-R4	R4. - Recommend moving this Section to CIP-005-1 and CIP-006-1 as they are more applicable to Electronic and Physical Security controls. R4.2 - The revocation of electronic access within 24 hours could be tough to implement. Instead recommend revocation of 'remote electronic access' within 24 hours and allow all electronic access to be revoked within 7 days	R4 addresses personnel, the subject of CIP-004. Disgruntled and terminated staff are significant vulnerabilities, and it is vital to address within a time frame reflecting that vulnerability. 24 hours represents industry consensus.
004-M1	The word 'program' is double entered.	The typo has been fixed.
004-M2		
004-M3		
004-M4	Relates to Requirement R4 – we are suggesting R4 be relocated to other CIP standards (electronic and physical security). This measure should be moved along with R4.	Please see response to R4, above.
004-C1,1		
004-C1,2		
004-C1,3		
004-C1,4		
004-C2,1		
004-C2,2		
004-C2,3		
004-C2,4		

CIP-004 Drafting Team Responses to Comments

Name	John Lim	
Entity	Con Edison	
Ready to Ballot:	No	
General Comments		
004-R1		
004-R2	R2.1 should be reworded to state "All personnel having access to Critical Cyber Assets shall have received cyber security training appropriate to their role."	Please see responses to Ray A'Brial, Central Hudson Gas & Electric Corp.
004-R3	Suggest the Drafting team combine and clarify R3.1 with/to R3.2. Change the old R3.2.2 from five years to ten years to be consistent with Federal security clearance.	
004-R4	R4.1 requires a quarterly review. This is too prescriptive and does not match M4. We recommend an annual review and signed by the person authorizing. Add R4.3 Unauthorized personnel must be escorted by authorized personnel	
004-M1		
004-M2		
004-M3		
004-M4		
004-C1,1		
004-C1,2		
004-C1,3		
004-C1,4		
004-C2,1		
004-C2,2		
004-C2,3		
004-C2,4		

CIP-004 Drafting Team Responses to Comments

Name	Deborah Linke	
Entity	Bureau of Reclamation	
Ready to Ballot:	Yes	
General Comments		
004-R1	Reclamation believes that annual training is adequate. If a more frequent reminder is desired, use opening banners on the system as those reminders.	An awareness program is an effective way to reinforce sound cyber security practices and procedures. Awareness is less rigorous than training and quarterly reinforcement should not be burdensome, especially in light of the benefit.
004-R2	R2.1: Authorized access needs clarification in order to understand who must receive training. It is probably infeasible to require that all vendors receive training in policies, access controls, and procedures. There should be an exception for vendors who are escorted and monitored by trained personnel. Delaying repairs and maintenance while waiting for a vendor background check will hurt reliability. R2.2.4: This requirement appears to result in training everyone, including service vendors, in procedures to recover or re-establish Critical Cyber Assets, which was probably not the intent. Clarification of the language to include only those who are actively involved in the recovery of the system would improve the section.	Authorized access has been clarified to include personnel, including service vendors and contractors, who have authorized cyber or unescorted physical access to Critical Cyber Assets. Escorted personnel do not require training. It is up to the Responsible Entity to determine how to ensure training of service vendors and contractors in accordance with the requirements of this standard. Training in action plans and recovery of Critical Cyber Assets has been clarified.
004-R3	R3.2.2: Updating a criminal check every five years on a long-standing employee for which the company has no grounds of suspicion or cause seems to be excessive. Reclamation feels that a better focus would be to establish a procedure to be used to update personnel risk assessments and document that the procedure has been followed.	Changed to 7 years. Personnel represent a significant vulnerability and periodic reassessment is useful in uncovering potentially serious problems that may not otherwise be discovered or observed. Please see FAQ on grandfathering personnel.
004-R4		
004-M1		
004-M2		
004-M3		
004-M4		
004-C1,1		
004-C1,2		
004-C1,3		
004-C1,4		
004-C2,1		

004-C2,2

004-C2,3

004-C2,4

CIP-004 Drafting Team Responses to Comments

Name	Greg Mason
Entity	Dynegy Generation
Ready to Ballot:	Yes

General Comments

004-R1

004-R2

004-R3

004-R4

004-M1

004-M2

004-M3

004-M4

004-C1,1

004-C1,2

004-C1,3

004-C1,4

004-C2,1

004-C2,2

004-C2,3

004-C2,4

CIP-004 Drafting Team Responses to Comments

Name	Paul McClay
Entity	Tampa Electric
Ready to Ballot:	No

General Comments	Purpose: This standard should not require that personnel having access to critical cyber assets have a higher level of risk assessment, training and security awareness than those not having access. It should require a high level for them, but if a company provides a "high level" of risk assessment, training and security awareness to personnel not having access to critical cyber assets, the company should not have to artificially create a "higher" level to comply.	The purpose has been revised.
004-R1	Access is defined in the FAQ as pertaining to those not escorted or otherwise supervised. Presumably that defines "Personnel subject to this standard." This should be clearly defined in the standard not in the FAQ, since the standard is what entities must be in compliance with. We strongly believe the standard should apply only to those with unescorted/unsupervised access. The requirement "….. to ensure that all personnel subject to the standard receive on-going reinforcement in sound security practices" seems to imply an organization must track when each such personnel takes advantage of quarterly security awareness offerings. If that is the intent, this is overly burdensome and expensive and provides no added value. It is difficult to determine if an individual received a memo or read intranet postings, posters, etc. We suggest this sentence be changed to "The responsible entity shall establish, maintain and document a security awareness program that offers personnel subject to this standard ongoing reinforcement in sound security practices."	The requirement has been clarified. Individual tracking of "awareness" is not required.
004-R2		
004-R3	R3.1 Change to "all personnel having unescorted access to critical cyber assets." It is not reasonable to require background checks or training for someone who may be brought in one time to assist with a repair or in a tour. R3.2.3 The FAQ indicates that the responsible entity must only ensure (via audit) that background screening is performed for third parties, in which case the responsible entity would not have those records. Many of our vendors have already indicated they will perform background checks, but will not provide records about their employees to us. However, the Requirement R3.2.3 indicates the Responsible Entity will document the results. The requirements should specifically address third parties, not leave this to the FAQ's. Suggest changing R3.2.3 to address only employees and add R3.2.4 The Responsible Entity shall perform background checks or shall contractually obligate vendors to perform the background checks on contract and service-vendor personnel with access to Critical Cyber Assets. If an Audit requirement is included, then guidance on what the audit must include should be provided, i.e. Is a statistical sampling enough? What constitutes the documentation of an audit, etc.	Revised for clarity. Access to the results of the personnel risk assessment are not needed for documentation by the Responsible Entity. The Responsible Entity must ensure that personnel risk assessments for service vendors and contractors are conducted pursuant to the requirements of the standard.

004-R4	R4.2 We suggest rewording this requirement to state "within 24 hours or one business day" to account for situations where "with cause" terminations occur immediately before a weekend or holiday, or other situations where immediate communication to all individuals who must remove access cannot reasonably be accomplished in 24 hours.	Disgruntled and terminated staff are significant vulnerabilities, and vital to address within a time frame reflecting that vulnerability. 24 hours reflects industry consensus.
004-M1		
004-M2		
004-M3	This measure is not very specific. What is required to be kept to document the process and that it has been applied? Is a database of the date of the last risk assessment and results (pass, fail?) sufficient to show it was applied. Ca the detailed report be discarded using existing corporate retention policies?	Please see the revised Requirement. The form of documentation will vary by Responsible Entity as determined using reasonable business judgment; records must be retained at least one year (see also D1.3).
004-M4		
004-C1,1		
004-C1,2		
004-C1,3	D1.3.1 Retention requirements seem excessive. We would suggest changing to "… shall keep personnel risk assessment documents in accordance with the company's policy for retaining such employee records." Anything else will require a huge burden as companies would then need to keep multiple files of the same record type with different retention schedules – some for personnel who once (potentially 20 years ago) had access to a critical cyber asset and those personnel who never had access. This seems very burdensome and absolutely useless. What is the rationale for keeping 3 years past end of employment? One year past "having approved access to critical cyber assets" would seem more than enough. Once updated, can previous personnel risk assessment records be destroyed?	Data retention for personnel risk assessments has been revised.
004-C1,4		
004-C2,1	The two comments below apply to all compliance levels not only 2.1: It would be more consistent if the items under levels of non-compliance were listed in the same order as the requirements or measures, as they are in the other standards. The threshold of non-compliance levels should address the size of a corporation. The non-compliance of a company that has 5 instances of terminations not being handled within 24 hours for cause when only 10 personnel have access to critical cyber assets versus a company that has 5 instances of terminations not begin handled within 24 hours for cause where 1,000 personnel have access is significantly different. Perhaps some percentage could be used instead of a number. D2.1.2 The requirement is to revoke access within 24 hours (and appropriately so), not to update the access control list within 24 hours. All of these compliance statements should be changed to "…. in which access to critical cyber assets was not revoked within 24 hours or one business day….."	The levels of noncompliance have been ordered as suggested. The levels of noncompliance have been rewritten. Escalation of noncompliance based on number of instances has been removed.
004-C2,2	D2.2.1 "Access control document: is not referenced in this standard. If you are referring to list of personnel with access, copy verbiage of D2.1.1 and change the time period to 6-12	The levels of noncompliance have been rewritten.

	months. D2.2.2 The requirement is to revoke access within 24 hours (and appropriately so), not to update the access control list within 24 hours. All of these compliance statements should be changed to "…. in which access to critical cyber assets was not revoked within 24 hours or one business day….."	
004-C2,3	D2.3.2 The requirement is to revoke access within 24 hours (and appropriately so), not to update the access control list within 24 hours. All of these compliance statements should be changed to "…. in which access to critical cyber assets was not revoked within 24 hours or one business day….." D2.3.6 "Adverse employment actions" and "hiring or retention of employees" are not mentioned in any requirement of this standard. This compliance level should be deleted or reworded to match a requirement. D2.3.7 Delete the first word "update" or change to "Updated"	The levels of noncompliance have been rewritten.
004-C2,4		

CIP-004 Drafting Team Responses to Comments

Name	David McCoy
Entity	Great Plains Energy/Kansas City Power & Light
Ready to Ballot:	No

General Comments		
004-R1		
004-R2	R.2 - Entities should be allowed a reasonable period of time to perform training. after the words "are trained" you should add the words "within three calendar months."	R2 has been clarified to state within 90 calendar days.
	R.2.2.4 - Training of "procedures to recover or re-establish Critical Cyber Assets" should be limited to just those involved in performing this recovery not all critical personnel.	The requirement has been clarified to address this issue.
004-R3	R.3.2 - after the words "shall conduct" you should add the words "or have contractor conduct to the responsible entity's standards." We need to make it clear that contractors can perform background checks.	Revised for clarity.
004-R4	R.4.2. - Replace the phrase "within 24 hours" with "within one business day." This is much more manageable.	Disgruntled and terminated staff are significant vulnerabilities, and vital to address within a time frame reflecting that vulnerability. 24 hours represents industry consesnsus.
004-M1		
004-M2		
004-M3		
004-M4	The words "annual review and update" should be replaced with "quarterly review and update" to make this measure consistent with Requirement R4.1	Measures have been reworded to refer back to the requirements.
004-C1,1		
004-C1,2		
004-C1,3		
004-C1,4		
004-C2,1	Remove the words "but not applied consistently" This appears meaningless and it would be very difficult to prove.	Levels of noncompliance have been rewritten.
004-C2,2		
004-C2,3	C2.3.6 should be eliminated. This standard is not the place to judge whether adverse employment actions are or are not consistent with legal and human resoruce practices for hiring and retention of employees or contrators.	Levels of noncompliance have been rewritten.

004-C2,4

CIP-004 Drafting Team Responses to Comments

Name	William McEvoy	
Entity	Northeast Utilities	
Ready to Ballot:	No	
General Comments	Change the purpose to "This standard requires that personnel having access to Critical Cyber Assets, including contractors and service vendors, have a higher level of personnel risk assessment, training and security awareness than personnel not provided access." Comment - access could be electronic, physical or both. This Standard's compliance is too prescriptive. This Standard has 4 Requirements and 4 Measures. The first three Compliance Levels have at least 5 clauses.	Please see responses to Ray A'Brial, Central Hudson Gas & Electric Corp.
004-R1		
004-R2	R2.1 should be reworded to state "All personnel having access to Critical Cyber Assets shall have received cyber security training appropriate to their role."	
004-R3	Remove R3.1 since it is covered by R3.2. Suggest that the correct order of these sections is R3 (risk assessment), R2 (training), R4 (access), and R1 (awareness). Change the old R3.2.2 from five years to ten years to be consistent with with Federal security clearance.	
004-R4	R4.1 requires a quarterly review. This is too prescriptive and does not match M4. We recommend an annual review and signed by the person authorizing. Add R4.3 Unauthorized personnel must be escorted by authorized personnel	
004-M1	Reorder to stay consistent with R1 - R4	
004-M2		
004-M3		
004-M4		
004-C1,1		
004-C1,2		
004-C1,3		
004-C1,4		

CIP-004 Drafting Team Responses to Comments

004-C2,1 Update 2.1.1 to remain consistent with R4.1 and M4. Failed to perform the annual review.

Failure to document the personnel risk assessment gives rise to both Level 1 non-compliance (2.1.3) and Level 3 non-compliance (2.3.3). This is confusing and should be resolved.

004-C2,2 Remove 2.2.1 since it is covered by the updated 2.1.1.

Failure of the Training program to address two or more required items gives rise to non-compliance at Level 2 (2.2.3) and Level 3 (2.3.4). This is confusing and should be resolved.

004-C2,3

004-C2,4 Eliminate 2.3.7 since it is covered by 2.1.3.

CIP-004 Drafting Team Responses to Comments

Name	Patrick Miller	
Entity	PacifiCorp	
Ready to Ballot:	No	
General Comments	In the Purpose statement, consider additional language that speaks to the physical or logical (cyber/policy) access. It is unclear if both are implied in the existing statement.	The purpose has been clarified.
004-R1		
004-R2		
004-R3	For R3.2.3, consider adding "product vendors" to the language that already includes contractors and service vendors. It will not be feasible for many organizations to conduct Personnel Risk Assessments for all service/product vendors. It would be more reasonable to contractually require Personnel Risk Assessments are performed by all contingent workforce vendors, professional service vendors, product and service vendors with auditable records that can be requested on an as-needed basis.	Anyone with "unescorted" access must be trained in accordance with the requirements of this standard. Service vendors can reasonably be interpreted to include product vendors. The requirement does not mandate that the Responsible Entities retain the results of personnel risk assessments for vendors and contractors. The Responsible Entity must retain the documentation that the service vendors and contractors have conducted personnel risk assessments in accordance with the requirements of this standard.
004-R4		
004-M1		
004-M2		
004-M3		
004-M4		
004-C1,1		
004-C1,2		
004-C1,3	For 1.3.1, It will not be feasible for many organizations to maintain records of Personnel Risk Assessments for all service/product vendors. It would be more reasonable to contractually require Personnel Risk Assessments are performed by all contingent workforce vendors, professional service vendors, product and service vendors with auditable records that can be requested on an as-needed basis for a period of three years.	See response above.
004-C1,4		
004-C2,1		
004-C2,2		

004-C2,3

004-C2,4

CIP-004 Drafting Team Responses to Comments

Name	Don Miller	
Entity	First Energy Corp	
Ready to Ballot:	Yes	
General Comments		
004-R1		
004-R2		
004-R3	R 3.1 should be the requirement, with R 3.2 being the FAQ for clearification, we feel that they are saying the same thing or redundent.	These requirements have been combined.
004-R4		
004-M1		
004-M2		
004-M3		
004-M4		
004-C1,1		
004-C1,2		
004-C1,3		
004-C1,4		
004-C2,1		
004-C2,2		
004-C2,3		
004-C2,4		

CIP-004 Drafting Team Responses to Comments

Name	Jeff Mitchell
Entity	ECAR
Ready to Ballot:	Yes
General Comments	N/A
004-R1	
004-R2	
004-R3	
004-R4	
004-M1	
004-M2	
004-M3	
004-M4	
004-C1,1	
004-C1,2	
004-C1,3	
004-C1,4	
004-C2,1	
004-C2,2	
004-C2,3	
004-C2,4	

CIP-004 Drafting Team Responses to Comments

Name	Scott Mix	
Entity	KEMA, Inc	
Ready to Ballot:	No	
General Comments		
004-R1		
004-R2	There should be a requirement for security training at initial employment or initial grant of access to Critical Cyber Assets.	The requirement has been clarified to state within 90 calendar days.
004-R3	Recommend that the Personnel Risk Assessment be applied to personnel with unescorted access, rather than the current wording of "having access to" and "granting authorized access to". Often, specialized service vendors will need access to equipment, but will not have undergone the entire assessment process, such as an emergency repair. In this case an escort, possibly including technical personnel and security personnel, should be sufficient.	The requirement has been clarified.
004-R4		
004-M1		
004-M2		
004-M3		
004-M4		
004-C1,1		
004-C1,2		
004-C1,3		
004-C1,4		
004-C2,1		
004-C2,2		
004-C2,3		
004-C2,4		

CIP-004 Drafting Team Responses to Comments

Name	Darrick Moe	
Entity	WAPA	
Ready to Ballot:	No	
General Comments	Please clarify the intentions regarding required training (and other CIP-004 requirements), for personnel that have only local physical and/or local electronic access to Critical Cyber Assets.	There is no security difference between local and remote access.
004-R1		
004-R2	R2.2.4 requires that the all personnel that have access to critical cyber assets be trained on the procedures used to recover those assets following an Incident. This requirement is too broad, as it apparently includes all people that use these assets in addition to the IT people that would be largely responsible for restoring them. The requirement should be that all individuals that have a role in restoration procedures be training in those roles. It is not only unnecessary to provide this type of training to everyone with access, but could even be detrimental as this training being provided too widely could result in unnecessary vulnerability, as some of this type of information should not be distributed more widely than needed.	The requirement has been clarified.
004-R3	R3.2.2 appears to require that existing employees go through a background screening, including criminal records check, at least every five years. This should be eliminated as a requirement and left to companies to decide as they deem appropriate. R3.2.2 should be rewritten to indicate: "The Responsible Entity shall document a procedure defining the process to be used to update personnel risk assessments, and shall be able to demonstrate that the procedure is being followed." Doing a criminal check every five years on a long-standing employee for which the company has no grounds of suspicion, for example, should not be required by the standard. Also, entities should be given the option of grandfathering existing employees as they see fit.	Revised to 7 years. Personnel represent a significant vulnerability and periodic reassessment is useful in uncovering potentially serious problems that may otherwise be undiscovered or unobserved.
004-R4		
004-M1		
004-M2		
004-M3		
004-M4		
004-C1,1		
004-C1,2		
004-C1,3		
004-C1,4		

CIP-004 Drafting Team Responses to Comments

004-C2,1	For Level 1 Non Compliance, 2.1.2, add the words "was not revoked" after "One instance of personnel termination (employee, contractor or service provider) in which access", to better match corresponding R4.2. Also, update Level 2, NC 2.2.2 and Level 3, NC 2.3.2 with the corresponding change.	Levels of noncompliance have been rewritten.
004-C2,2		
004-C2,3	Level 3 Non Compliance 2.3.6 should be eliminated – it is simply a requirement to comply with existing corporate policy.	Levels of noncompliance have been rewritten.
004-C2,4		

CIP-004 Drafting Team Responses to Comments

Name	Selby Mohr
Entity	Sacramento Municipal Utility District
Ready to Ballot:	Yes

General Comments

004-R1

004-R2

004-R3

004-R4

004-M1

004-M2

004-M3

004-M4

004-C1,1

004-C1,2

004-C1,3

004-C1,4

004-C2,1

004-C2,2

004-C2,3

004-C2,4

CIP-004 Drafting Team Responses to Comments

Name	Kurt Muehlbauer	
Entity	Exelon	
Ready to Ballot:	No	
General Comments	The documentation and processes around the responsible entity s tasks are too prescriptive. The industry needs to be extremely careful to avoid the creation of purely documentation-based non-compliances. With increasing legal requirements for compliance, and the associated penalties for noncompliance, noncompliance should be reserved for real security issues. It is simply too easy to make a mistake in documentation in light of the constantly evolving cyber environment. Each entity should develop its own processes in support of the requirements, and these processes should be required to contain provisions for periodic review and approval applicable to each requirement. The processes should also be required to produce reasonable documentation to demonstrate compliance. However, it is not necessary to specify the details of the documentation or review periods. The above approach can be met by removing references to documentation from the requirements section. Then, in the measures section require each entity to reasonably document programs and processes that support the security requirements and to produce reasonable documentation required to demonstrate compliance to the security requirements. Please refer to our overall comments on defining reasonable. If the above approach is taken, it will be possible to delete many of the sub-bullet points under each requirement (because the details will be specified by each entity in their program or process, as applicable). This will also ensure that documentation and excessive low-value administrative tasks are removed from the requirements.	The Drafting Team has reviewed the standards and removed prescription where possible. The prescriptiveness that remains is necessary to provide the clarity requested by a majority of commenters. The documentation required by these standards allow Responsible Entities to demonstrate that the policies, processes, and procedures that they have implemented consistently comply with the requirements of these standards.
004-R1		
004-R2	R2 – Training should be required for everyone upon obtaining access to CCA.	It may not be possible to implement training before access is granted, so some flexibility is permitted.
	Remove annually . The frequency of reviewing the training program should be at the discretion of each entity, based the entity s policy.	Some minimal level of uniformity among all Responsible Entities is necessary.
	Delete 2.2.1 – 2.2.4. The content of the training should be determined by the entity.	Some minimal level of uniformity among all Responsible Entities is necessary.
	R2.3 – The training program should include the necessary verification. Per above, eliminate reference to frequency – it will be prescribed in the program. Also, remove reference to attendance records. This would not apply to web based training.	Some minimal level of uniformity among all Responsible Entities is necessary. The Responsible Entity is expected to use reasonable business judgment to determine the record methodology.

004-R3	3.2.2 – Instead of requiring checks every 5 years, require periodic checks based on cause only.	The period has been changed to 7 years. Personnel represent a significant vulnerability and periodic reassessment is useful in uncovering potentially serious problems that may otherwise be undiscovered or unobserved.
004-R4	R4 – Is within the security perimeter(s) needed?	R4 has been revised for clarity.
	4.1 – Language needs to be clarified about what we are removing access from. Rather than focusing on removing someone from the list , we should focus on removing his or her actual access. The list is incidental, and should be updated in a reasonable time frame.	R4.2 addresses access revocation.
	4.2 – Need to make C2.2.2 consistent with R4. In C2.2.2, the requirement is to remove the person from the list within 24hrs. But R4.2 talks about actual revocation of rights within 24 hrs. This should be changed in C2.2.2 to measure compliance by actual revocation of rights, not when the list is updated.	The Levels of Noncompliance have been rewritten.
004-M1	Refer to general, overall comments submitted on CIP-002 through CIP-009 regarding revision of the measures and compliance specification.	Please see response to General Comments.
004-M2	Refer to general, overall comments submitted on CIP-002 through CIP-009 regarding revision of the measures and compliance specification.	
004-M3		
004-M4	Refer to general, overall comments submitted on CIP-002 through CIP-009 regarding revision of the measures and compliance specification.	
004-C1,1	Refer to general, overall comments submitted on CIP-002 through CIP-009 regarding revision of the measures and compliance specification.	
004-C1,2	Refer to general, overall comments submitted on CIP-002 through CIP-009 regarding revision of the measures and compliance specification.	
004-C1,3	Refer to general, overall comments submitted on CIP-002 through CIP-009 regarding revision of the measures and compliance specification.	
004-C1,4	Refer to general, overall comments submitted on CIP-002 through CIP-009 regarding revision of the measures and compliance specification.	
004-C2,1	Refer to general, overall comments submitted on CIP-002 through CIP-009 regarding revision of the measures and compliance specification.	
004-C2,2	Refer to general, overall comments submitted on CIP-002 through CIP-009 regarding revision of the measures and compliance specification.	
004-C2,3	Refer to general, overall comments submitted on CIP-002 through CIP-009 regarding revision of the measures and compliance specification.	
004-C2,4	Refer to general, overall comments submitted on CIP-002 through CIP-009 regarding revision of the measures and compliance specification.	

CIP-004 Drafting Team Responses to Comments

Name	Jeffrey Mueller	
Entity	PSEG Companies	
Ready to Ballot:	No	
General Comments	The PSEG Companies have reviewed and share the concerns expressed in the Comments of PJM and EEI. Accordingly, the PSEG Companies support the comments of PJM and EEI, and request that the concerns expressed in those comments be properly addressed in the next version of the draft standard.	Please see responses to Laurence W. Brown, Edison Electric Institute.
004-R1		
004-R2		
004-R3		
004-R4		
004-M1		
004-M2		
004-M3		
004-M4		
004-C1,1		
004-C1,2		
004-C1,3		
004-C1,4		
004-C2,1		
004-C2,2		
004-C2,3		
004-C2,4		

CIP-004 Drafting Team Responses to Comments

Name	Mitchell Needham	
Entity	Tennessee Valley Authority	
Ready to Ballot:	No	
General Comments	There are a number of concerns as to whether an entity would be able to meet all of the requirements with respect to contractors or other temporary personnel.	
004-R1		
004-R2	TVA suggests the addition of a Requirement 2.4 - The Responsible Entity shall provide for and document recurrent training on an annual basis.	Documentation is already required by R2.3.
004-R3	This requirement might have a very adverse financial impact on some entities.	The period has been changed to 7 years. Personnel represent a significant vulnerability and periodic reassessment is useful in uncovering potentially serious problems that may otherwise be undiscovered or unobserved.
004-R4	R4.2 - revocation within 24 hours might prove difficult in instances where a person does not have a physical 'key' but uses some other type of entry token (i.e. password on keypad, biometrics).	Disgruntled and terminated staff are significant vulnerabilities, and vital to address within a time frame reflecting that vulnerability.
004-M1		
004-M2		
004-M3		
004-M4		
004-C1,1		
004-C1,2		
004-C1,3		
004-C1,4		
004-C2,1		
004-C2,2		
004-C2,3		
004-C2,4		

CIP-004 Drafting Team Responses to Comments

Name	Dave Norton	
Entity	Entergy Transmission	
Ready to Ballot:	No	
General Comments		
004-R1	R.1: As written, the language says the Responsible Entities must employ each communication method listed as bullets. Is this intended? Are these examples and alternatives, or requirements?	The phrase “such as” indicates the bullets are examples.
004-R2	R2: Suggestion: Change "shall review and update the program annually" to "review annually and update as necessary"	Modified as suggested.
004-R3	R3.2: Jurisdictions are well delineated, but which laws, types of law, or even 'fields' of law apply? Labor? Health? Tax? Etc.	Any and all applicable laws are intended.
004-R4		
004-M1		
004-M2		
004-M3		
004-M4		
004-C1,1		
004-C1,2		
004-C1,3		
004-C1,4		
004-C2,1		
004-C2,2		
004-C2,3		
004-C2,4		

CIP-004 Drafting Team Responses to Comments

Name	Doug Orlofske
Entity	Wisconsin Public Power Inc
Ready to Ballot:	Yes

General Comments

004-R1

004-R2

004-R3

004-R4

004-M1

004-M2

004-M3

004-M4

004-C1,1

004-C1,2

004-C1,3

004-C1,4

004-C2,1

004-C2,2

004-C2,3

004-C2,4

CIP-004 Drafting Team Responses to Comments

Name	Kevin Perry	
Entity	Southwest Power Pool	
Ready to Ballot:	No	
General Comments	The purpose statement references "authorized access". Does this refer to any sort of access or only unescorted access? This is assumed to refer to both physical access as well as electronic access.	The purpose has been clarified.
004-R1		
004-R2	See the general comment above. What constitutes "authorized access?" If a person, including vendors and contractors, is physically escorted or is granted electronic access under controlled, observed conditions, is prior security training required?	Authorized access has been clarified as authorized cyber or unescorted physical access. (Please see FAQs.) Training is not required for escorted or supervised personnel.
	R2.2.2 should not be a mandatory aspect of the security training, especially where vendors and contractors are involved. Training on the access policies, and not the specific controls, is appropriate.	R2.2 has been clarified to address this training issue.
	R2.2.4 is not appropriate for all personnel, especially vendors and contractors, that might have access to a CCA. This training is appropriate for the specific staff charged with managing the system in question and the Incident Response Team.	R2.2 has been clarified to address this training issue.
	The implication of requirement R2.3 is that training of vendors and contractors must be done in person, in a formal training setting. To that end, this requirement needs to be clarified as to what forms of training and record keeping are acceptable.	Training "in person" is not specified. How training is delivered is up to the Responsible Entity's reasonable business judgment.
004-R3	Once again, what constitutes "authorized access?" Does this include general users of the applicable system or just those that have management or update privileges?	See response above.
	R3.2.3: Typically, vendors and contractors are willing to disclose their background check criteria and whether or not a particular employee has been subjected to such a check. They are very reluctant, if not prohibited by law or bargaining agreement, from disclosing the specific results of the background check to the client. The presumption to this point has been if the contractor or vendor has not found anything that would preclude the individual from continued employment or assignment to a project per their own criteria, the specifics of which should be reviewed by the client entity, then the requirements of the background check have been satisfied with the certification by the vendor/contractor company that such checks have been completed. This requirement implies that the client company can no longer trust the vendor/contractor company to conduct a background check, subjecting the contractor or vendor employee to numerous, redundant background checks at a cost to each entity. Please clarify.	Access to the results of the personnel risk assessment are not needed for documentation by the Responsible Entity. The Responsible Entity must ensure that personnel risk assessments for service vendors and contractors are conducted pursuant to the requirements of the standard.
004-R4	R4.1: How does an entity ensure compliance with the 7-day updating requirement when it comes to vendors and contractors. The entity can require its vendor/contractor company to	Responsible Entities should have processes in place with vendors to notify the Responsible Entity of personnel changes, if those

	confirm continued need for access as part of the quarterly review, but the entity must rely upon the vendor/contractor company to provide prompt notification of any changes in their personnel or project assignments. This requirement, as written, may well be unenforceable.	personnel have access to Critical Cyber Assets.
	R4.2: The seven-day window is too long for any change involving a suspension or revocation of authorized access. Any adverse personnel actions should be subject to the same 24-hour provision as a terminated employee.	Upon termination in R4.2 reflects industry consensus. This is a minimum requirement and Responsible Entities may go beyond the minimum as they deem appropriate.
004-M1		
004-M2		
004-M3		
004-M4		
004-C1,1		
004-C1,2		
004-C1,3	C1.3.1: The retention requirement of three years is unnecessary. A one year retention period is reasonable. A five-year reverification of the background check should be sufficient documentation. There is no need to maintain past background check documentation.	
004-C1,4	Approval of exceptions should not be delegated.	Exceptions cannot be taken to NERC standards. It is up to Responsible Entities to define policies, exception handling, and delegation authority.
004-C2,1	C2.1.2 references termination "for cause". Subject to the comments in R4.1, this compliance requirement should include all adverse personnel actions in the 24-hour action window.	Levels of noncompliance have been rewritten. Please see response at R4.
004-C2,2	C2.2.2 references termination "for cause". Subject to the comments in R4.1, this compliance requirement should include all adverse personnel actions in the 24-hour action window.	Levels of noncompliance have been rewritten.
004-C2,3	C2.3.2 references termination "for cause". Subject to the comments in R4.1, this compliance requirement should include all adverse personnel actions in the 24-hour action window. C2.3.6 has no corresponding requirement statement.	Levels of noncompliance have been rewritten.
004-C2,4		

CIP-004 Drafting Team Responses to Comments

Name	Tom Pruitt
Entity	Duke Power Company
Ready to Ballot:	No

General Comments	A.3 -- Define "access." Suggest clarifying that this includes physical and cyber access.	The purpose has been clarified.
	A.4.1 -- Given the critical role of the PSE, why are these standards not applicable to that entity?	The standards reflect the Standard Authorization Request (SAR), which excluded PSEs. The drafting team must respect the scope of the SAR and not extend it during standards development. The SAR reflects industry consensus on the scope of the standard to be developed.
	A.4.2.2 -- Appears to be inconsistent with definition of "Cyber Asset".	The SAR specifically excluded communication links.
	A.5 -- This should reference the proposed Implementation Plan. Alternatively, the compliance implementation plan should be referenced in the compliance sections for all of CIP002 thru CIP 009.	Although reviewed and commented upon by the industry, the Implementation Plan is not part of the standard and cannot be referenced therein.
004-R1	R1 -- This requirement will be difficult and costly to implement and manage.	An awareness program is an effective way to reinforce sound cyber security practices and procedures. Awareness is less rigorous than training and quarterly reinforcement should not be burdensome, especially in light of the benefit. Responsible Entities are expected to interpret and implement this requirement using reasonable business judgment.
004-R2	R2.3 -- Clarify whether the Responsible Entity can task the contracting vendor to perform, and maintain records of, the training referenced here. Require Responsible Entity to define and audit contractor and vendor service providers personnel risk programs so that reasonable assurance exists that all contractors and vendors are adequately screened.	The existing language in R2 and R3.3 does not preclude this arrangement. The Responsible Entity must ensure the requirements of this standard are met.
004-R3	R3.1 -- Clarify whether the Responsible Entity can task the contracting vendor to perform, and maintain records of, the screening referenced here. This requirement prohibits the use of specialized internal resources during emergency conditions. This will have a serious impact on the ability to get an asset back on line in the event of a failure. Some balancing of the reliability needs with the security needs is needed here.	That is the intent as worded in R3.3. Emergency situations are addressed in CIP-003, R1.1.
	R3.2.2 -- For the initial certification, for non grandfathered employees (those not employed longer than 5 years), when do the initial, or updated, screenings have to be completed?	The requirement for updates of personnel risk assessments has been clarified. Please see FAQ.
	R3.2.3 -- Clarify whether the Responsible Entity can task the contracting vendor to perform, and maintain records of, the screening referenced here.	That is the intent as worded in R3.3. The Responsible Entity must ensure that personnel risk assessments for service vendors and contractors are conducted pursuant to the requirements of the standard.

CIP-004 Drafting Team Responses to Comments

004-R4	R4.2 -- Clarify as to whether this is 24 clock or business hours.	The requirement calls for 24 clock hours.
004-M1		
004-M2		
004-M3		
004-M4	M4 -- The annual review period is not consistent with R4.1.	The measures have been reworded to refer back to the requirements.
004-C1,1		
004-C1,2		
004-C1,3		
004-C1,4		
004-C2,1		
004-C2,2		
004-C2,3		
004-C2,4		

CIP-004 Drafting Team Responses to Comments

Name	Duane Radzwion
Entity	Consumers Energy
Ready to Ballot:	Yes

General Comments

004-R1

004-R2

004-R3

004-R4

004-M1

004-M2

004-M3

004-M4

004-C1,1

004-C1,2

004-C1,3

004-C1,4

004-C2,1

004-C2,2

004-C2,3

004-C2,4

CIP-004 Drafting Team Responses to Comments

Name	Howard Rulf	
Entity	We Energies	
Ready to Ballot:	No	
General Comments	General question: What about emergency waivers? Storms and other disasters may require personnel from other utilities to access critical assets for restoration. This access may be unescorted. This section should note this special case.	Standard CIP-003 R1.1 addresses emergency situations.
004-R1	Awareness training. Change reinforcement period from quarterly to bi-annual.	An awareness program is an effective way to reinforce sound cyber security practices and procedures. Awareness is less rigorous than training and quarterly reinforcement should not be burdensome, especially in light of the benefit.
004-R2	R2.1: Training requirements for new access should be completed within 30-90 days of obtaining such access. Clarify that the requirement for training is for those who have authorized access to critical cyber assets, not those who just have access to the physical perimeter. R2.3.6: Adverse employment actions. Omit this section. This goes beyond the scope of NERC and this standard.	The requirement has been clarified. The requirement has been removed.
004-R3	Delete "Responsible Entities may conduct …of the position."	This language is intended to allow Responsible Entities flexibility.
004-R4		
004-M1		
004-M2		
004-M3		
004-M4		
004-C1,1		
004-C1,2		
004-C1,3		
004-C1,4		
004-C2,1		
004-C2,2		
004-C2,3		
004-C2,4		

CIP-004 Drafting Team Responses to Comments

Name	Randy Schimka	
Entity	San Diego Gas and Electric Co.	
Ready to Ballot:	No	
General Comments		
004-R1		
004-R2	We're all for training contractors and vendors, as required in R2.1. We are currently doing that. However, as outlined in R2.2.4, we don't believe it is necessary to train contractors and vendors and action plans and procedures to recover or re-establish critical cyber assets. R2.2.1 and 2.2.2 are appropriate for contractors and vendors. As a reference point, our contractors and vendors are carpet cleaners, janitorial employees, HVAC repair folks, etc.	R2 has been clarified to address this issue.
004-R3	The phrase "conduct a documented personnel risk assessment" is confusing in R3.2. It sounds like a background check. If that's the case, please see extensive comments in Draft 2 about background checks or assessments with respect to contractors and service vendors (as discussed in R3.2.3).	Access to the results of the personnel risk assessment are not needed for documentation by the Responsible Entity. Responsible Entities must ensure that personnel risk assessments for contractors and service vendors are conducted pursuant to the requirements in this standard.
004-R4		
004-M1		
004-M2		
004-M3		
004-M4		
004-C1,1		
004-C1,2		
004-C1,3		
004-C1,4		
004-C2,1		
004-C2,2		
004-C2,3		
004-C2,4		

CIP-004 Drafting Team Responses to Comments

Name	Lyman Shaffer
Entity	PG&E
Ready to Ballot:	Yes

General Comments

004-R1

004-R2

004-R3

004-R4

004-M1

004-M2

004-M3

004-M4

004-C1,1

004-C1,2

004-C1,3

004-C1,4

004-C2,1

004-C2,2

004-C2,3

004-C2,4

CIP-004 Drafting Team Responses to Comments

Name	Neil Shockey	
Entity	Southern California Edison	
Ready to Ballot:	Yes	
General Comments		
004-R1	Change R1 to read: "Awareness - The Responsible Entity … to ensure personnel subject to this standard receive on-going …"	Personnel has been clarified.
004-R2		
004-R3		
004-R4		
004-M1		
004-M2		
004-M3		
004-M4		
004-C1,1		
004-C1,2		
004-C1,3		
004-C1,4		
004-C2,1		
004-C2,2		
004-C2,3		
004-C2,4		

CIP-004 Drafting Team Responses to Comments

Name	William Smith	
Entity	Allegheny Power	
Ready to Ballot:	No	
General Comments	The Purpose shouldn’t be that those having access to critical cyber assets have a higher level of risk assessment, training, security awareness have a higher level than those who don’t; it should be that those having access to critical assets have the appropriate level of risk assessment etc…	Purpose has been clarified.
004-R1		
004-R2	R2.1 should be modified to reflect training requirements are to be commensurate with the individual’s level of access. It should be modified to say, "This program will ensure that all personnel having access to Critical Cyber Assets, including contractors and vendors, are trained commensurate with their level of access."	The requirement has been modified.
004-R3		
004-R4		
004-M1	The word "program" is double entered.	Corrected.
004-M2		
004-M3		
004-M4		
004-C1,1		
004-C1,2		
004-C1,3		
004-C1,4		
004-C2,1		
004-C2,2		
004-C2,3		
004-C2,4		

CIP-004 Drafting Team Responses to Comments

Name	Paul Sorenson	
Entity	Open Access Technology International	
Ready to Ballot:	Yes	
General Comments	R3.1 and R3.2 (Personnel Risk Assessment) seem to be identical; is there a reason they are stated separately?	These requirements have been combined.
004-R1		
004-R2		
004-R3		
004-R4		
004-M1		
004-M2		
004-M3		
004-M4		
004-C1,1		
004-C1,2		
004-C1,3		
004-C1,4		
004-C2,1		
004-C2,2		
004-C2,3		
004-C2,4		

CIP-004 Drafting Team Responses to Comments

Name	Robert Strauss	
Entity	NYSEG	
Ready to Ballot:	No	
General Comments	Change the purpose to "This standard requires that personnel having access to Critical Cyber Assets, including contractors and service vendors, have a higher level of personnel risk assessment, training and security awareness than personnel not provided access." Comment - access could be electronic, physical or both. This Standard's compliance is too prescriptive. This Standard has 4 Requirements and 4 Measures. The first three Compliance Levels have at least 5 clauses.	Please see responses to Ray A'Brial, Central Hudson Gas & Electric Corp.
004-R1		
004-R2	R2.1 should be reworded to state "All personnel having access to Critical Cyber Assets shall have received cyber security training appropriate to their role."	
004-R3	NPCC Participating Members suggest the Drafting team combine and clarify R3.1 with/to R3.2. Suggest that the correct order of these sections is R3 (risk assessment), R2 (training), R4 (access), and R1 (awareness). Change the old R3.2.2 from five years to ten years to be consistent with with Federal security clearance.	
004-R4	R4.1 requires a quarterly review. This is too prescriptive and does not match M4. We recommend an annual review and signed by the person authorizing. Add R4.3 Unauthorized personnel must be escorted by authorized personnel	
004-M1	Reorder to stay consistent with R1 - R4	
004-M2		
004-M3		
004-M4		
004-C1,1		
004-C1,2		
004-C1,3		
004-C1,4		

CIP-004 Drafting Team Responses to Comments

004-C2,1 Update 2.1.1 to remain consistent with R4.1 and M4. Change the words from "for more than three months but less than six months;

to

annually.

Failure to document the personnel risk assessment gives rise to both Level 1 non-compliance (2.1.3) and Level 3 non-compliance (2.3.3). This is confusing and should be resolved.

004-C2,2 Remove 2.2.1 since it is covered by the updated 2.1.1.

Failure of the Training program to address two or more required items gives rise to non-compliance at Level 2 (2.2.3) and Level 3 (2.3.4). This is confusing and should be resolved.

004-C2,3

004-C2,4 Eliminate 2.3.7 since it is covered by 2.1.3.

CIP-004 Drafting Team Responses to Comments

Name	Karl Tammar	
Entity	IRC	
Ready to Ballot:	No	
General Comments		
004-R1		
004-R2	1. R2.1 should be reworded to state "All personnel having access to Critical Cyber Assets shall have received cyber security training or shall be escorted by personnel who have had such training."	Authorized access has been clarified.
004-R3	2. The text of R3.1 and R3.2 overlap somewhat. The two requirements should be combined into one statement and the remaining sections re-numbered.	These requirements have been combined.
	3. R3.1 and R3.2 should be reworded to be applicable only to personnel, vendors and contractors who are granted unescorted access to Critical Cyber Assets.	Revised to clarify.
004-R4	4. R4 requires quarterly review of access lists, where as M4 suggests that annual review is sufficient. The discrepancy should be resolved.	Measures have been reworded to refer back to requirements.
004-M1		
004-M2		
004-M3		
004-M4		
004-C1,1		
004-C1,2		
004-C1,3		
004-C1,4		
004-C2,1	5. Failure to document the personnel risk assessment gives rise to both Level 1 non-compliance (2.1.3) and Level 3 non-compliance (2.3.3). This is confusing and should be resolved.	Levels of noncompliance have been rewritten.
004-C2,2	6. Failure of the Training program to address two or more required items gives rise to non-compliance at Level 2 (2.2.3) and Level 3 (2.3.4). This is confusing and should be resolved.	Levels of noncompliance have been rewritten.
004-C2,3	7. If documentation of the personnel risk assessment program reveals that the program fails to require risk assessment updates every 5 years, a Responsible Entity could legitimately claim non-compliance at Level 1 (2.1.3) whereas 2.3.7 characterizes this as Level 3 non-compliance. This is confusing and should be resolved.	Levels of noncompliance have been rewritten.

004-C2,4

CIP-004 Drafting Team Responses to Comments

Name	Todd Thompson	
Entity	PJM Interconnection	
Ready to Ballot:	No	
General Comments		
004-R1		
004-R2	R2.1 should be reworded to state "All personnel having access to Critical Cyber Assets shall have received cyber security training or shall be escorted by personnel who have had such training."	Please see responses to Karl Tammar, IRC.
004-R3	The text of R3.1 and R3.2 overlap somewhat. The two requirements should be combined into one statement and the remaining sections re-numbered. R3.1 and R3.2 should be reworded to be applicable only to personnel, vendors and contractors who are granted unescorted access to Critical Cyber Assets.	
004-R4	R4 requires quarterly review of access lists, where as M4 suggests that annual review is sufficient. The discrepancy should be resolved.	
004-M1		
004-M2		
004-M3		
004-M4		
004-C1,1		
004-C1,2		
004-C1,3		
004-C1,4		
004-C2,1	Failure to document the personnel risk assessment gives rise to both Level 1 non-compliance (2.1.3) and Level 3 non-compliance (2.3.3). This is confusing and should be resolved. If documentation of the personnel risk assessment program reveals that the program fails to require risk assessment updates every 5 years, a Responsible Entity could legitimately claim non-compliance at Level 1 (2.1.3) whereas 2.3.7 characterizes this as Level 3 non-compliance. This is confusing and should be resolved.	
004-C2,2	Failure of the Training program to address two or more required items gives rise to non-	

compliance at Level 2 (2.2.3) and Level 3 (2.3.4). This is confusing and should be resolved.

004-C2,3

004-C2,4

CIP-004 Drafting Team Responses to Comments

Name	Steven Townsend	
Entity	Consumers Energy Co.	
Ready to Ballot:	No	
General Comments	Consumers Energy has also submitted comments via the ECAR CIPP.	Please see responses to Larry Conrad, ECAR CIPP.
004-R1		
004-R2		
004-R3		
004-R4		
004-M1		
004-M2		
004-M3		
004-M4		
004-C1,1		
004-C1,2		
004-C1,3		
004-C1,4		
004-C2,1		
004-C2,2		
004-C2,3		
004-C2,4		

CIP-004 Drafting Team Responses to Comments

Name	Martin Trence	
Entity	Xcel Energy - Northen States Power (NSP)	
Ready to Ballot:	No	
General Comments		
004-R1		
004-R2		
004-R3	R3.2.2 - Delete the words "at least every five years or" from the requirement. A time based personnel risk assessment does not serve the purpose intended for, that is to rescreen existing personnel for continued access to Critical Cyber Assets, especially in the absence of industry wide defined criteria to be applied for such an assessment. Significant impacts arise in Human Resource related issues, and subsequent legal challenges are certainly to occur if such a requirement were adopted in its present form. Updated personnel assessments based on cause have a historically accepted basis behind them, and are more than adequate to satify this requirement.	The period has been changed to 7 years. Personnel represent a significant vulnerability and periodic reassessment is useful in uncovering potentially serious problems that may otherwise be undiscovered or unobserved.
004-R4		
004-M1		
004-M2		
004-M3		
004-M4		
004-C1,1		
004-C1,2		
004-C1,3		
004-C1,4		
004-C2,1		
004-C2,2		
004-C2,3	C 2.3.7 - Remove the words "at least every five years or" from this Section, consistent with comments supplied concerning R3.2.2 of this Standard.	Please see response above.
004-C2,4		

CIP-004 Drafting Team Responses to Comments

Name	Rick Vermeers	
Entity	Avistacorp	
Ready to Ballot:	No	
General Comments		
004-R1		
004-R2		
004-R3		
004-R4		
004-M1		
004-M2		
004-M3		
004-M4	I believe that the Q/A related to this item (shown below) should be incorporated in the standard. Otherwise, it appears to me to be unenforceable and may lead to gaming.	This comment does not contain enough specificity to address.
004-C1,1		
004-C1,2		
004-C1,3		
004-C1,4		
004-C2,1		
004-C2,2		
004-C2,3		
004-C2,4		

CIP-004 Drafting Team Responses to Comments

Name	Robert C. Webb	
Entity	Instrumentation, Systems and Automation Society	
Ready to Ballot:	No	
General Comments	1. Who is ISA and Why is ISA commenting on CIP-002 through CIP-009? These comments were developed by members of the Instrumentation, Systems and Automation Society, (ISA), SP99, "Manufacturing and Control Systems Security" committee's leadership team. The overall committee is composed of over 200 members including many users, government representatives, academics, control systems manufactures, and engineers with expertise in automation and control systems. ISA's SP99 is working to develop control systems security standards that provide sufficient guidance to the control systems and IT domain stakeholders to assure that security risks can be appropriately reduced without adversely affecting the intended functionality of those systems. ISA has published over 150 pages of guidance specific to the application of cyber security to control systems, in the form of two technical reports: ISA's ANSI/ISA-TR99.00.01-2004, "Security Technologies for Manufacturing and Control Systems", and ANSI/ISA-TR99.00.02-2004, "Integrating Electronic Security into the Manufacturing and Control Systems Environment." Both highlight the unique aspects of control systems which must be considered when applying security procedures and technology to control systems. ISA's constituency includes both fossil and nuclear power plant automation practitioners, and ISA has active standards committees in both of these areas (SP77, Fossil Power Plant Standards, and SP67, Nuclear Power Plant Standards). 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 have been working with NERC to establish a liaison process that would allow such considerations to be addressed earlier in the process. The development of that liaison process is nearly complete. However, comments are due at this time, and we believe these issues need to be addressed now, before approval of these standards, for the standards to be effective, without damaging the systems they are intended to protect. Thus members of the SP99 committee leadership team, with domain expertise in power generation and associated control systems have put together summary comments in several areas that should be addressed before issue of these standards. 2. Overview and Summary of Essential Changes In general, we found these documents to be excellent examples of how an industry group can (and should) provide coherent and well structured guidance on cybersecurity. We commend NERC's drafting team and review process; it has resulted in a quality set of documents that should be widely used. At the same time, and in fact because of the expected wide application of these documents, we believe that three general areas should be addressed before approval of these documents.	Regarding comment #2a, the exclusionary language concerning generation assets has been removed with the exception of nuclear generation which is excluded by the SAR. Because distribution assets are not considered part of the Bulk Electric System, these resources remain excluded as well. Regarding comment #2b, much of the prescriptive language on how certain security measures should be applied has been removed. For example, the requirement for port scans in CIP 005, R4.2 has been replaced by a requirement to review only ports and services required for operations are enabled. In addition, the Drafting Team has removed most references to "how" security measures should be applied throughout the Standards unless it is required for compliance purposes. Regarding comment #2c, language has been added to reflect the fact that some security solutions that are available today were not available when some legacy systems were designed and put into service. CIP-003, CIP- 004, CIP-005, and CIP-006 contain language addressing exceptions to their policies that may be required to deal with legacy systems and facilities where modern security solutions are not technically possible. In these cases, the Responsible Entities must identify and document the exception and describe the mitigating steps they are taking to secure the assets in lieu of the modern solution. Regarding the comments #3, #4, and #5 related to scope, the Standard reflects the Standard Authorization Request which excluded distribution, nuclear generation, and telecommunication infrastructure. The Drafting Team cannot exceed the scope of the SAR. A SAR reflects the industry consensus on the scope of any particular standard to be developed. Once SAR has been approved for standards drafting, the scope cannot be changed. The NERC Reliability Standards process would require new SARs to address these scope issues.

a) Broader scope - to address a larger % of generation resources and key distribution resources, and avoid excessive reliance on one boundary or layer of defense from cyber attacks. While we recognize the need to prioritize and prevent excessive requirements, we believe the current scope is overly restrictive, and excludes a significant portion of generation, and thereby significant vulnerabilities, in some areas. This is addressed in our specific comments on CIP-002-1, (and also CIP-003-1 through 009-1), which follow.
b) Additional cautions and guidance for control systems - in the form of specific requirements and references to key industry documents, to assure that the measures applied do not result in systems failures and reduced reliability instead of reduced risk. These cautions and guidance are necessary to address the special considerations needed when applying many normal security practices to control systems and control system networks – particularly the bulk of legacy systems in operation today. Many do not have any ability to provide most of the required security features, and can be adversely affected by the application of other requirements. One good example is the requirement to do port scans (CIP 005-1, R4.2). Many legacy control networks are halted by port scans. The standard should include this caution, and suggest the use of alternatives to identify open ports on operational systems which have not been specifically designed and demonstrated to support this kind of testing without production failures. In general, more specific guidance on how to apply these requirements to the many legacy systems in use today should be provided.
c) Mandatory additional protection for inadequate legacy systems – The phrase "where technically feasible" is used in a number of locations throughout the document. In many of these cases, alternatives are required. However, in others, no alternatives are required. Clearly stated requirements to add protection or barriers to cyber attack ("mitigation measures"), where they cannot be configured or incorporated into existing systems, should be added. It is not acceptable, in our view, to identify unacceptable risks, and then leave them because the existing equipment cannot be appropriately hardened. Appropriate countermeasures, to reduce risks to acceptable levels, should be required in all cases.

Addressing these concerns does not mean significant revision to this set of standards, or significant delay, in our opinion. It can be done effectively with minor changes and references in the generic text and in several specific locations. We suggest some of the specifics below. We believe these considerations are important to prevent the standards from being counterproductive or missing significant vulnerabilities.

3. Scope - Distribution assets that could have cyber impacts on transmission assets are excluded. All distribution assets that could have cyber impacts on Bulk Electric system assets should be included, to meet the objectives of the Standards. This comment also applies to the identical sections of the remaining standards (CIP-003 – CIP-009).

4. Scope - Exclusion 3.2.1 should be removed; it excludes some of the larger generators that would otherwise be included under R1.1.4, and the NRC's requirements should be coordinated with, not independent of these requirements. This comment also applies to the identical sections of the remaining standards, (Section 4.2.1 of CIP-003 – CIP-009).

5. Scope - Exclusion 3.2.2 should be removed; even when those communications systems are

	provided by others, the defined entities are still ultimately responsible for their proper operation and security. This comment also applies to the identical sections of the remaining standards, (Section 4.2.2 of CIP-003 – CIP-009).	
004-R1	Additional cautions and guidance for control systems – The awareness program for the critical cyber assets needs to include specific information on the scope and nature of the control systems involved, and the issues associated with the unique features of these systems. Experience has shown that unless this is emphasized, routine activities, such as the use of floppy disks or network connections, taken for granted in most business networks, can and will compromise and cause control system failures. This can be addressed by inserting a requirement into R1: "The program shall include specific discussion of control systems and their unique features and security awareness reinforcement on at least a quarterly basis using mechanisms such as:…"	The awareness program reinforces sound security practices. Responsible Entities may define the appropriate content.
004-R2	Additional cautions and guidance for control systems – In a similar fashion, R2 should be modified to include requirements for training specific to control system as well as other Critical Cyber Assets. While all of us who understand the full scope of these systems do not need this additional emphasis, we consistently find the majority of industry participants who have not been involved do need the emphasis to avoid overlooking the unusual aspects of control systems.	The required content of the training program is a minimum. Responsible Entities may go beyond the minimum as they deem appropriate.
004-R3		
004-R4		
004-M1		
004-M2		
004-M3		
004-M4		
004-C1,1		
004-C1,2		
004-C1,3		
004-C1,4		
004-C2,1		
004-C2,2		
004-C2,3		
004-C2,4		

Name	Laurent Webber	
Entity	Western Area Power Administration	
Ready to Ballot:	No	
General Comments		
004-R1	Quarterly awareness reinforcement is too often, annually would be adequate. Training and awareness can be combined into one annual event, thus this requirement can be removed and combined with the training requirement.	Awareness and training are distinctly different. An awareness program is an effective way to reinforce sound cyber security practices and procedures. Awareness is less rigorous than training and quarterly reinforcement should not be burdensome, especially in light of the benefit.
004-R2	R2.1: Clearly define what "authorized access" means as related to who must receive training. It is too much to ask that all vendors receive training in policies, access controls, and procedures. There should be an exception for vendors who are escorted and monitored by trained personnel. Delaying repairs and maintenance while waiting for a vendor background check will hurt reliability. R2.2.4: This requirement results in training everyone, including service vendors, in procedures to recover or re-establish Critical Cyber Assets. This is way too much. Change the wording to "Those individuals who have a role in recovering or re-establishing access to Critical Cyber Assets after a Cyber Security Incident shall be trained in the procedures and action plans for such recovery."	Authorized access has been clarified as authorized cyber or unescorted physical access. Please see the FAQs. Training is not required for escorted or supervised personnel. The requirement has been clarified.
004-R3	R3.1: The terms "access" and "authorized access" are used as though they have different meanings, but the meanings are not clear. It is too much to ask that all vendors have personnel risk assessments. There should at least be an exception for vendors who are escorted and monitored by trained and cleared personnel. R3.2.1: Privacy Act rules allow any person to withhold their Social Security Number (SSN) from everyone but their employer and the IRS. If a vendor or contractor refuses to give their SSN, how can this requirement be met? It is illegal to require this for vendors and contractors. R3.2.2: Updating a criminal check every five years on a long-standing employee for which the company has no grounds of suspicion should not be required by the standard. Entities should be given the option of grandfathering existing employees as they see fit. Change the wording to "The Responsible Entity shall document a procedure defining the process to be used to update personnel risk assessments, and shall be able to demonstrate that the procedure is being followed."	Personnel risk assessments are required for personnel, including vendors and contractors, who have authorized cyber or unescorted physical access to Critical Cyber Assets. They are not required for personnel who are escorted or otherwise supervised. The standard no longer requires Social Security Number. Responsible Entities must ensure that contractor and vendor personnel risk assessments are conducted pursuant to the requirements in this standard. The period has been changed to 7 years. Personnel represent a significant vulnerability and periodic reassessment is useful in uncovering potentially serious problems that may otherwise be undiscovered or unobserved..
004-R4		
004-M1	Combine awareness and training into one annual requirement. Eliminate this measure.	See response to R1 above.

CIP-004 Drafting Team Responses to Comments

004-M2		
004-M3		
004-M4	What sort of evidence that access revocation has occurred is adequate?	Measures have been rewritten to refer back to the requirements.
004-C1,1		
004-C1,2		
004-C1,3	Compliance 1.3.1: Retention of personnel risk assessment documents for contractors and vendors for 3 years beyond their engagement will require additional privacy protection.	Data retention for personnel risk assessments has been changed.
004-C1,4		
004-C2,1	Compliance 2.1.5: Remove the requirement for quarterly awareness reinforcement. This should be annual and part of the training requirement.	Levels of noncompliance have been rewritten. See response to R1, above.
004-C2,2		
004-C2,3	Compliance 2.3.6: This simply requires that an entity follow their own internal practices and should be eliminated.	Measures have been rewritten to refer back to the requirements.
004-C2,4		

CIP-004 Drafting Team Responses to Comments

Name	Michal Zeithammel
Entity	Brascan Power
Ready to Ballot:	Yes

General Comments

004-R1

004-R2

004-R3

004-R4

004-M1

004-M2

004-M3

004-M4

004-C1,1

004-C1,2

004-C1,3

004-C1,4

004-C2,1

004-C2,2

004-C2,3

004-C2,4

CIP-004 Drafting Team Responses to Comments

Name	Guy Zito	
Entity	NPCC	
Ready to Ballot:	No	
General Comments	Change the purpose to "This standard requires that personnel having access to Critical Cyber Assets, including contractors and service vendors, have a higher level of personnel risk assessment, training and security awareness than personnel not provided access." Comment - access could be electronic, physical or both. This Standard's compliance is too prescriptive. This Standard has 4 Requirements and 4 Measures. The first three Compliance Levels have at least 5 clauses.	Please see responses to Ray A'Brial, Central Hudson Gas & Electric Corp.
004-R1		
004-R2	R2.1 should be reworded to state "All personnel having access to Critical Cyber Assets shall have received cyber security training appropriate to their role."	
004-R3	NPCC Participating Members suggest the Drafting team combine and clarify R3.1 with/to R3.2. Suggest that the correct order of these sections is R3 (risk assessment), R2 (training), R4 (access), and R1 (awareness). Change the old R3.2.2 from five years to ten years to be consistent with with Federal security clearance.	
004-R4	R4.1 requires a quarterly review. This is too prescriptive and does not match M4. We recommend an annual review and signed by the person authorizing. Add R4.3 Unauthorized personnel must be escorted by authorized personnel	
004-M1	Reorder to stay consistent with R1 - R4	
004-M2		
004-M3		
004-M4		
004-C1,1		
004-C1,2		
004-C1,3		
004-C1,4		

CIP-004 Drafting Team Responses to Comments

004-C2,1 Update 2.1.1 to remain consistent with R4.1 and M4. Change the words from "for more than three months but less than six months;

to

annually.

Failure to document the personnel risk assessment gives rise to both Level 1 non-compliance (2.1.3) and Level 3 non-compliance (2.3.3). This is confusing and should be resolved.

004-C2,2 Remove 2.2.1 since it is covered by the updated 2.1.1.

Failure of the Training program to address two or more required items gives rise to non-compliance at Level 2 (2.2.3) and Level 3 (2.3.4). This is confusing and should be resolved.

004-C2,3 Eliminate 2.3.7 since it is covered by 2.1.3.

004-C2,4

CIP-005 Drafting Team Responses to Comments

Name	Raymond A'Brial	
Entity	Central Hudson Gas & Electric Corp	
Ready to Ballot:	No	
General Comments		
005-R1		
005-R2	Recommend removing the second and third paragraph in R2.4. These paragraphs are too much detail, too prescriptive and border on examples.	The second and third paragraphs have been removed.
005-R3	Logs can be very large. People review reports that use logs as input. R3.3 should be changed to "At least every ninety calendar days assess access logs for unauthorized access or attempts."	The word "assess" has been added
005-R4		
005-R5		
005-M1		
005-M2		
005-M3		
005-M4		
005-M5		
005-C1,1		
005-C1,2		
005-C1,3		
005-C1,4		
005-C2,1	Compliance Statements 2.1.2, 2.2.2, and 2.3.4 effectively impose requirements on the availability of monitoring controls which are inconsistent with the requirements of R3.2	Requirement R3.2 has been removed and R3 has been clarified.
005-C2,2		
005-C2,3	Either Compliance statement 2.3.2 is redundant (given compliance statement 2.2.3) or it appears that the Standard authors contemplate that Responsible Entities need to perform both an annual assessment of open ports and services and an annual vulnerability assessment. In otherwords, failure to perform a vulnerability assessment in the past year would result in Level 2 non-compliance, but would also result in Level 3 non-compliance.	Non-compliance level 2.3.2 specifically addresses network ports and services at the access points. Non-compliance level 2.2.3 addresses the vulnerability assessment requirements. A vulnerability assessment includes more than just an assessment of ports and services. If the vulnerability assessment includes a review of ports and services, then the requirement for review of ports and services has been satisfied. The

	We suggest that the 2.3.4.1 words should resemble 2.2.2.	wording in 2.3.4.1 has been revised and the levels of non-compliance have been adjusted for better clarity.
005-C2,4		

CIP-005 Drafting Team Responses to Comments

Name	Ori Artman
Entity	Teltone
Ready to Ballot:	Yes
General Comments	
005-R1	
005-R2	
005-R3	
005-R4	
005-R5	
005-M1	
005-M2	
005-M3	
005-M4	
005-M5	
005-C1,1	
005-C1,2	
005-C1,3	
005-C1,4	
005-C2,1	
005-C2,2	
005-C2,3	
005-C2,4	

CIP-005 Drafting Team Responses to Comments

Name	Steve Badgett
Entity	Riverside Public Utilitities
Ready to Ballot:	Yes
General Comments	
005-R1	
005-R2	
005-R3	
005-R4	
005-R5	
005-M1	
005-M2	
005-M3	
005-M4	
005-M5	
005-C1,1	
005-C1,2	
005-C1,3	
005-C1,4	
005-C2,1	
005-C2,2	
005-C2,3	
005-C2,4	

CIP-005 Drafting Team Responses to Comments

Name	Terry Baker
Entity	Platte River Power Authority
Ready to Ballot:	Yes
General Comments	
005-R1	
005-R2	
005-R3	
005-R4	
005-R5	
005-M1	
005-M2	
005-M3	
005-M4	
005-M5	
005-C1,1	
005-C1,2	
005-C1,3	
005-C1,4	
005-C2,1	
005-C2,2	
005-C2,3	
005-C2,4	

CIP-005 Drafting Team Responses to Comments

Name	Terry Bilke
Entity	Midwest ISO
Ready to Ballot:	No
General Comments	
005-R1	
005-R2	
005-R3	
005-R4	
005-R5	
005-M1	
005-M2	
005-M3	
005-M4	
005-M5	
005-C1,1	
005-C1,2	
005-C1,3	
005-C1,4	
005-C2,1	
005-C2,2	
005-C2,3	
005-C2,4	

CIP-005 Drafting Team Responses to Comments

Name	Pat Bourassa	
Entity	Wisconsin Public Service Corporation	
Ready to Ballot:	No	
General Comments		
005-R1	R1.4 Non critical cyber assets within the perimeter should not be subject to the standard. By definition a non critical cyber asset would not affect the grid. R1.5 Access control and monitoring requires more clarification and thought. As written, one could argue that this would include all access control and monitoring systems used on the network.	R1.4. CIP-005 addresses controls at access points to the Electronic Security Perimter. 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 protected perimeter may affect the operation of the Critical Cyber Assets within it. Please refer to the FAQs for CIP-005. R1.5 This requirement clearly states "used in the access control and monitoring of the Electronic Security Perimeter(s)."
005-R2		
005-R3	R3.1 Single point access control at each location is technically feasible but may be cost prohibitive and imprudent based on location and level of risk.	R3.1 requires that if monitoring is technically feasible, it must be implemented using reasonable business judgment. Refer to the FAQ for a discussion of technical feasibility.
005-R4		
005-R5	This requirement implies performance of vulnerability testing against every access point in every electronic security perimeter annually. This is both risky and expensive. Vulnerability tests can be extremely resource intensive and time consuming. Risk evaluations should be conducted and testing of the identified vulnerabilities can then be conducted.	We believe you are referring to R4. The requirement in R4.2 has been changed to review. Scanning is not required.
005-M1		
005-M2		
005-M3		
005-M4		
005-M5		
005-C1,1		
005-C1,2		

CIP-005 Drafting Team Responses to Comments

005-C1,3

005-C1,4

005-C2,1

005-C2,2

005-C2,3

005-C2,4

Name	Laurence W. Brown	
Entity	Edison Electric Institute	
Ready to Ballot:	No	
General Comments		
005-R1	R1.4 -- The reference to "this standard" is somewhat confusing. By being afforded the protections of CIP-005, and with the specific reference to coverage in CIP-007-R1, non-critical cyber assets are essentially covered under all of the proposed Standards. Thus the phrase "this standard" should in this particular circumstance be changed to "these standards." Alternatively, explicit references should be added to assist Responsible Entities in understanding how such matters as personnel training, policies, etc. should apply to such non-critical assets. However, consideration should also be given to moving this item to, or mentioning such assets in, CIP-002, as that is the Standard generally addressing covered assets. Certainly, it is unnecessarily inconvenient, and even somewhat confusing, that a full determination of the responsibilities regarding such assets cannot be ascertained without reference both to CIP-007 and this Standard.	R1.4 This requirement has been revised to refer specifically to CIP-005. R1.5 The word reasonable is subjective and difficult to assess in compliance monitoring. The wording has been amended to refer to protective measures specified in Standard CIP-004 Requirement R3, Standard CIP-005 Requirements R2 and R3, Standard CIP-006 Requirements R2 and R3, Standard CIP-008, and Standard CIP-009.
	R1.5 -- It would be unreasonable to assume that this Requirement is intended to produce an infinite regression, or "race condition," yet a literal reading would have that effect. Some clarification should be placed here, or in the FAQs, to indicate otherwise. Further, the definition of Cyber Asset in this context could lead to affording a high level of protection to such assets as remotely-controlable video cameras. An approach that could remedy both problems would be to require that these facilities be given "reasonable" protections "similar" to those afforded to Critical Cyber Assets. Consideration should also be given to moving this item to, or mentioning these assets in, CIP-002, as that is the Standard generally addressing covered assets.	
005-R2	R2.1 -- The phrase "emergency operations" is unclear in this context. Are such ports and services to be enabled at all times, or only during emergency operations? The latter would appear to be safer, but the former might be necessary to enable immediate use. Also, this appears to duplicate CIP-007-R3. The two should be combined and located in only one Standard.	R2.1 The requirement, in its current wording, gives the Responsible Entity the option of taking either one of these approaches without being non-compliant. The "emergency" clause has been removed because the term "operations" include all cases where they are necessary for operations.
	R2.1, 2.1.1, and 2.1.2 together appear more detailed and burdensome than necessary. The level of documentation required will not guarantee effective security. Both sub-requirements R2.1.1 and 2.1.2 could be eliminated or relaced with a requirement for sufficient documentation to indicate reasonable procedures to assure security.	The standard has been revised and 2.1.1 and 2.1.2 have been removed. A record of configuration could be sufficient documentation. Grouping is specifically allowed.
	If R2.1.1 and 2.1.2 are retained, however, R2.1.2 appears to require an individual accounting of each and every single port and service, at each and every individual access point, and thus is overly burdensome (SEE C2.3.3, below). Producing and maintaining documentation on each individual port and service is futile because many services are dynamic, bringing themselves up and taking themselves down as needed, many services	CIP-005 addresses access points to the Electronic Security Perimeter, while CIP-007 addresses cyber assets themselves.

	use dynamic port numbers, and there is some thought that port-number information is not really crucial, since they are represented simply by a data field in the packet header that can be manipulated. Moreover, scanning pursuant to R4.2 below, and/or assessments pursuant to CIP-009-R9 should provide sufficient knowledge to permit appropriate protection. For all of these considerations, no reasonable entity would attempt such detailed accounting, and thus the Standard must be clarified to indicate that some form of grouping or class accounting is permitted. SEE ALSO the below comments relating to CIP-007-R3. Again, much of this requirement should reference that one, or one or the other should be relocated. Suggested Alternative Wording: "The Responsible Entity shall document>, either individually and/or by specified grouping, reasonable assessment and control of< the status and configuration of >< ports and services enabled on >< access points to the Electronic Security Perimeter(s)."	
005-R3		
005-R4	SEE ALSO the below comments relating to CIP-007-R3. This requirement should reference that one, or one or the other should be relocated.	CIP-005 addresses access points to the Electronic Security Perimeter, while CIP-007 addresses requirements to assets within the Electronic Security Perimeter.
005-R5		
005-M1	This should be simplified in the same manner as have been most of the Measures for CIP-007. The below proposed language for M2 is an appropriate model.	Measures have been reworded and simplified.
005-M2	Measures have been reworded and simplified.	Measures have been reworded and simplified.
005-M3	This should be simplified in the same manner as have been most of the Measures for CIP-007. The above proposed language for M2 is an appropriate model.	Measures have been reworded and simplified.
005-M4	This should be simplified in the same manner as have been most of the Measures for CIP-007. The above proposed language for M2 is an appropriate model.	Measures have been reworded and simplified.
005-M5	This should be simplified in the same manner as have been most of the Measures for CIP-007. The above proposed language for M2 is an appropriate model.	Measures have been reworded and simplified.
005-C1,1		
005-C1,2		
005-C1,3		
005-C1,4		
005-C2,1	C2.1.2 -- The term "aggregate" is unclear. Does it cover all perimeters, or the aggregate for each perimeter? Also, the six-hour criterion is not consistent with the seven-day criterion for Physical Security Perimeters specified in CIP-006-C2.1.2. Six hours is far too short for such frequent interruptions as are caused by lightening.	The criteria for non-compliance have been changed from duration to percentage of sites which are deficient. The time-frame has been removed.

005-C2,2		
005-C2,3	C2.3.3 -- The phrase "one or more access points" seems to reinforce the comments above at R2.1. Consistent with the comments at that location, such point-by-point documentation is overly burdensome and should not be required.	Please refer to response at R2.
005-C2,4		

CIP-005 Drafting Team Responses to Comments

Name	Peter Burke	
Entity	American Transmission Company	
Ready to Ballot:	No	
General Comments	American Transmission Company concurs with the comments submitted separately by the Edison Electric Institute and by the Midwest Reliability Organization.	See responses to Laurence Brown, EEI.
005-R1	American Transmission Company concurs with the comments submitted separately by the Edison Electric Institute.	
005-R2	American Transmission Company concurs with the comments submitted separately by the Edison Electric Institute.	
005-R3	American Transmission Company concurs with the comments submitted separately by the Midwest Reliability Organization.	
005-R4	American Transmission Company concurs with the comments submitted separately by the Edison Electric Institute.	
005-R5		
005-M1	American Transmission Company concurs with the comments submitted separately by the Edison Electric Institute.	
005-M2		
005-M3	American Transmission Company concurs with the comments submitted separately by the Edison Electric Institute.	
005-M4	American Transmission Company concurs with the comments submitted separately by the Edison Electric Institute.	
005-M5	American Transmission Company concurs with the comments submitted separately by the Edison Electric Institute.	
005-C1,1		
005-C1,2		
005-C1,3		
005-C1,4		
005-C2,1	American Transmission Company concurs with the comments submitted separately by the Edison Electric Institute.	
005-C2,2		
005-C2,3	American Transmission Company concurs with the comments submitted separately by the Edison Electric Institute.	

005-C2,4

CIP-005 Drafting Team Responses to Comments

Name	Marc Butts	
Entity	Southern Company	
Ready to Ballot:	No	
General Comments		
005-R1	R1.4 Clarify 'this' in the phrase 'this standard'. Since the standard states in the purpose that "this standard should be read as part of a group of standards numbered CIP-002 through CIP-009" it is unclear from the language what standards apply. Suggest replacing "this standard" with "CIP-005" if that is the intent. R1.5 Change "shall be afforded the same protections as" to "shall be subject to the requirements of this standard."	The language in the standard has been modified to clarify that this standard refers to CIP-005. 1.5 --The language has been clarified to read "afforded the protective measures specified in StandardCIP-004 Requirement R3, Standard CIP-005 Requirements R2 and R3, Standard CIP-006 Requirements R2 and R3, Standard CIP-008 and Standard CIP-009."
005-R2	R2.1. We suggest replacing this section with the following language: At all access points to the Electronic Security Perimeter(s), the Responsible Entity shall enable, during "production" usage, only those ports and services that are required for normal operations or for operation during emergencies, as well as those required for monitoring Cyber Assets within the Electronic Security Perimeter, and shall provide documentation thereof. With the following conforming change to Level 3 Noncompliance #2.3.3: Electronic access controls document(s) exist, but (either individually or by specified grouping) regarding some access point or points one or more "open" or enabled access ports or services have not been identified, or the documents fail to identify or describe access controls; or, R2.1.1. - We suggest adding language that says "the ports need to be closed after testing". R2.1.2. - This section is redundant to section 2.1 and should be removed. R2.1 - On the issue of ports, the requirements and measures around ports and services need to be reworked. This section should be re-worded to create two short requirements that say something like: a. That all unnecessary ports/services are disabled, and b. That the entity audits itself against the above requirement on a periodic (at least annual) basis and maintains documentation of these audits. This audit is already required in R4.2 of CIP-005. This would apply at both the perimeter (CIP-005) and at the asset itself (CIP-007). What we should show a regional auditor is documentation that shows we audited ourselves, with the date of our audit, the results of our audit, and a mitigation plan to show we fixed/are fixing any problems we found.	The language in 2.1 has been amended and simplified, taking these comments into consideration.
005-R3		

005-R4		
005-R5		
005-M1		
005-M2		
005-M3		
005-M4		
005-M5		
005-C1,1		
005-C1,2		
005-C1,3		
005-C1,4		
005-C2,1	2.1.2 Level 1 - There is a wide disparity between the gaps allowed in monitoring of the electronic vs physical perimeters before a L1 noncompliance is reached. For an electronic perimeter, it's six hours, for a physical perimeter, it's a week. We suggest keeping the non-compliance levels the same and the physical measures seem the most reasonable. It may take six hours to travel and replace a failed monitoring component and this should not trigger a non-compliance. This trickles down through all the non-compliance levels of this standard. Replace "aggregate" with "cumulative" in all these sections. 2.1.2 Level 1 - Does this apply 'per perimeter' or 'across all perimeters'? This needs to be addressed on all non-compliance levels for both electronic and physical perimeters. The standard drives one to establish numerous small perimeters around individual cyber assets and measuring and monitoring the amount of aggregate downtime is an effort that may be above and beyond the benefit.	The criteria for non-compliance have been changed from duration to percentage of electronic security perimeters that are non-compliant. References to monitoring hours have been removed.
005-C2,2		
005-C2,3		
005-C2,4		

CIP-005 Drafting Team Responses to Comments

Name	Linda Campbell	
Entity	FRCC	
Ready to Ballot:	No	
General Comments		
005-R1	R1.4 and R1.5 Is it the intent of these two requirements are to bring "non-critical assets in the electronic security perimeter" and "cyber assets used in control and monitoring of the electronic security perimeter" into the scope of all CIP-02 thru 009 standards or only that they meet the requirements of the CIP-005 standard? If into the scope of all the standards, shouldn’t these requirements be identified in CIP-002 rather than here? If it is intended that they meet the requirements of CIP-005, then should both should say "shall be subject to the requirements of CIP-005-001? If not subject to all requirements, please be specific as to which requirements each of these types of assets are subject to. The wording of 1.5 needs to be clarified and our hope is that the committee will consider the central security organizations and not intentionally (or unintentionally) cause reorganizations or physical movement of groups in order to manage firewall consoles. R1.5 What is considered "a protection"? For instance, the physical security controls have a specific requirement to be tested and maintained. CIP-005 doesn’t mention the same specific requirements for the electronic controls, monitoring, and logging. Are these "the protections" to which you refer? R1.5 Do the "same protections" mean electronic protections or electronic and physical protection? How far do you take this? Are you including workstations? - for instance, what protection does a laptop or workstation not in the electronic (nor physical) perimeter but which has access to protected networks through a firewall to access the firewall console for log monitoring purposes require? For centralized security departments, these workstations or laptops may also access non-protected assets to monitor their firewall consoles.	The language of the standard has been clarified to read " Any non-critical Cyber Asset within a defined Electronic Security Perimeter shall be identified and subjected to the requirements of Standard CIP-005." 1.5 The requirement was never intended to cause a general re-location or re-organization of people or equipment. However, the cyber assets referred to must be protected per the specified requirements. It is up to Responsible Entities to determine what circumstances may necessitate relocation or reorganization. R1.5 has been changed to read "afforded the protective measures specified in StandardCIP-004 Requirement R3, Standard CIP-005 Requirements R2 and R3, Standard CIP-006 Requirements R2 and R3, Standard CIP-008 and Standard CIP-009." R1.5 specifies the protection of assets used to control and monitor the Electronic Security Perimeter(s).
005-R2	R2.1 Change the following wording: From: ...only those ports and services that .... To: ...only those ports and services, and only those specific hosts, that... R2.2.3 I don’t see any review checklists defined in CIP-003 or 004 -- what is "review checklists" referring to?? If truly an example, and not required, perhaps this belongs in the FAQs. R2.5 Should replace "technically feasible" with "practical", because anything can be technically feasible or not depending on an entity’s budget. If the wording is not changed	CIP-005 addresses access points to the Electronic Security Perimeter, while CIP-007 addresses requirements to assets within the Electronic Security Perimeter. The examples will be removed from this requirement. R2.5 requires that if the banner is technically feasible, it must be implemented using reasonable business judgment. Refer to the FAQ for a discussion of technical feasibility.

	the requirement could force the Responsible Entity to implement an exception.	
005-R3	R3.1 Should replace "technically feasible" with "practical", because anything can be technically feasible or not depending on an entity's budget. If the wording is not changed the requirement could force the Responsible Entity to implement an exception.	R3.1 requires that if monitoring is technically feasible, it must be implemented using reasonable business judgment. Refer to the FAQ for a discussion of technical feasibility.
005-R4	R4.2 Control Systems are typically not tolerant of scanning as it can create enough console messages to affect the performance or bring down the system. We strongly feel the Drafting Team should reconsider this requirement to scan ports and services through the access points (i.e. a firewall). An organization that has misconfigured a firewall would run the risk of impacting stability or performance of control systems. The same information can be gathered through a detailed assessment of the rule base or filtering on an access point to the perimeter at no risk. Since this assessment is required in R3 of CIP-007-1, this requirement should be removed.	The requirement in R4.2 has been changed to review. Scanning is not required.
005-R5		
005-M1		
005-M2	The reference to business records has been removed. The Drafting Team has revised the standards for consistency. Please see the FAQs.	The reference to business records has been removed. The Drafting Team has revised the standards for consistency. Please see the FAQs.
005-M3	M3 This is first use of the term "business records" in the standard. What constitutes a "business record" and how does it differ from measures in previous sections of the standards from "data", "document" or "documentation." M3.2 To correspond with R3.2, add to the beginning of this measure, "For those assets where monitoring controls have not been implemented, ..." M3.3 same question re "business records" as above	See response to comment, above.
005-M4	Strike M4.1 and M4.2 as they restate R4. M4 includes every type of documentation as listed under R4 should suffice. Or the measurements section can mirror R4 by restating all five sections.	Measures have been rewritten to refer back to the requirments.
005-M5		
005-C1,1	In the applicability section 4.1.10 and 4.1.11, RRO's and NERC are included. Who has the monitoring responsibility for a RRO or NERC?	NERC will monitor the RROs and a third party without vested interest in the outcome will monitor NERC.
	Add Self-Certification and Audit information to this section. Proposed language would be: 1.1.--Complaince Monitoring Responsibility Regional Reliability Organization. 1.1.1.--The Compliance Monitor will request a self-certification annually. 1.1.2.--The Compliance Monitor will perform an audit at least once every three (3) calendar years.	Self-certification has been added under "Additional Compliance Information."

005-C1,2		
005-C1,3	To complement a audit every three years, the data retention period should be 3 years.	Only the compliance monitor is required to keep records of an audit for 3 years.
005-C1,4		
005-C2,1		
005-C2,2		
005-C2,3		
005-C2,4		

CIP-005 Drafting Team Responses to Comments

Name	Gary Campbell	
Entity	MAIN	
Ready to Ballot:	No	
General Comments	Need to address items below	See responses below.
005-R1		
005-R2		
005-R3		
005-R4		
005-R5		
005-M1		
005-M2		
005-M3		
005-M4		
005-M5		
005-C1,1		
005-C1,2		
005-C1,3		
005-C1,4		
005-C2,1	2.1.1 Delete "Aggregate", Too vague. Leave as "Interruptions in the ...."	The criteria for levels of non-compliance have been changed to percentages of Electronic Security Perimeters.
005-C2,2	2.2.1 Do not see the requirement where all documents must be updated annually.	R5 specifies review and update requirements.
005-C2,3	2.3.1 How is the entity to ensure or verify that all assets are within the perimeter. Specify the conditions int the requirement which will define a valid verification. 2.3.2 What is "only necessary"? Be Specific. 2.3.3 As an auditior, how can I be sure that one or more access point may not have been identified? 2.3.4. Could not find the requirement covering 7 calendar days.	2.3.1 Reference to verification has been removed. Compare actual network configuration to documented perimeters and ensure that all critical cyber asset listed in CIP-002 are accounted for in these perimeters. 2.3.2 Reference has been removed. 2.3.3 Compliance monitors must rely on reviews and comparisons of required documentation and interviews with appropriate personnel.

		2.3.4 The reference to 7 days has been removed.
005-C2,4	2.4.2 Suggest changing to " Access Records do not exist for all access points of 5 or more electronic security perimenters. You would also need to define some lesser level of non-compliance of the same nature. 2.4.3 Suggest changing to " Monitoring Records do not exist for all access points of 5 or more electronic security perimenters. You would also need to define some lesser level of non-compliance of the same nature. As written, both 2.4.2 and 2.4.3 leave large gaps in the measuring for non-compliance.	Pertinent levels of non-compliance have been rewritten and gaps have been eliminated. The criteria for levels of non-compliance have been changed to percentages of Electronic Security Perimeters.

CIP-005 Drafting Team Responses to Comments

Name	Roger Champagne	
Entity	Hydro-Québec TransÉnergie	
Ready to Ballot:	No	
General Comments	NERCNet should be clearly discussed here. 4.2.1. Nuclear should be included since US NRC or Canadian NSC don't cover cyber security. We thought that the use of the word "routable" was a good idea, but in practice, it would not cover a lot of problems. First, a modem using pcAnywhere (or other) are not using routable protocol. So the standard allows someone, from his own computer at home, to control the network if he has an antivirus, a firewall and using pcAnywhere. If his children access that computer, it is very dangerous. Remote computers should be only allowed if the computer is owned by the company, the person does not have admin rights on it, the connection does not allow another connection at the same time, a lot of tests are done before making the connection, a two factor authentification is used (SecudID is only one factor authentification !), and the connection is intiated inside the electronic perimeter... Second, a lot of protocol (like X.25) are routable, but there is no firewall for them. X.25 is so old that it is very secure against hackers ! So most of these protocols will use C1.4 "Duly authorized exception"	Communication links between electronic security perimeters such as NERCnet are outside the scope of these standards. Nuclear facilities are outside the scope of these standards. A dial-up modem is an access point to the perimeter, and is subject to the access control and monitoring controls of this standard. In addition, CIP-005 R2 clearly states that strong procedural and technical mechanisms are required. Note that SecurId is considered two factor authentication: something you have (the SecurId token) and something you know (the PIN number). X.25 is not a network layer routable protocol, it is a link layer protocol. For answers to the remaining comments, refer to the response to Ray A'Brial, Central Hudson Gas and Electric Corp.
005-R1		
005-R2	Recommend removing the second and third paragraph in R2.4. These paragraphs are too much detail, too prescriptive and border on examples.	
005-R3	Logs can be very large. People review reports that use logs as input. R3.3 should be changed to "At least every ninety calendar days, the Responsible Entity shall assess access logs for unauthorized access or attempts."	
005-R4		
005-R5		
005-M1		
005-M2		
005-M3		
005-M4		
005-M5		
005-C1,1		

005-C1,2	
005-C1,3	
005-C1,4	
005-C2,1	Compliance Statements 2.1.2, 2.2.2, and 2.3.4 effectively impose requirements on the availability of monitoring controls which are inconsistent with the requirements of R3.2
005-C2,2	
005-C2,3	Either Compliance statement 2.3.2 is redundant (given compliance statement 2.2.3) or it appears that the Standard authors contemplate that Responsible Entities need to perform both an annual assessment of open ports and services and an annual vulnerability assessment. In otherwords, failure to perform a vulnerability assessment in the past year would result in Level 2 non-compliance, but would also result in Level 3 non-compliance.
	We suggest that the 2.3.4.1 words should resemble 2.2.2.
005-C2,4	

CIP-005 Drafting Team Responses to Comments

Name	Larry Conrad
Entity	ECAR Critical Infrastructure Protection Panel
Ready to Ballot:	Yes
General Comments	
005-R1	
005-R2	
005-R3	
005-R4	
005-R5	
005-M1	
005-M2	
005-M3	
005-M4	
005-M5	
005-C1,1	
005-C1,2	
005-C1,3	
005-C1,4	
005-C2,1	
005-C2,2	
005-C2,3	
005-C2,4	

CIP-005 Drafting Team Responses to Comments

Name	Larry Conrad	
Entity	Cinergy	
Ready to Ballot:	No	
General Comments		
005-R1	Please provide additional explanation of the phrase "define an electronic security perimeter for that single access point at the dial up device." Consider including this answer as an FAQ.	A clarification has been included in the FAQ.
005-R2	Please explain what is required by: "The Responsible Entity shall document the status and configuration of all ports and services enabled on all access points to the Electronic Perimeter."	Different access control devices implement different mechanisms for allowing ports or services. For most firewalls, the firewall rules can provide such documentation. For routers, the access control lists provide such information.
005-R3	Logs of electronic access must be reviewed for unauthorized access or attempts every 90 days. A full review of logs showing all electronic access is impractical on any timeframe. Modify this requirement to make it clear that only the electronic logs will be reviewed. Recommend changing the language to indicate that a report showing only exceptions such as unauthorized electronic access or unsuccessful attempts at electronic access (as opposed to all access or attempts) will be reviewed. Cinergy also recommends that CIP-005-1 Requirements section be modified to include language that excludes operator consoles from being included in the electronic perimeter.	The requirement has been modified to require an assessment of logs at least every 90 calendar days where real-time alerting has not been implemented. Operator consoles are critical cyber assets if they are used to control critical assets, and therefore, must be inside an Electronic Security Perimeter.
005-R4		
005-R5		
005-M1		
005-M2		
005-M3		
005-M4		
005-M5		
005-C1,1		
005-C1,2		
005-C1,3		

CIP-005 Drafting Team Responses to Comments

005-C1,4

005-C2,1

005-C2,2

005-C2,3

005-C2,4

CIP-005 Drafting Team Responses to Comments

Name	Theodore Creedon, P.E.	
Entity	Creedon Engineering	
Ready to Ballot:	No	
General Comments	Defense in depth is not required. Large systems need multiple rings of protection.	Responsible Entities may implement controls that are beyond theminimum requirements in the standard.
005-R1	R 1. Recommend multiple rings of protection where necessary. R 1.2 Include RF and optical (IR) links.	Responsible Entities may implement controls that are beyond the minimum requirements in the standard. RF and IR are implicit in the R1, whereas R1.2 specifically addresses dial-up accessible assets. R1.2 specifically addresses dial-up accessible assets. Entities may apply the standards to additional assets.
005-R2		
005-R3	Clarify that R 3.3 requires logging of attacks at the firewall. Recommend that all IP packets be recorded and archived. Unauthorized access attempts result in dropped packets. Successful attacks result in accepted packets. Intrusion can not be detected without extensive logging. THere is a vast amount of data involved here. See http://www.nswc.navy.mil/ISSEC/CID/ for information on implementation.	Responsible Entities may implement controls that are beyond the minimum requirements in the standard.
005-R4		
005-R5		
005-M1		
005-M2		
005-M3		
005-M4		
005-M5		
005-C1,1		
005-C1,2		
005-C1,3		

005-C1,4

005-C2,1

005-C2,2

005-C2,3

005-C2,4

CIP-005 Drafting Team Responses to Comments

Name	Joel De Granda
Entity	Florida Power and Light
Ready to Ballot:	Yes
General Comments	
005-R1	
005-R2	
005-R3	
005-R4	
005-R5	
005-M1	
005-M2	
005-M3	
005-M4	
005-M5	
005-C1,1	
005-C1,2	
005-C1,3	
005-C1,4	
005-C2,1	
005-C2,2	
005-C2,3	
005-C2,4	

CIP-005 Drafting Team Responses to Comments

Name	Richard Engelbrecht	
Entity	RGE	
Ready to Ballot:	No	
General Comments		Please refer to answers to Ray A'Brial of Central Hudson Gas and Electric Corp.
005-R1		
005-R2	Recommend removing the second and third paragraph in R2.4. These paragraphs are too much detail, too prescriptive and border on examples.	
005-R3	Logs can be very large. People review reports that use logs as input. R3.3 should be changed to "At least every ninety calendar days assess access logs for unauthorized access or attempts."	
005-R4		
005-R5		
005-M1		
005-M2		
005-M3		
005-M4		
005-M5		
005-C1,1		
005-C1,2		
005-C1,3		
005-C1,4		
005-C2,1	Compliance Statements 2.1.2, 2.2.2, and 2.3.4 effectively impose requirements on the availability of monitoring controls which are inconsistent with the requirements of R3.2	
005-C2,2		
005-C2,3	Either Compliance statement 2.3.2 is redundant (given compliance statement 2.2.3) or it appears that the Standard authors contemplate that Responsible Entities need to perform both an annual assessment of open ports and services and an annual vulnerability assessment. In otherwords, failure to perform a vulnerability assessment in the past year would result in Level 2 non-compliance, but would also result in Level 3 non-compliance.	

We suggest that the 2.3.4.1 words should resemble 2.2.2.

005-C2,4

CIP-005 Drafting Team Responses to Comments

Name	Ken Fell	
Entity	New York ISO	
Ready to Ballot:	No	
General Comments		Please refer to answers to Ray A’Brial of Central Hudson Gas and Electric Corp.
005-R1		
005-R2	Recommend removing the second and third paragraph in R2.4. These paragraphs are too much detail, too prescriptive and border on examples.	
005-R3	Logs can be very large. People review reports that use logs as input. R3.3 should be changed to "At least every ninety calendar days assess access logs for unauthorized access or attempts."	
005-R4		
005-R5		
005-M1		
005-M2		
005-M3		
005-M4		
005-M5		
005-C1,1		
005-C1,2		
005-C1,3		
005-C1,4		
005-C2,1	Compliance Statements 2.1.2, 2.2.2, and 2.3.4 effectively impose requirements on the availability of monitoring controls which are inconsistent with the requirements of R3.2	
005-C2,2		
005-C2,3	Either Compliance statement 2.3.2 is redundant (given compliance statement 2.2.3) or it appears that the Standard authors contemplate that Responsible Entities need to perform both an annual assessment of open ports and services and an annual vulnerability assessment. In otherwords, failure to perform a vulnerability assessment in the past year would result in Level 2 non-compliance, but would also result in Level 3 non-compliance.	

We suggest that the 2.3.4.1 words should resemble 2.2.2.

005-C2,4

CIP-005 Drafting Team Responses to Comments

Name	Francis Flynn	
Entity	National Grid USA	
Ready to Ballot:	No	
General Comments		Please refer to answers to Ray A’Brial of Central Hudson Gas and Electric Corp.
005-R1		
005-R2	Recommend removing the second and third paragraph in R2.4. These paragraphs are too much detail, too prescriptive and border on examples.	R2.4 has been rewritten.
	National Grid also believes that Requirements R2.1, R2.1.1 and R2.1.2 seem to suggest that the access control model of requirment R2 be based soley on IP port numbers (e.g. services). If this is the case then the access control model is not adequate. As an example, if port 20000 (DNP via IP) access is allowed, the proposed model does not prohibit an unauthorized IP host to make a connection to an RTU via port 20000. Accordingly, Requirment R2 should be enhanced to require an access control model based on both IP port numbers and IP addresses.	The requirement for ports and services only ensures that only authorized services are enabled. Requirement R2.2 deals with access control. The access control may be based on IP address, or other parameters such as a host certificate or a two factor authentication, both of which do not use the IP address as authentication of the source host.
005-R3	Logs can be very large. People review reports that use logs as input. R3.3 should be changed to "At least every ninety calendar days assess access logs for unauthorized access or attempts."	Please refer to answers to Ray A’Brial of Central Hudson Gas and Electric Corp.
005-R4		
005-R5		
005-M1		
005-M2		
005-M3		
005-M4		
005-M5		
005-C1,1		
005-C1,2		
005-C1,3		
005-C1,4		
005-C2,1	Compliance Statements 2.1.2, 2.2.2, and 2.3.4 effectively impose requirements on the availability of monitoring controls which are inconsistent with the requirements of R3.2	Please refer to answers to Ray A’Brial of Central Hudson Gas and Electric Co.

005-C2,2		
005-C2,3	Either Compliance statement 2.3.2 is redundant (given compliance statement 2.2.3) or it appears that the Standard authors contemplate that Responsible Entities need to perform both an annual assessment of open ports and services and an annual vulnerability assessment. In otherwords, failure to perform a vulnerability assessment in the past year would result in Level 2 non-compliance, but would also result in Level 3 non-compliance. We suggest that the 2.3.4.1 words should resemble 2.2.2.	Please refer to answers to Ray A'Brial of Central Hudson Gas and Electric Co.
005-C2,4		

CIP-005 Drafting Team Responses to Comments

Name	Greg Fraser	
Entity	Manitoba Hydro	
Ready to Ballot:	No	
General Comments	Introduction 4.2.3 should read the same as in CIP-009-1 which is: "Responsible Entities that, in compliance with Standard CIP-002, identify that they have no Critical Cyber Assets."	The language in the standard has been modified.
005-R1	Non-Critical Cyber Assets in R1.4 and Cyber Assets in R1.5 should be mentioned in the paragraph R1 which just mentions Critical Cyber Assets. It needs to be made very clear that all three of these Cyber Assets must be managed including documentation (lists), access controls, etc. Most of the requirements in CIP-005 where it just mentions Critical Cyber Assets should specify all three types of Cyber Assets as they all can affect the security of the Critical Cyber Assets.	The requirements have been clarified to state that an Electronic Security Perimeter must be defined for Critical Cyber Assets. Requirement R1.4 qualifies that the protections defined in CIP-005 are applicable to non-critical Cyber Assets that are also within that perimeter. R1.5 qualifies that cyber assets used in the control and monitoring of the Electronic Security Perimeter must also be protected per specific requirements.
005-R2		
005-R3	R3.2 see comment under R1.	R3.2 has been removed.
005-R4		
005-R5		
005-M1		
005-M2		
005-M3		
005-M4	In M4.2 "...the execution status of the plan" is a new item which is not included in the requirement.	The documentation of the execution status of the plan has been included in the requirement.
005-M5		
005-C1,1		
005-C1,2		
005-C1,3		
005-C1,4		
005-C2,1	In 2.1.2 "Aggregate interruptions" is not defined as to whether this in the summation of multi-interruptions per year or the same interruption for multi-assets or both. Tracking the interruptions for the assets is not part of the requirements. This compliance requirement appears to be unrealistic and too stringent depending on the response the comments above.	The criteria for levels of non-compliance have been changed to percentages of Electronic Security Perimeters.

CIP-005 Drafting Team Responses to Comments

005-C2,2

005-C2,3

005-C2,4

CIP-005 Drafting Team Responses to Comments

Name	Jerry Freese	
Entity	American Electric Power	
Ready to Ballot:	Yes	
General Comments	Based on the expanded scope set forth in CIP-002 R1 for the Critical Assets and the subsequently expanded scope of the Critical Cyber Assets and the Electronic Security Perimeter, it would be impractical and infeasible to meet the obligations set forth in this requirement.	CIP-002 has been changed.
005-R1		
005-R2		
005-R3	R3.1 - The standard requires implementation of "monitoring controls" at a single access point. It was unclear to me what this meant. An example(s) might be helpful.	R3 has been changed to refer to electronic or manual process(es) for monitoring and logging at access points to the Electronic Security Perimeter(s). 3.1 qualifies that if the access point is a modem, and if call logging is available, then a review of the log constitutes monitoring.
005-R4		
005-R5		
005-M1		
005-M2		
005-M3		
005-M4		
005-M5		
005-C1,1		
005-C1,2		
005-C1,3		
005-C1,4		
005-C2,1		
005-C2,2		
005-C2,3		
005-C2,4		

Name	Edwin C. Goff III	
Entity	Progress Energy	
Ready to Ballot:	No	
General Comments	Log/data retention is not addressed consistently between the physical and electronic security standards. In the electronic standard there is a data retention section in the compliance area. In the physical security standard there is a requirement (CIP-006-1 R6). Question for clarification: For the following discussion and question, please consider a scenario where there is a central data center housing a centralized Energy Management System (EMS) and a business Information System (IS). Assume there are a number of remote substations with each substation interconnected to the central data center through an IP router linked through a core IP network. Assume further the only electronic link between the substations and the central data center is through this core IP network. Assume also the remote SCADA systems at each of the substations are classified as Critical Assets and are contained within an Electronic Security Perimeter established at that substation. Assume further that an Electronic Security Perimeter has been established around the centralized EMS at the centralized data center. It is assumed the core transport IP network itself may not be secure. However, consider the use of Virtual Private Network (VPN) tunnels using 3DES (or other robust encryption systems) to provide two data tunnels between each of the remote substation sites and the centralized data center. One of the VPN tunnels at each substation would serve the SCADA (Critical Asset) systems exclusively, and the other VPN tunnel would serve the business needs of the craft personnel at that substation. The VPN dedicated for the Critical Cyber Assets would extend from the Electronic Security Perimeter at that substation to the Electronic Security Perimeter of the EMS system at the central data center. This would provide a secure, isolated, and protected electronic tunnel between the remote Critical Cyber Assets (i.e. the RTUs and connected equipments) at each substation and the centralized EMS. The only electronic access to the remote Critical Assets would be through these secured VPN links. Access to other non Critical Asset business systems (e-mail and other general business systems) by personnel at a remote substation could be accessed through the same IP data link and common core IP Network but through a different VPN. The use of VPNs would then provide secured, private, and protected links between the local and remote Electronic Security Perimeters as depicted in the Draft 3 FAQs. In effect, the use of VPNs would extend the Electronic Security Perimeters from the remote substations to the Electronic Security Perimeter of the centralized EMS.	Noted. This has been made consistent for all standards. The VPN is a communication path between discrete Electronic Security Perimeters, rather than extend one Electronic Security Perimeter. For this reason, some form of access control is required at the remote substation. The communication pathways between discrete Electronic Security Perimeters are outside the scope of the standard.

	Given this scenario, will there still be a need for an additional discrete firewall at the Electronic Security Perimeter at the remote substations?	
005-R1		
005-R2	The terminology "electronic access points to the Electronic Security Perimeter(s)" implies that there is NOT a host level (workstation, server, network gear, etc.) access control requirement. We believe the intent and expectation is to include access control to the assets within and CIP-007-1 R6 could not be met without it. Suggest that the wording be improved to include Critical Cyber Assets WITHIN the perimeter.	CIP-005 is specifically concerned with the Electronic Security Perimeter and the access points to that perimeter. If one of the access points to that perimeter is on a host within the perimeter (i.e. a modem connected to a host within that perimeter), then that access point is subject to the requirements of this standard. Controls that concern access to the host itself are covered in CIP-007.
005-R3		
005-R4		
005-R5		
005-M1		
005-M2		
005-M3		
005-M4		
005-M5		
005-C1,1		
005-C1,2		
005-C1,3		
005-C1,4		
005-C2,1	2.1.2 & 2.2.2-- These items indicate non-compliance for "Aggregate interruptions in the monitoring capability over a full calendar year exist for more than six hours (2.1.2) ...one calendar day(2.2.2)..." There is no previously stated requirement for keeping up with the availability of the access monitoring systems. This appears to create a requirement for logging the availability of the monitoring systems.	The criteria for levels of non-compliance have been changed to percentages of Electronic Security Perimeters.
005-C2,2	2.1.2 & 2.2.2-- These items indicate non-compliance for "Aggregate interruptions in the monitoring capability over a full calendar year exist for more than six hours (2.1.2) ...one calendar day(2.2.2)..." There is no previously stated requirement for keeping up with the availability of the access monitoring systems. This appears to create a requirement for logging the availability of the monitoring systems.	The criteria for levels of non-compliance have been changed to percentages of Electronic Security Perimeters.
005-C2,3		
005-C2,4		

CIP-005 Drafting Team Responses to Comments

Name	Kenneth Goldsmith	
Entity	Alliant Energy	
Ready to Ballot:	No	
General Comments		
005-R1	R1.5 should have the work"monitored" removed. Flexibility should be allowed to use a risk assessmsnt to determine the appropriate level of protection.	The intention is that cyber assets used to control and monitor access to critical cyber assets must be protected as specified. Responsible Entities retain flexibility in how they implement the requirements.
005-R2	R2.1 is weakened by including emergency operations. Consider changing to "... Responsible Entity shall enable only those ports and services that are required for operations, and monitoring of Cyber Assets..."	The "emergency" clause has been removed. Operations is inclusive of these situations.
005-R3		
005-R4		
005-R5		
005-M1		
005-M2		
005-M3		
005-M4		
005-M5		
005-C1,1		
005-C1,2		
005-C1,3		
005-C1,4		
005-C2,1		
005-C2,2		
005-C2,3		
005-C2,4		

Name	Kathleen Goodman	
Entity	ISO New England Inc	
Ready to Ballot:	No	
General Comments	We believe that CIP002 through CIP009 go beyond the scope of the original SAR for 1300. The final SAR for 1300, dated March 8, 2004, clearly states that the U/A Standard 1200 is the basis for development of a permanent standard to replace it. The intent of both U/A 1200 and SAR 1300 is to establish a minimum set of cyber security best practices as a standard baseline for general cyber protection of a reliable BES. In establishing a baseline, all care should be taken to aviod dictating particular tools, technologies and/or methodologies. Where such are referenced, those references should be removed.	The Drafting Team has modified these standards to the extent practical to remove references to specific technologies. However, where appropriate, certain accepted methodologies and security-practice specific terms are still referenced; examples are passwords, access controls and access logs.
005-R1	R1.4 & R1.6 should be removed as redundent with CIP007.	CIP-005 addresses access points to the Electronic Security Perimeter, while CIP-007 addresses requirements to assets within the Electronic Security Perimeter.
005-R2	R2.1.2Remove the words "status and...". All that is required should be the configuration. R2.2 Re-write to be "...identifying controls for each access point through the electronic perimeter." R2.2.1 What access request? R2.2.3 Change to "for securing dial-up and wireless access." R2.4 Remove second paragraph as it is not a requirement statement and does not add value.	R2 has been rewritten to add clarity and reduce prescriptiveness.
005-R3	R3.3 Remove. Why would you require a review of something every 90 days when it is already being monitored?	The requirement has been modified to require a review at least every 90 calendar days where real-time alerting has not been implemented.
005-R4	R4 should be limited to Internet-facing perimeter cyber assets. R4.3 Add in wireless. R4.4 Remove "network management community strings." We do not know of such devices and, as such, believe them to be technology-specific.	The vulnerability assessment ensures that controls for the Electronic Security Perimeter are in place and effective. It is meant to assess the controls for the Electronic Security Perimeter protecting the Critical Cyber Assets from any connected network, whether it is the Internet, the corporate business network, or third-party networks. R4.3 has been modified to refer to all access points and an FAQ has been written to provide examples. R4.4 Network management community strings are not technology

		specific. They are similar to passwords and are commonly used for access to device management and configuration functions. An example is SNMP -- please refer to A Simple Network Management Protocol (SNMP) RFC dated 1990 at http://www.ietf.org/rfc/rfc1157.txt
005-R5		
005-M1	Remove reference to anything inside the perimeter. This is addressed in CIP007.	A listing of the contents of the Electronic Security Perimeter, both Critical and non-critical, is essential to the measure of a properly configured Electronic Security Perimeter and access points.
005-M2		
005-M3	Remove (see comment on R3.3).	See response to R3.3
005-M4	Remove (see comment on R4.4).	See response to R4.4.
005-M5		
005-C1,1		
005-C1,2		
005-C1,3	It is not clear when you mean documents, records, or data. These are three distinct items and should not be referenced interchangeably. Please clarify.	The Drafting Team has revised the standards for consistency. Please see FAQs.
005-C1,4		
005-C2,1		
005-C2,2		
005-C2,3	Either compliance statement 2.3.2 is redundant (given compliance statement 2.2.3) or it appears that the Standard authors contemplate that Responsible Entities need to perform both an annual assessment of open ports and services and an annual vulnerability assessment. In otherwords, failure to perform a vulnerability assessment in the past year would result in Level 2 non-compliance, but would also result in Level 3 non-compliance. We suggest that the words in 2.3.4.1 resemble 2.2.2.	Levels of non-compliance have been rewritten.
005-C2,4		

CIP-005 Drafting Team Responses to Comments

Name	Tim Hattaway
Entity	Alabama Electric Cooperative
Ready to Ballot:	Yes
General Comments	
005-R1	
005-R2	
005-R3	
005-R4	
005-R5	
005-M1	
005-M2	
005-M3	
005-M4	
005-M5	
005-C1,1	
005-C1,2	
005-C1,3	
005-C1,4	
005-C2,1	
005-C2,2	
005-C2,3	
005-C2,4	

CIP-005 Drafting Team Responses to Comments

Name	Jerry Heeren	
Entity	MEAG Power	
Ready to Ballot:	No	
General Comments		
005-R1		
005-R2	Many network devices do not have full port control options. Does this suggest all access points should have full port control or be firewalled?	The standard requires a deny by default stance for access controls meaning that service ports at these access points must be explicitly allowed. This does imply that access points should implement controls that allow these requirements to be met. A firewall or router that can implement access lists satisfies this particular requirement.
005-R3	The phrase "where technically feasible" needs to be inserted regarding the logging of authorized access attempts. Due to technical limitations on certain router and/or other network hardware, the compliance w/ this requirement could be cost prohibitive without significant network upgrades.	R3 has been changed to refer to electronic or manual processes for logging access. If logging is technically feasible, it must be implemented using reasonable business judgment. Refer to the FAQ for a discussion of technical feasibility.
005-R4		
005-R5		
005-M1		
005-M2		
005-M3		
005-M4		
005-M5		
005-C1,1		
005-C1,2		
005-C1,3		
005-C1,4		
005-C2,1		
005-C2,2		
005-C2,3		
005-C2,4		

CIP-005 Drafting Team Responses to Comments

Name	Peter Henderson	
Entity	Independent Electricity System Operator (IESO)	
Ready to Ballot:	No	
General Comments		
005-R1	1. R1.4 is unclear when one considers requirments statements in CIP-005 that refer explicitly to Critical Cyber Assets rather than to the more generic "cyber assets". For instance, R1 requires the Responsible Entity to identify the electronic security perimeter around its "Critical Cyber Assets". On one hand, the wording of R1.4 could be taken to mean that one should replace the words "Critical Cyber Assets" by the words "Critical and Non-Critical Cyber Assets" when interpreting the standard. Under this interpretation, the Responsible Entity should identify the electronic security perimeter around non-critical cyber assets even if there are no Critical Cyber Assets within that perimeter. Alternatively, one could argue that the wording of R1 explicitly excludes non-critical cyber assets, and therefore failure to consider non-critical cyber assets is not a cause for concern. 2. Please clarify. Given R1.5 and given that this standard focuses on the definition and management of the electronic security perimeter, it is suggested that R1.4 can be deleted without any ill effect.	The requirements have been clarified to state that an Electronic Security Perimeter must be defined for Critical Cyber Assets. Requirement R1.4 qualifies that the protections defined in CIP-005 are applicable to non-critical Cyber Assets that are also within that perimeter. R1.5 qualifies that cyber assets used in the control and monitoring of the Electronic Security Perimeter must also be protected per specific requirements. R1.4 and R1.5, therefore, are relevant.
005-R2		
005-R3	1. R3.2 should be clarified by rewording it as, "The Responsible Entity shall implement a procedure to verify authorized access to the protected Critical Cyber Assets on a periodic basis as determined and documented by the Responsible Entity's risk based assessment. 2. Logs can be very large. People review reports that use logs as input. R3.3 should be changed to "At least every ninety calendar days assess access logs for unauthorized access or attempts."	R3.2 has been removed and The word "assess" has been added.to R3.3.
005-R4		
005-R5		
005-M1	Measure M1 effectively imposes a new requirement - the need to identify all non-critical cyber assets within the security perimeter. If this is a requirement is should be identified in the Requirements section of the Standard. Note that such a requirement would be redundant given R1 of CIP-007.	R1.4 requires Responsible Entities to identify non-critical cyber assets within the Electronic Security Perimeter. Requirement R1.6 defines the requirement to document critical and non-critical cyber assets within the Electronic Security Perimeter. The requirement has been removed from CIP-007.
005-M2		
005-M3		

005-M4		
005-M5		
005-C1,1		
005-C1,2		
005-C1,3		
005-C1,4		
005-C2,1	Compliance Statements 2.1.2, 2.2.2, and 2.3.4 effectively impose requirements on the availability of monitoring controls which are inconsistent with the requirements of R3.2.	Requirement R3.2 has been removed and the levels of non-compliance rewritten.
005-C2,2	Compliance Statements 2.1.2, 2.2.2, and 2.3.4 effectively impose requirements on the availability of monitoring controls which are inconsistent with the requirements of R3.2.	Requirement R3.2 has been removed and the levels of non-compliance rewritten.
005-C2,3	Compliance Statements 2.1.2, 2.2.2, and 2.3.4 effectively impose requirements on the availability of monitoring controls which are inconsistent with the requirements of R3.2.	Requirement R3.2 has been removed and the levels of non-compliance rewritten..
005-C2,4		

CIP-005 Drafting Team Responses to Comments

Name	E. Nick Henery	
Entity	SMUD	
Ready to Ballot:	Yes	
General Comments	The Drafting Team will need to go through the Standard and assign responsibility to each function from the functional model like the Version 0 STD. For this Standard to enforceable the generic use of Responsible Entity is the same as the generic use of Control Area. Even if the Standard lists the different functions it leaves open the possibility of misinterpretation as to which function is truly responsible.	The Responsible Entities are clearly enumerated in the standard Section A, item 4.
005-R1		
005-R2		
005-R3		
005-R4		
005-R5		
005-M1		
005-M2		
005-M3		
005-M4		
005-M5		
005-C1,1		
005-C1,2		
005-C1,3		
005-C1,4		
005-C2,1		
005-C2,2		
005-C2,3		
005-C2,4		

CIP-005 Drafting Team Responses to Comments

Name	Jack Hobbick
Entity	Consumers Energy
Ready to Ballot:	Yes
General Comments	
005-R1	
005-R2	
005-R3	
005-R4	
005-R5	
005-M1	
005-M2	
005-M3	
005-M4	
005-M5	
005-C1,1	
005-C1,2	
005-C1,3	
005-C1,4	
005-C2,1	
005-C2,2	
005-C2,3	
005-C2,4	

CIP-005 Drafting Team Responses to Comments

Name	Richard Kafka	
Entity	Pepco Holdings, Inc.	
Ready to Ballot:	No	
General Comments		
005-R1	1.4 this standard 005 only? 1.5 include electronic security control and monitoring in definition or cip002-R2 critical cyber? apply to individual security cameras? risk assessment?	The language has been clarified to refer to CIP-005. The risk assessment in CIP-002 identifies Critical Assets related to the Bulk Electric System. The assets described in CIP-005 R1.5 control and monitor electronic access to the Critical Cyber Assets associated with the assets identified in that risk assessment.
005-R2	Suggest rewrite as follows: R2.1. At all access points to the Electronic Security Perimeter(s), the Responsible Entity shall enable only those ports and services that are required for normal operations or for operation during emergencies, as well as those required for monitoring Cyber Assets within the Electronic Security Perimeter. R2.1.1. All other ports and services at these access points, including those used for testing purposes, shall be disabled during production usage. R2.1.2. The Responsible Entity shall document (either individually and/or by specified grouping) "due diligence" regarding secure configuration and operation of all ports and services enabled on all access points to the Electronic Security Perimeter(s). 2.1 are you opening up ports all the time that you would need for emergency 2.1.2 What is the scope of documentation and frequency? 007-R3 009-scans	R2.1 The requirement, in its current wording, gives the Responsible Entity the option of taking either one of these approaches without being non-compliant. The "emergency" clause has been removed because the term "operations" include all cases where they are necessary for operations. CIP-005 addresses access points to the Electronic Security Perimeter, while CIP-007 addresses requirements to assets within the Electronic Security Perimeter. The standard has been revised and 2.1.1 and 2.1.2 have been removed. A record of configuration could be sufficient documentation. Grouping is specifically allowed.
005-R3		
005-R4		
005-R5		
005-M1		
005-M2	The measure has been revised to refer back to the requirement.	The measure has been revised to refer back to the requirement.
005-M3		

CIP-005 Drafting Team Responses to Comments

005-M4		
005-M5		
005-C1,1		
005-C1,2		
005-C1,3		
005-C1,4		
005-C2,1	C2.1.2 -- The term "aggregate" is unclear. Does it cover all perimeters, or the aggregate for each perimeter? Why 7 days for physical perimeter (CIP006 C2.1.2) different from cyber security 6 hours? Six hours is far too short for such frequent interruptions as are caused by lightening.	The criteria for levels of non-compliance have been changed to percentages of Electronic Security Perimeters. Please see the FAQ. Reference to time has been removed.
005-C2,2		
005-C2,3	Change Level 3 Noncompliance #2.3.3 as follows with corresponding R2.1 changes above. Electronic access controls document(s) exist, but one or more "open" or enabled access ports or services have not been identified (either individually or by specified grouping), or the documents fail to identify or describe access controls for some access point (either individually or by specified grouping); or,	Level 3 has been modified for clarity.
005-C2,4		

CIP-005 Drafting Team Responses to Comments

Name	Tony Kroskey	
Entity	Brazos Electric Power Cooperative	
Ready to Ballot:	No	
General Comments		
005-R1		
005-R2		
005-R3		
005-R4		
005-R5		
005-M1		
005-M2	The wording has been amended to refer to the requirement.	The wording has been amended to refer to the requirement.
005-M3		
005-M4		
005-M5		
005-C1,1		
005-C1,2		
005-C1,3		
005-C1,4		
005-C2,1	Suggest changing the aggregate time from "more than six hours, but less than twenty-four hours" to "more than twelve hours, but less than twenty-four hours".	The criteria for levels of non-compliance have been changed to percentages of Electronic Security Perimeters. Please see the FAQ.
005-C2,2		
005-C2,3		
005-C2,4		

CIP-005 Drafting Team Responses to Comments

Name	Carol Krysevig	
Entity	Allegheny Energy Supply Co. LLC	
Ready to Ballot:	No	
General Comments	D2.1.1 and D2.2.1. - 'Document(s) exist, but have not been updated within ninety calendar days of any changes...' What documents are you talking about? There are many documented items within this section, and none of them have time periods associated with them. Need to clarify. D2.3.1 -- Clarification needed on exactly what type of 'verification' will suffice to ensure that all Critical and Non-Critical Cyber Assets are within the perimeter(s) described. D2.3.2 -- Specify exactly what documents NERC is looking for.	The documentation requirements have been clarified; R5 enumerates review and update periods. Reference to verification has been removed. Compare actual network configuration to documented perimeters and ensure that all critical cyber asset listed in CIP-002 are accounted for in these perimeters. The requirement calls for system configuration documentation identifying active ports and services. Depending on the systems, these could be firewall configuration files, system network configuration files, or other system documentation depicting the configuration of ports and services.
005-R1		
005-R2	R2.4. - The definition for 'interactive access' is better, but still needs some refinement. 'Human interaction' is too broad. For example - telnet access would be considered interactive, but ODBC access might not be considered interactive. Both, however, may require 'human interaction'.	R2 has been clarified and "human interaction" has been removed.
005-R3	The phrase 'twenty-four hours a day, seven days a week' is colloquial. Revise to state 'continuously'.	This phrase twenty-four hours a day, seven days a week is precise in defining the requirement.
005-R4		
005-R5		
005-M1	Add 'Cyber Assets deployed for access control and monitoring of the access points' after 'within the Electronic Security Perimeter(s)'.	The measures have been rewritten to refer back to the requirements.
005-M2		
005-M3		
005-M4		
005-M5		
005-C1,1		
005-C1,2		
005-C1,3		

CIP-005 Drafting Team Responses to Comments

005-C1,4

005-C2,1

005-C2,2

005-C2,3

005-C2,4

CIP-005 Drafting Team Responses to Comments

Name	John Lim	
Entity	Con Edison	
Ready to Ballot:	No	
General Comments		
005-R1		
005-R2		
005-R3	Logs can be very large. People review reports that use logs as input. R3.3 should be changed to "At least every ninety calendar days, the Responsible Entity shall assess access logs for unauthorized access or attempts." "Review" implies a manual review. "assess" can include either a manual review or other automated processes for assessing the access logs.	The word "assess" hs been added.
005-R4		
005-R5		
005-M1		
005-M2		
005-M3		
005-M4		
005-M5		
005-C1,1		
005-C1,2		
005-C1,3		
005-C1,4		
005-C2,1		
005-C2,2		
005-C2,3		
005-C2,4		

CIP-005 Drafting Team Responses to Comments

Name	Deborah Linke	
Entity	Bureau of Reclamation	
Ready to Ballot:	No	
General Comments	General comment: CIP-005 is focused on Electric Security Perimeter protections, which is certainly a key consideration. Reclamation believes that the definition in R.1.6, which requires that Responsible Entities define their Electronic Security Perimeters, is clearer than much of the preceding language and should form the central definition for the section. Reclamation is also concerned about Section R1.4 which requires that all non-critical cyber assets within the electronic security perimeter be protected to the same degree as the critical assets, which seems to be a non-value added activity.	R1.4 requires Responsible Entities to identify non-critical cyber assets within the Electronic Security Perimeter and control and monitor access to them at the access points on the perimeter. Controlling access to non-critical assets residing in the same perimeter as Critical Cyber Assets is essential because the non-critical cyber assets introduce vulnerabilities exposing the Critical Cyber Assets to threats that must be protected against.
005-R1		
005-R2	R2: The phrase "shall use an access control model that denies access by default unless explicit access permissions are specified" is applicable to perimeter protections such as firewalls and router access control lists, but may not be appropriate for all dial-up modems. For example for a single, stand-alone metering device associated with a Critical Cyber Asset, there is no risk that dial-up access will lead to any control actions or unauthorized access to other assets.	As we understand your example, unauthorized manipulation of the meter could adversely impact operation of the Critical Cyber Asset, and, therefore, such dial-up access would need to be protected.
005-R3		
005-R4		
005-R5		
005-M1		
005-M2		
005-M3		
005-M4		
005-M5		
005-C1,1		
005-C1,2		
005-C1,3		
005-C1,4		
005-C2,1		

005-C2,2

005-C2,3

005-C2,4

CIP-005 Drafting Team Responses to Comments

Name	Greg Mason	
Entity	Dynegy Generation	
Ready to Ballot:	No	
General Comments		
005-R1	R1.4 and M1 state that the non Critical Cyber Assets within the defined Electronic Security Perimeter(s) shall be subject to the requirements of this standard. This wording needs to be modified to make the requirements of the standard only applicable to "those non Critical Cyber Assets within the Electronic Security Perimeter which can be used as access points to the perimeter."	R1.4 requires Responsible Entities to identify non-critical cyber assets within the Electronic Security Perimeter and control and monitor access to them at the access points on the perimeter. Controlling access to non-critical assets residing in the same perimeter as Critical Cyber Assets is essential because the non-critical cyber assets introduce vulnerabilities exposing the Critical Cyber Assets to threats that must be protected against.
005-R2		
005-R3		
005-R4		
005-R5		
005-M1	See comment on R1 above	See response above.
005-M2		
005-M3		
005-M4		
005-M5		
005-C1,1		
005-C1,2		
005-C1,3		
005-C1,4		
005-C2,1		
005-C2,2		
005-C2,3		
005-C2,4		

CIP-005 Drafting Team Responses to Comments

Name	Paul McClay	
Entity	Tampa Electric	
Ready to Ballot:	No	
General Comments	R1.4 and R1.5 - Is it the intent of these two requirements to bring "non-critical assets in the electronic security perimeter" and "cyber assets used in control and monitoring of the electronic security perimeter" into the scope of all CIP-02 thru 009 standards or only that they meet the requirements of the CIP-005 standard? If into the scope of all the standards, shouldn't these requirements be identified in CIP-002 rather than here? If it is intended that they meet the requirements of CIP-005, then both should say "shall be subject to the requirements of CIP-005-001? We do not believe these assets should be subject to all requirements. Please be specific as to which requirements each of these types of assets are subject to.	Please see response to Linda Campbell, FRCC.
005-R1	The wording of 1.5 needs to be clarified and our hope is that the committee will consider central security organizations and not intentionally (or unintentionally) cause reorganizations or physical movement of groups in order to manage firewall consoles. R1.5 What is considered "a protection"? For instance, the physical security controls have a specific requirement to be tested and maintained. CIP-005 doesn't mention the same specific requirements for the electronic controls, monitoring, and logging. Are these "the protections" to which you refer? R1.5 Do the "same protections" mean electronic protections or electronic and physical protection? How far do you take this? Are you including workstations? - for instance, what protection does a laptop or workstation not in the electronic (nor physical) perimeter, but which has access to protected networks through a firewall to access the firewall console for log monitoring purposes, require? For centralized security departments, these workstations or laptops may also access non-protected assets to monitor their firewall consoles.	
005-R2	R2.2.3 I don't see any review checklists defined in CIP-003 or 004 -- what is "review checklists" referring to?? If truly an example, and not required, perhaps this belongs in the FAQs.	
005-R3	R3.2 The only requirement for a risk-based assessment applies to critical assets (R1.2 of CIP-002), not critical cyber assets so it is not clear what this requirement is trying to say -- did you mean the vulnerability assessment of section R4? Suggest putting a period after "on a periodic basis." R3.3 Review of Access Logs - Please clarify within the standard what access logs the standard applies to. Our interpretation would be IDS, firewall, and dial-up logs since CIP005 covers the electronic perimeter components and access points. If this is a correct interpretation, the drafting team should also consider the cost versus the benefit of such a review. Even within an internal network, a very large percentage of "unauthorized	R3.2 has been removed. R3.3 This requirement's opening paragraph clearly states the applicability to access points on the perimeter. The requirement has included an additional clause to clarify that other log assessment methods, such as automated scripts, or other technical product features which process logs, also satisfy this requirement.

	attempts" will be false positives due to the nature of TCP/IP communications and software that discovers/broadcasts to the network (i.e. printer software, active directory, etc.). We recommend elimination of this requirement or a clarification to reduce the scope of work. However, if not eliminated, depending on the size of the organization, the review of all unauthorized access attempts could be very onerous. It is unclear from this requirement what the expectations and disposition of results of a review of unauthorized access are? What's the point of the review? Please be more specific as to what the requirement is.	
005-R4	R4.2 Control Systems may not tolerate scanning as it can affect performance or bring down the system. We strongly feel the Drafting Team should reconsider this requirement to scan ports and services through the access points (i.e. a firewall). An organization that has misconfigured a firewall would run the risk of impacting stability or performance of control systems. The same information can be gathered through a detailed assessment of the rule-base or filtering on an access point to the perimeter at no risk. Since this assessment is required in R3 of CIP-007-1, this requirement should be removed.	Please see responses to Linda Campbell, FRCC.
005-R5		
005-M1		
005-M2	Please see responses to Linda Campbell, FRCC.	Please see responses to Linda Campbell, FRCC.
005-M3	M3.2 To correspond with R3.2, add to the beginning of this measure, "For those assets where monitoring controls have not been implemented, ..." M3 and M3.3 What constitutes a "business record" and how does it differ from measures in previous sections of the standards from "data", "document" or "documentation."	Please see responses to Linda Campbell, FRCC.
005-M4		
005-M5		
005-C1,1		
005-C1,2		
005-C1,3		
005-C1,4		
005-C2,1		
005-C2,2		
005-C2,3		
005-C2,4		

CIP-005 Drafting Team Responses to Comments

Name	David McCoy	
Entity	Great Plains Energy/Kansas City Power & Light	
Ready to Ballot:	No	
General Comments		
005-R1		
005-R2		
005-R3		
005-R4		
005-R5		
005-M1		
005-M2	The measures have been modified to refer back to the requirement. The requirement has been changed to allow grouping.	The measures have been modified to refer back to the requirement. The requirement has been changed to allow grouping.
005-M3		
005-M4		
005-M5		
005-C1,1		
005-C1,2		
005-C1,3		
005-C1,4		
005-C2,1	2.1.2 - More than 6 hours of interruption in monitoring capability is deemed to be non compliant. The standard should be 7 calendar days like it is for physical security. It is also unclear whether this standard applies to each individual electronic perimeter or the aggregate of all electronic security perimeters in an entity's system.	The critieria for non-compliance have been changed from duration to percentage of sites that are deficient. The timeframe has been removed.
005-C2,2		
005-C2,3		
005-C2,4		

CIP-005 Drafting Team Responses to Comments

Name	Patrick Miller	
Entity	PacifiCorp	
Ready to Ballot:	No	
General Comments		
005-R1	For R1.6, there are too many requirements in the verbiage to represent a single, stand-alone item. Please break this out into multiple standards. Additionally, there is no langauge specific to revision/review frequency requirements.	The language of the requirement has been simplified. This requirement defines a general documentation requirement for the Requirements R1.1 through 1.5.
005-R2		
005-R3	For R3.3, consider adding language that specifies NERC's position with respect to manual (human) or logical (cyber/automated) review.	An addition has been included in the requirement to account for automated log assessment methods.
005-R4		
005-R5		
005-M1		
005-M2		
005-M3		
005-M4		
005-M5		
005-C1,1		
005-C1,2		
005-C1,3		
005-C1,4		
005-C2,1		
005-C2,2		
005-C2,3		
005-C2,4		

CIP-005 Drafting Team Responses to Comments

Name	Don Miller
Entity	First Energy Corp
Ready to Ballot:	Yes
General Comments	
005-R1	
005-R2	
005-R3	
005-R4	
005-R5	
005-M1	
005-M2	
005-M3	
005-M4	
005-M5	
005-C1,1	
005-C1,2	
005-C1,3	
005-C1,4	
005-C2,1	
005-C2,2	
005-C2,3	
005-C2,4	

CIP-005 Drafting Team Responses to Comments

Name	Jeff Mitchell
Entity	ECAR
Ready to Ballot:	Yes
General Comments	N/A
005-R1	
005-R2	
005-R3	
005-R4	
005-R5	
005-M1	
005-M2	
005-M3	
005-M4	
005-M5	
005-C1,1	
005-C1,2	
005-C1,3	
005-C1,4	
005-C2,1	
005-C2,2	
005-C2,3	
005-C2,4	

CIP-005 Drafting Team Responses to Comments

Name	Scott Mix	
Entity	KEMA, Inc	
Ready to Ballot:	No	
General Comments	Since the standards have been split up into multiple standards, the titles should be made clearer so that they stand on their own. Therefore, I am resubmitting the request to change the title of this standard to "Electronic Security of Critical Cyber Assets".	The title of the standard has been amended to specifically refer to Electronic Security Perimeters.
005-R1	The requirement to document the non-Critical Cyber Assets within the Electronic Security Perimeter is duplicated in CIP-007 Requirement R1. It should only be in one location (probably CIP-007).	The requirement has been removed from CIP-007.
005-R2	Should there be a minimum periodicity requirement (i.e., annually) for the authorization rights review?	Documentation and procedure/process review requirements are defined in R5.
005-R3	In order to provide consistence with CIP-006 R6, replace Requirement R3.3 with the following: "The responsible entity shall retain electronic access logs for at least 90 days, unless required as part of a Cyber Security Incident report as required in CIP-008 R2. The logs shall be reviewed for unauthorized access or attempts every 2 months. Is a 2-month review cycle sufficient to detect and investigate an intrusion?	The documentation retention requirements defined in R5 have been redefined in R5 and made consistent with other standards. In addition, R3.3 defines a period of at least 90 days at a minimum for the review.
005-R4		
005-R5		
005-M1		
005-M2		
005-M3		
005-M4		
005-M5		
005-C1,1		
005-C1,2		
005-C1,3		
005-C1,4		
005-C2,1		
005-C2,2		

005-C2,3

005-C2,4

CIP-005 Drafting Team Responses to Comments

Name	Darrick Moe	
Entity	WAPA	
Ready to Ballot:	No	
General Comments		
005-R1		
005-R2		
005-R3	In R3.2, the word "partially" should be changed or rephrased to something more measurable.	Partially means that some, but not all, monitoring control requirements have been implemented.
005-R4		
005-R5		
005-M1		
005-M2		
005-M3		
005-M4		
005-M5		
005-C1,1		
005-C1,2		
005-C1,3		
005-C1,4		
005-C2,1		
005-C2,2		
005-C2,3		
005-C2,4		

CIP-005 Drafting Team Responses to Comments

Name	Selby Mohr
Entity	Sacramento Municipal Utility District
Ready to Ballot:	Yes
General Comments	
005-R1	
005-R2	
005-R3	
005-R4	
005-R5	
005-M1	
005-M2	
005-M3	
005-M4	
005-M5	
005-C1,1	
005-C1,2	
005-C1,3	
005-C1,4	
005-C2,1	
005-C2,2	
005-C2,3	
005-C2,4	

CIP-005 Drafting Team Responses to Comments

Name	Kurt Muehlbauer	
Entity	Exelon	
Ready to Ballot:	No	
General Comments	The documentation and processes around the responsible entity s tasks are too prescriptive. The industry needs to be extremely careful to avoid the creation of purely documentation-based non-compliances. With increasing legal requirements for compliance, and the associated penalties for noncompliance, noncompliance should be reserved for real security issues. It is simply too easy to make a mistake in documentation in light of the constantly evolving cyber environment. Each entity should develop its own processes in support of the requirements, and these processes should be required to contain provisions for periodic review and approval applicable to each requirement. The processes should also be required to produce reasonable documentation to demonstrate compliance. However, it is not necessary to specify the details of the documentation or review periods. The above approach can be met by removing references to documentation from the requirements section. Then, in the measures section require each entity to reasonably document programs and processes that support the security requirements and to produce reasonable documentation required to demonstrate compliance to the security requirements. Please refer to our overall comments on defining reasonable. If the above approach is taken, it will be possible to delete many of the sub-bullet points under each requirement (because the details will be specified by each entity in their program or process, as applicable). This will also ensure that documentation and excessive low-value administrative tasks are removed from the requirements.	The Drafting Team has reviewed the standards and removed prescription where possible. The prescriptiveness that remains is necessary to provide the clarity requested by a majority of commenters. The documentation required by these standards allow Responsible Entities to demonstrate that the policies, processes, and procedures that they have implemented consistently comply with the requirements of these standards.
005-R1	We do not agree with having to maintain complete documentation on non-critical cyber assts or making all of the requirements in this standard applicable to non-critical assets. Each entity should be responsible for securing other assets so as not to compromise any of the critical cyber assets. A select set of requirements, such as virus updates and patch management, would be applicable to non-critical assets. R1.5 -- Per above, non-critical assets should not be included. Delete this. R1.6 -- Per above, non-critical assets should not be included. Delete this. R1.6 -- Depicting every asset with the perimeter on the Electronic Security perimeter diagram, and keeping it up to date, requires excessive cost and is of questionable value. An electronic list or table should be the primary method to keep track of assets and where they are located. Recommend rewording: R1.6.--The Responsible Entity shall maintain documents depicting the Electronic Security	This standard seeks to ensure that adequate controls are in place to protect the electronic security perimeter in which Critical Cyber Assets reside. If non-critical cyber assets reside within the same perimeter, then these devices must be subject to the same controls at the access points. Weaker controls for non-critical cyber assets introduce vulnerabilities that could threaten Critical Cyber Assets within the perimeter. A good approach would be to set the perimeter as close to the Critical Cyber Assets as possible and to minimize the number of non-critical cyber assets that are within the perimeter. This increases the security posture of the perimeter around the Critical Cyber Assets. The required documentation matches the protection activities that are required.

	Perimeter(s) and all electronic access points to the security perimeter(s). The entity shall ensure that all Critical Cyber Assets have been identified and are within the documented Electronic Security Perimeter(s).	
005-R2	R2.1 - Why is this requirement separate from CIP-007 R3? Drawing a distinction between being on or within the perimeter is arbitrary for this requirement. Would these requirements ever be executed or audited separately, in the real world? Recommend thinking through this and potentially consolidating the requirements. Delete R2.1.1 -- The statement is implied in R2.1 and is too prescriptive. Please also see the general comments to this standard. Delete R2.1.2 -- It is too prescriptive and documentation focused. Consider a network consisting of 1000 nodes. With 64,000 possible ports per node, you then have 64,000,000 data points. And this is even before you add services. Creating configuration documentation that is always representative of the network does not seem feasible. Recommend replacing this requirement with a general measure that requires reasonable documentation that access points to the electronic perimeter have been secured. R2.2 appears to duplicate CIP-003 R5. Could the two requirements be consolidated, or further clarified to explain their different focus?	There is a very distinct difference between ports at the access points and ports on a system. Ports and services at access points should be enabled only for those necessary for servicing requirements that systems within the perimeter have to access resources or applications outside the perimeter, or that originate from outside the perimeter into the perimeter. Ports and services on a system within a perimeter include those necessary to also service those applications and resources within the perimeter as well. R2 has been reworded and the sub-requirements removed. R2 allows documentation by grouping and is intended for enabled ports only. CIP-003, R5 requires access controls for information pertaining to Critical Cyber Assets. CIP-005, R2 requires accress controls pertaining to the Electronic Security Perimeter.
005-R3	R3 - This requirement should not apply to all assets on the perimeter. Each company/organization should have the leeway to define which assets should be monitored, and what type of monitoring is required. The combination of host and network, perimeter and internal monitoring is best implemented by each company/organization, based on their own assessment of risk and network topology. R3 - Why is this requirement separated from CIP-007 R7? Drawing a distinction between being on or within the perimeter is arbitrary for this requirement. Would these requirements ever be executed or audited separately, in the real world? Recommend thinking through this and potentially consolidating the requirements. Delete R3.3. Please see the general comments to this standard for our rationale. In place of this statement, we recommend adding a general measure in the measures section to the affect, Each entity shall have processes for monitoring electronic access, which shall include provisions for periodic reviews and approvals.	This standard seeks to define minimum requirements to monitor access points to the Electronic Security Perimeter. These requirements must be specific enough to allow compliance auditing. The standards drafting team has attempted to provide adequate room for Responsible Entities to implement measures to satisfy requirements in a manner that is appropriate to their environment. Controls for access points to the perimeter are distinct and different from monitoring controls on systems within the Electronic Security Perimeter. The DT believes a minimum is necessary. Ninety days was selected because it reflects a compromise between commenters who suggested a short period of time between reviews and commenters who believe a longer period is warranted.
005-R4	R4 - Why is this requirement separated from CIP-007 R9? Drawing a distinction between being on or within the perimeter is arbitrary for this requirement. Would these requirements ever be executed or audited separately, in the real world? Recommend thinking through this and potentially consolidating the requirements. Requiring annual vulnerability assessments is a costly way to implement the security benefits of this requirement. Full vulnerability scans are highly intrusive to any network, especially real time control systems. A more cost effective way to achieve the same result would be to provide more flexibility in how often full scans are done (e.g. at least every 5	Vulnerability assessments for Electronic Security Perimeters have different requirements distinct from assessments of host systems. These requirements must be specific enough to allow compliance auditing. The standards drafting team has attempted to provide adequate room for Responsible Entities to implement measures to satisfy requirements in a manner that is appropriate to their environment, while defining minimum requirements to provide

	years), but making sure security test procedures adequately assess vulnerabilities of any incremental changes, as part of the security testing and change management process. Simply require frequency of review according to the entity s own risk assessment, policies and procedures.	adequate protection. The requirements have been revised to include, among other requirements, a review and verification for ports, not necessarily a port scan. Regular vulnerability assessments are essential elements of any security program.
005-R5		
005-M1	Refer to general, overall comments submitted on CIP-002 through CIP-009 regarding revision of the measures and compliance specification.	Refer to responses above.
005-M2	Refer to responses above.	Refer to responses above.
005-M3	Refer to general, overall comments submitted on CIP-002 through CIP-009 regarding revision of the measures and compliance specification.	Refer to responses above.
005-M4	Refer to general, overall comments submitted on CIP-002 through CIP-009 regarding revision of the measures and compliance specification.	Refer to responses above.
005-M5	Refer to general, overall comments submitted on CIP-002 through CIP-009 regarding revision of the measures and compliance specification.	Refer to responses above.
005-C1,1	Refer to general, overall comments submitted on CIP-002 through CIP-009 regarding revision of the measures and compliance specification.	Refer to responses above.
005-C1,2	Refer to general, overall comments submitted on CIP-002 through CIP-009 regarding revision of the measures and compliance specification.	Refer to responses above.
005-C1,3	Refer to general, overall comments submitted on CIP-002 through CIP-009 regarding revision of the measures and compliance specification.	Refer to responses above.
005-C1,4	Refer to general, overall comments submitted on CIP-002 through CIP-009 regarding revision of the measures and compliance specification.	Refer to responses above.
005-C2,1	Refer to general, overall comments submitted on CIP-002 through CIP-009 regarding revision of the measures and compliance specification.	Refer to responses above.
005-C2,2	Refer to general, overall comments submitted on CIP-002 through CIP-009 regarding revision of the measures and compliance specification.	Refer to responses above.
005-C2,3	Refer to general, overall comments submitted on CIP-002 through CIP-009 regarding revision of the measures and compliance specification.	Refer to responses above.
005-C2,4	Refer to general, overall comments submitted on CIP-002 through CIP-009 regarding revision of the measures and compliance specification.	Refer to responses above.

CIP-005 Drafting Team Responses to Comments

Name	Jeffrey Mueller	
Entity	PSEG Companies	
Ready to Ballot:	No	
General Comments	The PSEG Companies have reviewed and share the concerns expressed in the Comments of PJM and EEI. Accordingly, the PSEG Companies support the comments of PJM and EEI, and request that the concerns expressed in those comments be properly addressed in the next version of the draft standard.	See responses to EEI and PJM.
005-R1		
005-R2		
005-R3		
005-R4		
005-R5		
005-M1		
005-M2		
005-M3		
005-M4		
005-M5		
005-C1,1		
005-C1,2		
005-C1,3		
005-C1,4		
005-C2,1		
005-C2,2		
005-C2,3		
005-C2,4		

CIP-005 Drafting Team Responses to Comments

Name	Mitchell Needham	
Entity	Tennessee Valley Authority	
Ready to Ballot:	No	
General Comments		
005-R1		
005-R2		
005-R3	The phrase "where technically feasible" should pertain to all parts of R3. Additionally, some other realistic options should be considered such as 1) making a device read-only such that no remote control or software changes can be made, and 2) making a device phone-home or dial-back to improve security.	The requirement has been changed to address electronic or manual processes for monitoring and logging access. The Responsible Entity has the flexibility to determine how to meet the requirement .
005-R4		
005-R5		
005-M1		
005-M2		
005-M3		
005-M4		
005-M5		
005-C1,1		
005-C1,2		
005-C1,3		
005-C1,4		
005-C2,1	2.1.2 is unrealistic from an accounting standpoint. Some entities might have very few devices to monitor while others might have literally thousands. Some type of normalization might be in order.	The criteria for non-compliance have been changed to the percentage of sites that are deficient. Please see the FAQ.
005-C2,2		
005-C2,3		
005-C2,4		

CIP-005 Drafting Team Responses to Comments

Name	Dave Norton	
Entity	Entergy Transmission	
Ready to Ballot:	No	
General Comments		
005-R1		
005-R2		
005-R3	R3: Re "Monitoring Electronic Access Control"... Shouldn't this either be made plural, i.e., Controls, or, the word Control itself be deleted?	The word "Control" has been removed from the header.
005-R4		
005-R5		
005-M1		
005-M2		
005-M3		
005-M4		
005-M5		
005-C1,1		
005-C1,2		
005-C1,3		
005-C1,4		
005-C2,1		
005-C2,2		
005-C2,3		
005-C2,4		

CIP-005 Drafting Team Responses to Comments

Name	Doug Orlofske
Entity	Wisconsin Public Power Inc
Ready to Ballot:	Yes
General Comments	
005-R1	
005-R2	
005-R3	
005-R4	
005-R5	
005-M1	
005-M2	
005-M3	
005-M4	
005-M5	
005-C1,1	
005-C1,2	
005-C1,3	
005-C1,4	
005-C2,1	
005-C2,2	
005-C2,3	
005-C2,4	

CIP-005 Drafting Team Responses to Comments

Name	Kevin Perry	
Entity	Southwest Power Pool	
Ready to Ballot:	No	
General Comments		
005-R1	While R.1.3 properly does not extend the electronic security perimeter beyond the local site, consideration needs to be made to protecting information transmitted over the communication links connecting two discrete electronic perimeters, including LAN and WAN connections. Technology to do so is readily available.	Communication between discrete electronic perimeters is beyond the scope of this standard, as defined in the Standard Authorization Request (SAR). The SAR reflects industry consensus on the scope of the standard to be developed. The drafting team must respect that scope and not extend it during standards development.
005-R2	R2.2: Does this requirement apply to direct access to the access control point system, or does it apply to any network traffic that is permitted though the access control point? Does R2.4 apply only to the actual electronic access control point device, such as a router or firewall, or does it apply to systems within the electronic perimeter? If the latter is the case, R2.4 is potentially unreasonable. Depending upon the classification of systems as CCA, it is entirely possible that an Internet-accessible CCA, such as a controlled access web or FTP server, may be colocated in the DMZ with a general access web or FTP server. The presence of the CCA defines the DMZ as being within the electronic perimeter. The requirement to extend the same protections (and thus strong authentication) to all non-CCA systems within the electronic perimeter would render the general access systems unusable or would require the entity to host discrete "secure" and "non-secure" Internet connections or take other steps to segregate the two classes of systems. The same would be true for any similar colocation of systems connected to WAN access points. It is more appropriate to require a multi-layer, defense in depth strategy that has succeedingly stronger electronic access controls as the data transits into the network layers.	This applies to traffic which is allowed through the access control point. Normal system level controls apply to the access control devices themselves.This requirement applies to access at the access points, not at the target host systems. Access to the host systems themselves is defined in CIP-007.
005-R3	Does R3 apply only to the actual electronic access control point device, such as a router or firewall, or does it apply to systems within the electronic perimeter? If the latter is the case, R3 is potentially unreasonable for the same reasons as R2.4 above. No provisions are made for publicly accessible non-CCA systems that happen to be within the electronic security perimeter. The important logging is the unauthorized access attempts (intrusions). It is not necessary to log authorized access attempts to every system within the electronic security perimeter. R3.3: The requirement to review unauthorized electronic access attempts every 90 days is not effective in detecting and deflecting a cyber attack. Unauthorized access attempts should be continually monitored, evaluated, and responded to as necessary to protect the CCA. The term "at least 90 days" relieves entities of the need to actively monitor for attacks as entities would remain compliant as long as they reviewed their logs quarterly.	R3 applies to access control devices on the perimeter. Critical Cyber Assets within the perimeter are addressed in CIP007. Reference to monitoring and logging authorized access has been removed. Ninety days was selected because it reflects a compromise between commenters who suggested a short period of time between reviews and those who believe a longer period is warranted.

005-R4	R4.2: This requirement may be impossible to comply with. While it is relatively easy to scan an Internet access point, it is extremely difficult to scan a WAN access point, such as the NERCNET connection. The requirement to lock down and confirm by scanning an electronic access point may not be effective. Access points, especially Internet access points, are generally configured to permit a wide variety of traffic, all of it legitimate to one end system or another. However, permitting port 80 traffic to pass unconditionally, while valid for any exposed web servers, also exposes the rest of the network to the same traffic. For scanning to be effective, it needs to be verified that the end system is not reachable except via the necessary IP addresses, ports, and services. And, in undertaking such a network scan, great care must be taken to not fail any operational systems. There are already documented instances where ICCP nodes have been failed as a result of a simple NESSUS scan.	The requirement has been amended to require an review and verification, not necessarily a port scan.
005-R5		
005-M1		
005-M2		
005-M3		
005-M4		
005-M5		
005-C1,1		
005-C1,2		
005-C1,3		
005-C1,4	Approval of exceptions to the requirements should not be delegated	Exceptions cannot be taken to NERC standards. It is up to Responsible Entities to define policies, exception handling, and delegation authority.
005-C2,1		
005-C2,2		
005-C2,3		
005-C2,4		

CIP-005 Drafting Team Responses to Comments

Name	Tom Pruitt	
Entity	Duke Power Company	
Ready to Ballot:	No	
General Comments	A.4.1 -- Given the critical role of the PSE, why are these standards not applicable to that entity? A.4.2.2 -- Appears to be inconsistent with definition of "Cyber Asset". A.5 -- This should reference the proposed Implementation Plan. Alternatively, the compliance implementation plan should be referenced in the compliance sections for all of CIP002 thru CIP 009.	The standards reflect the Standard Authorization Request (SAR), which excluded PSEs. The drafting team must respect the scope of the SAR and not extend it during standards development. The SAR reflects industry consensus on the scope of the standard to be developed. The SAR specifically excluded communication links. Although reviewed and commented upon by the industry, the Implementation Plan is not part of the standard and cannot be referenced therein.
005-R1		
005-R2	R2.4 -- External interactive access into an electronic perimeter now requires "strong procedural or technical controls" beyond "static user name and password". For folks wanting to access from outside the electronic perimeter, this means multi-factor authentication. It is the right thing to do, but this will be a very expensive and time-consuming thing to implement. R2.5 -- Appropriate Use Banner requirement is not measured.	Please refer to FAQ for discussions of strong authenticastion as well as discussions of technical feasibility and reasonable business judgment. The measures have been modified to refer back to the requirement.
005-R3	R3 -- The requirements for monitoring electronic access control implies an Intrusion Detection System (IDS) at each access point. If there are large numbers of access points, say at each generation plant, IDS costs are going to be potentially very large.	The requirement has been changed to read "electronic or manual process(es)..." An alternative is to reduce the number of perimeters that must be monitored. Remember that these apply only to Electronic Security Perimeters surrounding Critical Cyber Assets.
005-R4	R4 -- This requirement will be difficult and costly to implement and manage.	A regular vulnerability assessment is an essential element of a cyber security program.
005-R5		
005-M1		
005-M2		
005-M3		
005-M4		
005-M5		
005-C1,1		

CIP-005 Drafting Team Responses to Comments

005-C1,2

005-C1,3

005-C1,4

005-C2,1

005-C2,2

005-C2,3

005-C2,4

CIP-005 Drafting Team Responses to Comments

Name	Duane Radzwion	
Entity	Consumers Energy	
Ready to Ballot:	No	
General Comments		
005-R1	Phone companies may choose to route SCADA data, regardless of the communications protocol used by the utility, and with or without the knowledge of the utility. Ignoring this fact, and yet implementing onerous requirements on the utility EMS and RTU ends is akin to barring all the windows yet leaving the front door wide open. Protection of the communications chain, from end to end, must be consistent. If not, there is only a false sense that we've protected our systems. Before balloting, the requirements for SCADA data that could become routed by the telco or other communcations company, must be made clear and consistent.	The standards reflect the Standard Authorization Request (SAR). The drafting team must respect the scope and not extend it during standards development. The SAR reflects industry consensus on the scope of the standard to be developed. The SAR specifically excluded communication links. The SAR specifically excluded communication links.
005-R2		
005-R3		
005-R4		
005-R5		
005-M1		
005-M2		
005-M3		
005-M4		
005-M5		
005-C1,1		
005-C1,2		
005-C1,3		
005-C1,4		
005-C2,1		
005-C2,2		
005-C2,3		
005-C2,4		

CIP-005 Drafting Team Responses to Comments

Name	Howard Rulf	
Entity	We Energies	
Ready to Ballot:	No	
General Comments		
005-R1	R1.4: Non critical cyber assets within the perimeter should not be subject to the standard. By definition a non- critical cyber asset would not affect the grid. R1.5: Access control and monitoring requires more clarification and thought. As written, one could argue that this would include all access control and monitoring systems used on the network.	R1.4. CIP-005 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 protected perimeter may affect the operation of the Critical Cyber Assets within it. Please refer to the FAQs for CIP-005. R1.5 This requirement clearly states "used in the access control and monitoring of the Electronic Security Perimeter(s)."
005-R2		
005-R3		
005-R4		
005-R5		
005-M1		
005-M2		
005-M3		
005-M4		
005-M5		
005-C1,1		
005-C1,2		
005-C1,3		
005-C1,4		
005-C2,1		
005-C2,2		
005-C2,3		
005-C2,4		

CIP-005 Drafting Team Responses to Comments

Name	Randy Schimka	
Entity	San Diego Gas and Electric Co.	
Ready to Ballot:	No	
General Comments		
005-R1	We have studied this portion of the standard, and are still not quite sure about the distinction between cyber assets and critical cyber assets in R1.4 / R1.5 / R1.6 and how the standard applies to them in this section. It appears that the policy states that non-critical and critical cyber assets within the Electronic Security Perimeter should be treated the same and subject to the standard. If that's the case, why do we differentiate between non-critical and critical cyber assets? Maybe the list of critical cyber assets should include everything within the electronic security perimeter? It's getting confusing about the difference between the types of assets in this section. Some clarification would help us understand exactly what we're trying to achieve.	The requirements have been clarified to state that an Electronic Security Perimeter must be defined for Critical Cyber Assets. Requirement R1.4 qualifies that the protections defined in CIP-005 are applicable to non-critical Cyber Assets that are also within that perimeter. R1.5 qualifies that cyber assets used in the control and monitoring of the Electronic Security Perimeter must also be protected per specific requirements.
005-R2		
005-R3		
005-R4		
005-R5		
005-M1		
005-M2		
005-M3		
005-M4		
005-M5		
005-C1,1		
005-C1,2		
005-C1,3		
005-C1,4		
005-C2,1		
005-C2,2		
005-C2,3		
005-C2,4		

CIP-005 Drafting Team Responses to Comments

Name	Lyman Shaffer	
Entity	PG&E	
Ready to Ballot:	Yes	
General Comments		
005-R1	R.1.5 "Cyber assets used in access control shall be afforded the same protection as Critical Cyber assets." Please clarify the scope of this requirement. It should be reworded to coincide with the language in R1.4 i.e. refer to this standard.	The requirement has been clarified to read "afforded the protective measures specified in StandardCIP-004 Requirement R3, Standard CIP-005 Requirements R2 and R3, Standard CIP-006 Requirements R2 and R3, Standard CIP-008 and Standard CIP-009."
005-R2		
005-R3	R.3.1 "For dial up accessible Critical Cyber Assets ...monitoring controls...where technically feasible." Please clarify the meaning of technicallt feasible, "technically possible" and "technically supported" which are used in this standard. This should mean within the inherent capabilities of a cyber asset. Just because something is technically feasible does not mean that it is a prudent thing to do based on the risk and the costs of implementation.	R3.1 requires that if monitoring is technically feasible, it must be implemented using reasonable business judgment. Refer to the FAQ for a discussion of technical feasibility.
005-R4	R.4.3 "The discovery of modems". It is not clear what is meant by this vulnerablity assessment. The associated measure suggests that the purpose is to test for default accounts.	The requirement has been clarified to specify the discovery of access points to the Electronic Security Perimeter. The discovery process is aimed at finding access points that are unknown or undocumented.
005-R5		
005-M1		
005-M2		
005-M3		
005-M4		
005-M5		
005-C1,1		
005-C1,2		
005-C1,3		
005-C1,4		
005-C2,1		

CIP-005 Drafting Team Responses to Comments

005-C2,2

005-C2,3

005-C2,4

CIP-005 Drafting Team Responses to Comments

Name	Neil Shockey
Entity	Southern California Edison
Ready to Ballot:	Yes
General Comments	
005-R1	
005-R2	
005-R3	
005-R4	
005-R5	
005-M1	
005-M2	
005-M3	
005-M4	
005-M5	
005-C1,1	
005-C1,2	
005-C1,3	
005-C1,4	
005-C2,1	
005-C2,2	
005-C2,3	
005-C2,4	

CIP-005 Drafting Team Responses to Comments

Name	William Smith
Entity	Allegheny Power
Ready to Ballot:	Yes
General Comments	
005-R1	
005-R2	
005-R3	
005-R4	
005-R5	
005-M1	
005-M2	
005-M3	
005-M4	
005-M5	
005-C1,1	
005-C1,2	
005-C1,3	
005-C1,4	
005-C2,1	
005-C2,2	
005-C2,3	
005-C2,4	

CIP-005 Drafting Team Responses to Comments

Name	Paul Sorenson	
Entity	Open Access Technology International	
Ready to Ballot:	Yes	
General Comments		
005-R1	It is not entirely clear by what is stated in R1.2, Dial-up. Does this mean there is basically a security perimeter drawn around that device having a non-routable dial-up access point? It is not entirely clear in the wording of R 1.4 whether a non-critical asset within the electronic security perimeter is subject to all CIP-002 through CIP-009 standards or just this CIP-005 standard (i.e., what exactly is "this standard"). The full range of applicable standards for such devices should be made clear.	Yes. Dial-up accessible access points can be directly dialed, and therefore do not need a routable protocol to access them. The language has been modified to specify CIP-005.
005-R2		
005-R3		
005-R4		
005-R5		
005-M1		
005-M2		
005-M3		
005-M4		
005-M5		
005-C1,1		
005-C1,2		
005-C1,3		
005-C1,4		
005-C2,1		
005-C2,2		
005-C2,3		
005-C2,4		

CIP-005 Drafting Team Responses to Comments

Name	Robert Strauss	
Entity	NYSEG	
Ready to Ballot:	No	
General Comments		See responses to Ray A'Brial of Central Hudson Gas and Electric Corp.
005-R1		
005-R2	Recommend removing the second and third paragraph in R2.4. These paragraphs are too much detail, too prescriptive and border on examples.	
005-R3	Logs can be very large. People review reports that use logs as input. R3.3 should be changed to "At least every ninety calendar days assess access logs for unauthorized access or attempts."	
005-R4		
005-R5		
005-M1		
005-M2		
005-M3		
005-M4		
005-M5		
005-C1,1		
005-C1,2		
005-C1,3		
005-C1,4		
005-C2,1	Compliance Statements 2.1.2, 2.2.2, and 2.3.4 effectively impose requirements on the availability of monitoring controls which are inconsistent with the requirements of R3.2	
005-C2,2		
005-C2,3	Either Compliance statement 2.3.2 is redundant (given compliance statement 2.2.3) or it appears that the Standard authors contemplate that Responsible Entities need to perform both an annual assessment of open ports and services and an annual vulnerability assessment. In otherwords, failure to perform a vulnerability assessment in the past year would result in Level 2 non-compliance, but would also result in Level 3 non-compliance.	

We suggest that the 2.3.4.1 words should resemble 2.2.2.

005-C2,4

CIP-005 Drafting Team Responses to Comments

Name	Karl Tammar	
Entity	IRC	
Ready to Ballot:	No	
General Comments		See responses to Pete Henderson of IESO.
005-R1	1.--R1.4 is unclear when one considers requirments statements in CIP-005 that refer explicitly to Critical Cyber Assets rather than to the more generic "cyber assets". For instance, R1 requires the Responsible Entity to identify the electronic security perimeter around its "Critical Cyber Assets". On one hand, the wording of R1.4 could be taken to mean that one should replace the words "Critical Cyber Assets" by the words "Critical and Non-Critical Cyber Assets" when interpreting the standard. Under this interpretation, the Responsible Entity should identify the electronic security perimeter around non-critical cyber assets even if there are no Critical Cyber Assets within that perimeter. Alternatively, one could argue that the wording of R1 explicitly excludes non-critical cyber assets, and therefore failure to consider non-critical cyber assets is not a cause for concern. Please clarify. Given R1.5 and given that this standard focuses on the definition and management of the electronic security perimeter, it is suggested that R1.4 can be deleted without any ill effect.	
005-R2		
005-R3	2.--R3.2 should be clarified by rewording it as, "The Responsible Entity shall implement a procedure to verify authorized access to the protected Critical Cyber Assets on a periodic basis as determined and documented by the Responsible Entity's risk based assessment.	
005-R4		
005-R5		
005-M1	3.--Measure M1 effectively imposes a new requirement - the need to identify all non-critical cyber assets within the security perimeter. If this is a requirement is should be identified in the Requirements section of the Standard. Note that such a requirement would be redundant given R1 of CIP-007.	
005-M2		
005-M3		
005-M4		
005-M5		
005-C1,1		

CIP-005 Drafting Team Responses to Comments

005-C1,2	
005-C1,3	
005-C1,4	
005-C2,1	4.--Compliance Statements 2.1.2, 2.2.2, and 2.3.4 effectively impose requirements on the availability of monitoring controls which are inconsistent with the requirements of R3.2
005-C2,2	4.--Compliance Statements 2.1.2, 2.2.2, and 2.3.4 effectively impose requirements on the availability of monitoring controls which are inconsistent with the requirements of R3.2
005-C2,3	4.--Compliance Statements 2.1.2, 2.2.2, and 2.3.4 effectively impose requirements on the availability of monitoring controls which are inconsistent with the requirements of R3.2
005-C2,4	

CIP-005 Drafting Team Responses to Comments

Name	Todd Thompson	
Entity	PJM Interconnection	
Ready to Ballot:	No	
General Comments		See responses to Peter Henderson from IESO, except as specifically responded to below.
005-R1	R1.4 is unclear when one considers requirements statements in CIP-005 that refer explicitly to Critical Cyber Assets rather than to the more generic "cyber assets". For instance, R1 requires the Responsible Entity to identify the electronic security perimeter around its "Critical Cyber Assets". On one hand, the wording of R1.4 could be taken to mean that one should replace the words "Critical Cyber Assets" by the words "Critical and Non-Critical Cyber Assets" when interpreting the standard. Under this interpretation, the Responsible Entity should identify the electronic security perimeter around non-critical cyber assets even if there are no Critical Cyber Assets within that perimeter. Alternatively, one could argue that the wording of R1 explicitly excludes non-critical cyber assets, and therefore failure to consider non-critical cyber assets is not a cause for concern. Please clarify. Given R1.5 and given that this standard focuses on the definition and management of the electronic security perimeter, it is suggested that R1.4 can be deleted without any ill effect.	
005-R2	The requirement in R2.1.2 would require data to be collected for up to 64,000 ports. The wording should be changed to "The Responsible Entity shall document enabled ports and services on all access points to the Electronic Security Perimeter(s)".	The wording has been clarified.
005-R3	R3.2 should be clarified by rewording it as, "The Responsible Entity shall implement a procedure to verify authorized access to the protected Critical Cyber Assets on a periodic basis as determined and documented by the Responsible Entity's risk based assessment.	R3.2 has been removed.
005-R4		
005-R5		
005-M1	Measure M1 effectively imposes a new requirement - the need to identify all non-critical cyber assets within the security perimeter. If this is a requirement is should be identified in the Requirements section of the Standard. Note that such a requirement would be redundant given R1 of CIP-007.	
005-M2		
005-M3		
005-M4		
005-M5		

CIP-005 Drafting Team Responses to Comments

005-C1,1	
005-C1,2	
005-C1,3	
005-C1,4	
005-C2,1	Compliance Statements 2.1.2, 2.2.2, and 2.3.4 effectively impose requirements on the availability of monitoring controls which are inconsistent with the requirements of R3.2
005-C2,2	Compliance Statements 2.1.2, 2.2.2, and 2.3.4 effectively impose requirements on the availability of monitoring controls which are inconsistent with the requirements of R3.2
005-C2,3	Compliance Statements 2.1.2, 2.2.2, and 2.3.4 effectively impose requirements on the availability of monitoring controls which are inconsistent with the requirements of R3.2
005-C2,4	

CIP-005 Drafting Team Responses to Comments

Name	Steven Townsend
Entity	Consumers Energy Co.
Ready to Ballot:	Yes
General Comments	
005-R1	
005-R2	
005-R3	
005-R4	
005-R5	
005-M1	
005-M2	
005-M3	
005-M4	
005-M5	
005-C1,1	
005-C1,2	
005-C1,3	
005-C1,4	
005-C2,1	
005-C2,2	
005-C2,3	
005-C2,4	

CIP-005 Drafting Team Responses to Comments

Name	Martin Trence	
Entity	Xcel Energy - Northen States Power (NSP)	
Ready to Ballot:	No	
General Comments		
005-R1		
005-R2		
005-R3	R2.2.3 Remove the word "periodic" from this requirement. Reference is already made with this requirement to CIP - 003 and CIP 004, and should only be located in one place in the standards. Comments on timebased review have been submitted in the CIP-004 section of the standards.	R2 has been rewritten and R2.2.3 has been removed.
005-R4		
005-R5		
005-M1		
005-M2		
005-M3		
005-M4		
005-M5		
005-C1,1		
005-C1,2		
005-C1,3		
005-C1,4		
005-C2,1		
005-C2,2		
005-C2,3		
005-C2,4		

CIP-005 Drafting Team Responses to Comments

Name	Rick Vermeers
Entity	Avistacorp
Ready to Ballot:	Yes
General Comments	
005-R1	
005-R2	
005-R3	
005-R4	
005-R5	
005-M1	
005-M2	
005-M3	
005-M4	
005-M5	
005-C1,1	
005-C1,2	
005-C1,3	
005-C1,4	
005-C2,1	
005-C2,2	
005-C2,3	
005-C2,4	

CIP-005 Drafting Team Responses to Comments

Name Robert C. Webb

Entity Instrumentation, Systems and Automation Society

Ready to Ballot: No

General Comments

1. Who is ISA and Why is ISA commenting on CIP-002 through CIP-009?

These comments were developed by members of the Instrumentation, Systems and Automation Society, (ISA), SP99, "Manufacturing and Control Systems Security" committee’s leadership team. The overall committee is composed of over 200 members including many users, government representatives, academics, control systems manufactures, and engineers with expertise in automation and control systems. ISA’s SP99 is working to develop control systems security standards that provide sufficient guidance to the control systems and IT domain stakeholders to assure that security risks can be appropriately reduced without adversely affecting the intended functionality of those systems. ISA has published over 150 pages of guidance specific to the application of cyber security to control systems, in the form of two technical reports: ISA’s ANSI/ISA-TR99.00.01-2004, "Security Technologies for Manufacturing and Control Systems", and ANSI/ISA-TR99.00.02-2004, "Integrating Electronic Security into the Manufacturing and Control Systems Environment." Both highlight the unique aspects of control systems which must be considered when applying security procedures and technology to control systems. ISA’s constituency includes both fossil and nuclear power plant automation practitioners, and ISA has active standards committees in both of these areas (SP77, Fossil Power Plant Standards, and SP67, Nuclear Power Plant Standards).

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 have been working with NERC to establish a liaison process that would allow such considerations to be addressed earlier in the process. The development of that liaison process is nearly complete. However, comments are due at this time, and we believe these issues need to be addressed now, before approval of these standards, for the standards to be effective, without damaging the systems they are intended to protect. Thus members of the SP99 committee leadership team, with domain expertise in power generation and associated control systems have put together summary comments in several areas that should be addressed before issue of these standards.

2. Overview and Summary of Essential Changes

In general, we found these documents to be excellent examples of how an industry group can (and should) provide coherent and well structured guidance on cybersecurity. We commend NERC’s drafting team and review process; it has resulted in a quality set of documents that should be widely used.

At the same time, and in fact because of the expected wide application of these documents, we believe that three general areas should be addressed before approval of these documents.

Regarding comment #2a, the exclusionary language concerning generation assets has been removed with the exception of nuclear generation which is excluded by the SAR. Because distribution assets are not considered part of the Bulk Electric System, these resources remain excluded as well.

Regarding comment #2b, much of the prescriptive language on how certain security measures should be applied has been removed. For example, the requirement for port scans in CIP 005, R4.2 has been replaced by a requirement to review and verify only ports and services required for normal and emergency operations are enabled. In addition, the Drafting Team has removed most references to “how” security measures should be applied throughout the Standards unless it is required for compliance purposes.

Regarding comment #2c, language has been added to reflect the fact that some security solutions that are available today were not available when some legacy systems were designed and put into service. CIP-003, CIP- 004, CIP-005, and CIP-006 contain language addressing exceptions to their policies that may be required to deal with legacy systems and facilities where modern security solutions are not technically possible. In these cases, the Responsible Entities must identify and document the exception and describe the mitigating steps they are taking to secure the assets in lieu of the modern solution.

Regarding the comments #3, #4, and #5 related to scope, the Standard reflects the Standard Authorization Request which excluded distribution, nuclear generation, and telecommunication infrastructure. The Drafting Team cannot exceed the scope of the SAR.

A SAR reflects the industry consensus on the scope of any particular standard to be developed. Once a SAR has been approved for standards drafting, the scope cannot be changed.

The NERC Reliability Standards process would require new SARs to address these scope issues.

a)--Broader scope - to address a larger % of generation resources and key distribution resources, and avoid excessive reliance on one boundary or layer of defense from cyber attacks. While we recognize the need to prioritize and prevent excessive requirements, we believe the current scope is overly restrictive, and excludes a significant portion of generation, and thereby significant vulnerabilities, in some areas. This is addressed in our specific comments on CIP-002-1, (and also CIP-003-1 through 009-1), which follow.
b)--Additional cautions and guidance for control systems - in the form of specific requirements and references to key industry documents, to assure that the measures applied do not result in systems failures and reduced reliability instead of reduced risk. These cautions and guidance are necessary to address the special considerations needed when applying many normal security practices to control systems and control system networks -- particularly the bulk of legacy systems in operation today. Many do not have any ability to provide most of the required security features, and can be adversely affected by the application of other requirements. One good example is the requirement to do port scans (CIP 005-1, R4.2). Many legacy control networks are halted by port scans. The standard should include this caution, and suggest the use of alternatives to identify open ports on operational systems which have not been specifically designed and demonstrated to support this kind of testing without production failures. In general, more specific guidance on how to apply these requirements to the many legacy systems in use today should be provided.
c)--Mandatory additional protection for inadequate legacy systems -- The phrase "where technically feasible" is used in a number of locations throughout the document. In many of these cases, alternatives are required. However, in others, no alternatives are required. Clearly stated requirements to add protection or barriers to cyber attack ("mitigation measures"), where they cannot be configured or incorporated into existing systems, should be added. It is not acceptable, in our view, to identify unacceptable risks, and then leave them because the existing equipment cannot be appropriately hardened. Appropriate countermeasures, to reduce risks to acceptable levels, should be required in all cases.

Addressing these concerns does not mean significant revision to this set of standards, or significant delay, in our opinion. It can be done effectively with minor changes and references in the generic text and in several specific locations. We suggest some of the specifics below. We believe these considerations are important to prevent the standards from being counterproductive or missing significant vulnerabilities.

3. Scope - Distribution assets that could have cyber impacts on transmission assets are excluded. All distribution assets that could have cyber impacts on Bulk Electric system assets should be included, to meet the objectives of the Standards. This comment also applies to the identical sections of the remaining standards (CIP-003 -- CIP-009).

4. Scope - Exclusion 3.2.1 should be removed; it excludes some of the larger generators that would otherwise be included under R1.1.4, and the NRC's requirements should be coordinated with, not independent of these requirements. This comment also applies to the identical sections of the remaining standards, (Section 4.2.1 of CIP-003 -- CIP-009).

	5. Scope - Exclusion 3.2.2 should be removed; even when those communications systems are provided by others, the defined entities are still ultimately responsible for their proper operation and security. This comment also applies to the identical sections of the remaining standards, (Section 4.2.2 of CIP-003 -- CIP-009).	
005-R1		
005-R2	Additional cautions and guidance for control systems -- R2.1 Ports and services used in control system applications are not always known. Control system suppliers may not be able to provide this information as they do not know what ports and services will be utilized by the utility. Consequently, this requirement may not be feasible for many legacy SCADA systems as well as power plant and substation control systems. This requirement should have explicit cautions to test any change on fully representative non-production systems before application, and/or to provide alternative mitigation measures external to the control network per se. A "where possible" caveat is not adequate; it does not adequately highlight the dangers to operational systems, in what would seem to be a very simple activity.	The requirement in CIP-005 addresses ports and services at the access points, not on the systems themselves, although there is necessarily some correlation. Recognizing the danger of actually reaching devices at ports inside the perimeter during a port scan, the wording in R4.2 has been changed to "review" and does not explicitly require a port scan. The language allows the entity to choose any method that would verify the intended configuration of the ports at the access points. It is inappropriate to explain the dangers of port scanning in legacy systems within the standard, which should only define requirements and associated measures and compliance information. A FAQ addresses the dangers of active port scanning on legacy systems.
005-R3		
005-R4	Additional cautions and guidance for control systems -- R4. should require that personnel familiar with control system operation must be involved in the Vulnerability Assessment process. R4.2 should be changed to state that a vulnerability assessment should be performed to identify vulnerabilities in control system assets as installed in the field. Requirements for scanning should be preceded with testing on non production systems, or alternative mitigation measures should be employed. Scanning can, and has, lead to control system shutdowns. Many legacy control systems will not survive commercially available scanning tools.	See comments above.
005-R5		
005-M1		
005-M2	See comments above.	See comments above.
005-M3	Additional cautions and guidance for control systems - M3.3 may not be possoble for many legacy control system assets as they have no logging capability. Alternative should be defined and allowed.	See comments above.
005-M4	Additional cautions and guidance for control systems -- M4.1 should be revised consistent with the changes in R4. It should require a vulnerability assessment of what has been installed in the field and what policies are being used. It should provide cautions and alternatives to assessments of open ports, services, and community strings as procedures such as scanning may not be possible without putting the control systems at risk.	See comments above.
005-M5		

005-C1,1		
005-C1,2		
005-C1,3		
005-C1,4		
005-C2,1		
005-C2,2		
005-C2,3	Additional cautions and guidance for control systems - 2.3.2 This may not be possible for control systems; allowances should be made in this and other areas as appropriate.	See comments above.
005-C2,4		

CIP-005 Drafting Team Responses to Comments

Name	Laurent Webber	
Entity	Western Area Power Administration	
Ready to Ballot:	No	
General Comments	CIP-005 is focused on the perimeter protections, but a great deal of time is devoted to identifying the Electronic Security Perimeter, access points, and exceptions. It should be adequate that Responsible Entities define their Electronic Security Perimeters without all the confusing "clarifications" under R1.	The "clarifications" under R1 further qualify what is included in the perimeter as well as what the perimeter can be. Many of these result from requests for more guidance from previous draft versions.
005-R1		
005-R2	R2: The phrase "shall use an access control model that denies access by default unless explicit access permissions are specified" is applicable to perimeter protections such as firewalls and router access control lists, but it is very costly to implement for dial-up modems. For a single, stand-alone metering device associated with a Critical Asset there is no risk that dial-up access will lead to any control actions or unauthorized access to other assets. This is a good example of cascading, unintentional, consequences of the proscriptive nature of the CIPs. This costly, unnecessarily proscriptive regulation is simply because you won't trust the Responsible Entities to evaluate their risks and take actions to mitigate those risks in a reasonable manner. R2.1.2: What do you mean by the term "status" as different from "configuration"? If these are not entirely separate concepts, remove the word "status".	Responsible Entities must ensure that when defining Electronic Security Perimeters, they are doing so for Critical Cyber Assets. As we understand your example, unauthorized manipulation of the meter could adversely impact operation of the Critical Cyber Asset, and, therefore, such dial-up access would need to be protected. To implement a deny by default posture, the Responsible Entity must ensure the authenticity of the calling party is established before allowing the connection. 2.1.2 has been removed.
005-R3		
005-R4		
005-R5		
005-M1		
005-M2	The measure has been changed to refer back to the requirement.	The measure has been changed to refer back to the requirement.
005-M3		
005-M4		
005-M5		
005-C1,1		
005-C1,2		
005-C1,3		

005-C1,4

005-C2,1

005-C2,2

005-C2,3

005-C2,4

CIP-005 Drafting Team Responses to Comments

Name	Michal Zeithammel	
Entity	Brascan Power	
Ready to Ballot:	No	
General Comments	CIP-005-1 (Electronic Security), CIP-006-1 (Physical Security), and the related FAQs imply that: a. critical cyber assets and all the other cyber assets on the same tcp/ip network segments (i.e., within an electronic security perimeter) must fully be located within one 6-wall physical security perimeter; and b. when two such tcp/ip network segments in two different cities (in their respective electronic and physical security perimeters) connect (e.g., tcp/ip over telco-supplied frame relay) at both ends must be a device that controls and monitors access (e.g., firewall). Adding pairs of firewalls on SCADA networks means: a. more capital, maintenance, and operations costs, and b. unpredictable / undesirable effects on SCADA / control communications. Brascan Power recommends that the requirement be relaxed to not require the pair of firewalls when the circuit is: a. point-to-point leased circuit (e.g., T1 or partial T1) or frame relay circuit from reputable telco or cable company, and, especially b. fiber optic cable owned and operated by the Responsible Entity If it is in fact NERC's intent, Brascan Power recommends that the wording be clarified to specifically say that all critical cyber assets and all the other cyber assets on the same routable network segment (i.e., within an electronic security perimeter) must fully be located within one 6-wall physical security perimeter.	Your understanding of the requirements is correct. The Responsible Entity is not prohibited from defining one Electronic Security Perimeter around two geographically dispersed segments connected through communication lines. The Responsible Entity must be cognizant that, by doing so, it may be including additional Cyber Assets that must comply with CIP-005. Therefore, it is more effective in most cases to define two separate electronic security perimeters with well defined access points. Furthermore, the standard does not specifically require hardware firewalls. The Responsible Entity has the flexibility to determine how to meet the requirements of the standard.
005-R1		
005-R2		
005-R3		
005-R4		
005-R5		
005-M1		
005-M2		
005-M3		
005-M4		

CIP-005 Drafting Team Responses to Comments

005-M5

005-C1,1

005-C1,2

005-C1,3

005-C1,4

005-C2,1

005-C2,2

005-C2,3

005-C2,4

CIP-005 Drafting Team Responses to Comments

Name	Guy Zito	
Entity	NPCC	
Ready to Ballot:	No	
General Comments		See the responses to Ray A'Brial of Central Hudson Gas and Electric Corp.
005-R1		
005-R2	Recommend removing the second and third paragraph in R2.4. These paragraphs are too much detail, too prescriptive and border on examples.	
005-R3	Logs can be very large. People review reports that use logs as input. R3.3 should be changed to "At least every ninety calendar days assess access logs for unauthorized access or attempts."	
005-R4		
005-R5		
005-M1		
005-M2		
005-M3		
005-M4		
005-M5		
005-C1,1		
005-C1,2		
005-C1,3		
005-C1,4		
005-C2,1	Compliance Statements 2.1.2, 2.2.2, and 2.3.4 effectively impose requirements on the availability of monitoring controls which are inconsistent with the requirements of R3.2	
005-C2,2		
005-C2,3	Either Compliance statement 2.3.2 is redundant (given compliance statement 2.2.3) or it appears that the Standard authors contemplate that Responsible Entities need to perform both an annual assessment of open ports and services and an annual vulnerability assessment. In otherwords, failure to perform a vulnerability assessment in the past year would result in Level 2 non-compliance, but would also result in Level 3 non-compliance.	

We suggest that the 2.3.4.1 words should resemble 2.2.2.

005-C2,4

CIP-006 Drafting Team Responses to Comments

Commentor	Raymond A'Brial
Entity Name	Central Hudson Gas & Electric Corp
Ready to Ballot:	No

General Comments

006-R1	Recommend that any device inside any electronic perimeter should also be inside at least one physical perimeter Requirement R1.4 is too prescriptive. R3 covers several possible access devices.	By definition, the Physical Security Perimeter houses all Critical Cyber Assets. R1.1 has been modified to address processes to identify and document that all Cyber Assets within the Electronic Security Perimeter also reside within an identified Physical Security Perimeter. R1.4 has been modified to include all access controls in R3.
006-R2		
006-R3	R3 should read, "the Responsible Entity shall document and implement ....". Otherwise, M 3 establishes a new requirement not identified in the Requirements section of the Standard.	This modification has been made and is now R2.
	R3.1 - R3.4 are too prescriptive. They should be removed.	The requirement has been modified to allow for other equivalent devices.
	R3 changes to "Physical Access Controls - The Responsible Entity shall document and implement the organizational, operational and procedural controls to manage physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day , seven days a week."	R3 has been changed as suggested.
006-R4	R4 should read, "the Responsible Entity shall document and implement ....". Otherwise, M 4 establishes a new requirement not identified in the Requirements section of the Standard.	R4 has been reworded.
	R4 should read "Monitoring Physical Access - The Responsible Entity shall document and implement the organizational, technical and procedural controls for monitoring physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day , seven days a week." R4.1 - R4.3 are too prescriptive. They should be removed.	Modifications to the subrequirements have been made to provide greater latitude regarding methods of monitoring as long as either human notification or observation is in place.
006-R5	R5 should read, "the Responsible Entity shall document and implement ....". Otherwise, M5 establishes a new requirement not identified in the Requirements section of the Standard.	This modification has been made.
	R5.1 - R5.3 are too prescriptive. They should be removed.	R5 has been modified to allow for other equivalent logging methods.
	R5 should read "Logging Physical Access - The Responsible Entity shall document and implement the organizational, technical and procedural mechanisms for logging and reviewing physical access at all access points to the Physical Security Perimeter(s). Methods shall record sufficient information to uniquely identify individuals and datetime stamps."	This change has been made.

CIP-006 Drafting Team Responses to Comments

006-R6	We recommend changing from "at least 90 calendar days" to "at least 30 calendar days". The log should be reviewed before it is dropped. Also, retaining video can be very be expensive with little benefit.	The drafting team received many comments on the length of time for retention of access logs. Some commenters believed 30 days was sufficient, some said 90 days was too short. When considering
006-R7		
006-M1		
006-M2		
006-M3		
006-M4		
006-M5		
006-M6		
006-M7		
006-C1,1		
006-C1,2		
006-C1,3	To remain consistent with R6, this "ninety days" should change to "30 days".	To remain consistent with the requirement, the level of non-compliance remains at "ninety". Please refer to response to comments on R6.
006-C1,4		
006-C2,1		
006-C2,2		
006-C2,3	In Compliance statement 2.3.1, please clarify what is meant by "record". If the reference is really to a "document", then Compliance statement 2.3.1 appears to contradict Compliance statement 2.4.3 in cases where one of the missing documents is the security plan. Note also that no non-compliance level has been defined for cases where one required document (or record) is missing unless that document is the security plan.	The levels of noncompliance have been rewritten and reference to record has been removed.
006-C2,4		

CIP-006 Drafting Team Responses to Comments

Commentor	Ori Artman
Entity Name	Teltone
Ready to Ballot:	Yes
General Comments	
006-R1	
006-R2	
006-R3	
006-R4	
006-R5	
006-R6	
006-R7	
006-M1	
006-M2	
006-M3	
006-M4	
006-M5	
006-M6	
006-M7	
006-C1,1	
006-C1,2	
006-C1,3	
006-C1,4	
006-C2,1	
006-C2,2	
006-C2,3	
006-C2,4	

CIP-006 Drafting Team Responses to Comments

Commentor	Steve Badgett
Entity Name	Riverside Public Utilitities
Ready to Ballot:	Yes
General Comments	
006-R1	
006-R2	
006-R3	
006-R4	
006-R5	
006-R6	
006-R7	
006-M1	
006-M2	
006-M3	
006-M4	
006-M5	
006-M6	
006-M7	
006-C1,1	
006-C1,2	
006-C1,3	
006-C1,4	
006-C2,1	
006-C2,2	
006-C2,3	
006-C2,4	

CIP-006 Drafting Team Responses to Comments

Commentor	Terry Baker
Entity Name	Platte River Power Authority
Ready to Ballot:	Yes
General Comments	
006-R1	
006-R2	
006-R3	
006-R4	
006-R5	
006-R6	
006-R7	
006-M1	
006-M2	
006-M3	
006-M4	
006-M5	
006-M6	
006-M7	
006-C1,1	
006-C1,2	
006-C1,3	
006-C1,4	
006-C2,1	
006-C2,2	
006-C2,3	
006-C2,4	

CIP-006 Drafting Team Responses to Comments

Commentor	Terry Bilke
Entity Name	Midwest ISO
Ready to Ballot:	No
General Comments	
006-R1	
006-R2	
006-R3	
006-R4	
006-R5	
006-R6	
006-R7	
006-M1	
006-M2	
006-M3	
006-M4	
006-M5	
006-M6	
006-M7	
006-C1,1	
006-C1,2	
006-C1,3	
006-C1,4	
006-C2,1	
006-C2,2	
006-C2,3	
006-C2,4	

CIP-006 Drafting Team Responses to Comments

Commentor	Pat Bourassa	
Entity Name	Wisconsin Public Service Corporation	
Ready to Ballot:	No	
General Comments	If the network for the bulk electric system is isolated from the corporate network, via a firewall, do telecommunication rooms need to be part of the physical security perimeter?	If the telecommunications rooms contain critical cyber assets, or assets that are within the electronic security perimeter, then they must be a part of the physical security perimeter.
006-R1		
006-R2		
006-R3		
006-R4		
006-R5		
006-R6	Unauthorized access should be reviewed every 2 months. This will not prevent any unauthorized access. After the fact monitoring provides little to no value. Real time notification of issues would be preventitive.	Wording on the timeliness of review of unauthorized access attempts has been modified, and moved into R4.
006-R7		
006-M1		
006-M2		
006-M3		
006-M4		
006-M5		
006-M6		
006-M7		
006-C1,1		
006-C1,2		
006-C1,3		
006-C1,4		
006-C2,1		

006-C2,2

006-C2,3

006-C2,4

Commentor	Laurence W. Brown	
Entity Name	Edison Electric Institute	
Ready to Ballot:	No	
General Comments		
006-R1	R1.1 -- The phrase "shall deploy measures" should be modified to read "shall deploy reasonable measures" to permit necessary flexibility. SEE suggested additional Definition; SEE ALSO the below comment to FAQ No. 14 for this Standard. R1.4 appears to be worded awkwardly with the possible implication that losing cards, and inappropriate uses such as piggy-backing and card-sharing, can have procedures for permitting them. Suggested Alternative Wording: "R1.4. Procedures for the >appropriate< use of access cards, including >response to< card loss, >for issuing, handling, and recovering< visitor passes, and >regarding the prohibition of< inappropriate uses>< such as piggybacking and card sharing."	The standard as worded provides Responsible Entities the latitude to use their judgment in the selection and deployment of appropriate measures for their facilities. The term reasonable within this context does not provide any further clarification. R1.4 has been changed.
006-R2	Consistent with several comments above, the phrase "any modification to any component" is exceedingly overbroad, and uses the undefined term "any component." Also consistent with those comments the phrase should be modified to permit reasonable application and to use terms defined or similar to those used in other Standards. Suggested Alternative Wording: The phrase should read "any reasonably critical modification of a covered asset" — where "covered asset" should indicate both Critical and Critical Cyber Assets, as well as the non-critical cyber assets that may be covered under the criteria of certain Standards.	The wording within this requirement has been changed to add clarity. Additionally, the requirement has been moved under R1.
006-R3	R3.2 -- The phrase "may include" does not clearly enough indicate that the following three cited technologies are a non-exclusive list of examples.	Change has been made to allow for equivalent technology.
006-R4		
006-R5		
006-R6		
006-R7		
006-M1		
006-M2		
006-M3		
006-M4		

006-M5		
006-M6		
006-M7		
006-C1,1		
006-C1,2		
006-C1,3		
006-C1,4		
006-C2,1	C2.1.2 -- The term "aggregate" is unclear. Does it cover all perimeters, or the aggregate for each perimeter? Also, the seven-day criterion is not consistent with the six-hour criterion for Electronic Security Perimeters specified in CIP-005-C2.1.2. Seven days is the more reasonable period, particularly considering frequent, short interruptions such as are caused by lightening.	The criteria for non-compliance have been changed from aggregate interruptions to percentage of physical security perimeters not controlled, monitored, and logged.
006-C2,2		
006-C2,3		
006-C2,4		

Commentor	Peter Burke	
Entity Name	American Transmission Company	
Ready to Ballot:	No	
General Comments	American Transmission Company concurs with the comments submitted separately by the Edison Electric Institute and by the Midwest Reliability Organization.	Please refer to responses to Laurence W. Brown, Edison Electric Institute.
006-R1	American Transmission Company concurs with the comments submitted separately by the Edison Electric Institute and by the Midwest Reliability Organization.	
006-R2	American Transmission Company concurs with the comments submitted separately by the Edison Electric Institute.	
006-R3	American Transmission Company concurs with the comments submitted separately by the Edison Electric Institute.	
006-R4		
006-R5		
006-R6		
006-R7		
006-M1		
006-M2		
006-M3		
006-M4		
006-M5		
006-M6		
006-M7		
006-C1,1		
006-C1,2		
006-C1,3		
006-C1,4		
006-C2,1	American Transmission Company concurs with the comments submitted separately by the Edison Electric Institute.	

006-C2,2

006-C2,3

006-C2,4

CIP-006 Drafting Team Responses to Comments

Commentor	Marc Butts	
Entity Name	Southern Company	
Ready to Ballot:	No	
General Comments		
006-R1	R1 - Do these requirements implicitly expect entrance and exit (ingress/egress) to be monitored or just entrance when "access" is considered? If so, it needs be stated explicitly. R1.4 - This is written in such a way as to require the entity to use cardkey access which is not the intent (R3 classifies it as one of several possible options). Suggest making this a subset of R1.3 with an 'if applicable' qualifier or just dropping it. R1.5 - The definition of "authorized" access needs to be defined. Does that mean a name appears on a list or is the person granted tangible access device (e.g., cardkey, traditional key, etc.) where access would be prohibited without the physical device? The expectation of when escort or non-escort is required is not clear. Is there an expectation (e.g. only those with cardkeys can be unescorted, only non-employees need to be escorted, etc.) or is it left to the responsible entity to define in its Physical Security Plan.	R1.2 has been modified to specify control over entry. R1.4 has been modified to include all access controls in R3. R1.5 Any person who has been granted unescorted access should also appear on the authorized access list as required in CIP-004 Requirement 4. In effect the individuals with unescorted access and those on the list should be one in the same. A new requirement R1.6 has been added to address escorted access.
006-R2	Need to remove the phrase 'modifications to any components'. This is overly broad. This would require that the plan be changed when simply changing a camera lens or the type of card reader.	The wording within this requirement has been changed to add clarity. Additionally, the requirement has been moved under R1.
006-R3	R3.2 should be changed to reflect language that recommends these locks, non reproducible keys, etc. as examples. R3.4- Same comment.	Change has been made to allow for equivalent technology.
006-R4	R4.2 - Remove the word "central". The intent is that a breach of security is reported for action or response. If left in would require the expensive construction of a central monitoring station.	References to central have been removed.
006-R5	R5 - Do these requirements implicitly expect entrance and exit (ingress/egress) to be monitored or just entrance when "access" is considered? If so, it needs be stated explicitly.	R1.2 has been modified to specify control over entry.
006-R6		
006-R7		
006-M1		
006-M2		
006-M3		
006-M4		
006-M5		
006-M6		

CIP-006 Drafting Team Responses to Comments

006-M7

006-C1,1

006-C1,2

006-C1,3

006-C1,4

006-C2,1

006-C2,2

006-C2,3

006-C2,4

Commentor	Linda Campbell	
Entity Name	FRCC	
Ready to Ballot:	No	
General Comments	Shouldn’t the cyber assets used in the control and monitoring of Physical Security have a similar requirement as those use in the control and monitoring of Electronic Security (i.e. similar to a hopefully-reword-R1.5 in CIP-005-1 for card key system, etc.)?	This has been added to Requirement R1.8.
006-R1		
006-R2		
006-R3		
006-R4		
006-R5		
006-R6	What exactly is meant by this statement: "Unauthorized access attempts shall be reviewed every two months." Shouldn’t unauthorized access be reviewed immediately? What constitute an unauthorized access attempt? Depending on the size of the organization, the review of all unauthorized access attempts could be very onerous. It is unclear from this requirement what the expectations and disposition of results of a review of unauthorized access are? What’s the point of the review?	Wording on the timeliness of review of unauthorized access attempts has been modified, and moved into R4.
	R6 contains data retention time of logs; that is also covered in D1.3.1. Probably should delete here to be consistent with other standards. There is nothing in either place about retaining information longer, including logs when an unauthorized access attempt is being investigated. Does information related to this need to be kept for a longer period of time?	The drafting team received many comments on the length of time for retention of access logs. Some commenters believed 30 days was sufficient, some said 90 days was too short. When considering these comments, the drafting team agreed that a 30 day time period is too short due to the risk of losing data that may be required in an investigation. More than 90 days would be difficult and potentially very expensive. Ultimately the Drafting Team agreed 90 days is a reasonable period for forensic purposes to allow for potential delay in discovery or investigation of an event. The Drafting Team would like to point out that Responsible Entities may choose to keep logs longer 90 days if they deem appropriate.
006-R7		
006-M1		
006-M2		
006-M3		
006-M4		
006-M5		

006-M6		
006-M7		
006-C1,1	In the applicability section 4.1.10 and 4.1.11, RRO's and NERC are included. Who has the monitoring responsibility for a RRO or NERC?	NERC will monitor the RROs and a third party without vested interest in the outcome will monitor NERC.
	Add Self-Certification and Audit information to this section. Proposed language would be: 1.1.--Complaince Monitoring Responsibility Regional Reliability Organization. 1.1.1.--The Compliance Monitor will request a self-certification annually. 1.1.2.--The Compliance Monitor will perform an audit at least once every three (3) calendar years.	Self-certification has been added under "Additional Compliance Information."
006-C1,2		
006-C1,3	To complement a audit every three years, the data retention period should be 3 years.	The data retention period matches the requirement. See Responses to R6. Only the compliance monitor is required to keep records of an audit for 3 years.
006-C1,4	1.4.3 Theis section restates requirements of CIP-002-1 and should be removed in order to minimize confusion. Proposed wording would be: 1.4.3 For generating facilities where electronic security perimeter extends to areas that cannot be physically secured for saftey reasons the Responsible Entity shall document exceptions along with compensating controls.	It is not the drafting team's intent to add any additional Critical Assets or Critical Cyber Assets beyond those identified by the entity in the risk assessment in CIP-002. However, this information (now D1.4.5) stipulates that Responsible Entities may not write an exception for securing control rooms or the computer rooms that support the control function and contain Critical Cyber Assets. In the event a Responsible Entity determines that the required physical security protections cannot be applied to other Critical Cyber Assets due to unsafe conditions, then the Responsible Entity must document the exception and acceptance of risk per its policies.
006-C2,1	D2.1.2, Change to "aggregate interruptions at a single facility." Companies with many facilities should not be penalized for this by adding together the interruptions from each facility. As currently worded, a company with one facility that has interruptions of systems or data availability for thirty days and a company with 15 facilities that has lost only 2 days of data at each facility would be at the same level on non-compliance.	The criteria for non-compliance have been changed from aggregate interruptions to percentage of physical security perimeters not controlled, monitored, and logged.
006-C2,2	D 2.2.2,Change to "aggregate interruptions at a single facility." Companies with many facilities should not be penalized for this by adding together the interruptions from each facility. As currently worded, a company with one facility that has interruptions of systems or data availability for thirty days and a company with 15 facilities that has lost only 2 days of data at each facility would be at the same level on non-compliance.	See response above.
006-C2,3	2.3.1 States "More than one required record does not exist," is this a entire log for physical access, a document contained in the security plan, or a single log entry of an individual attempting to gain access to a physical site?	The levels of noncompliance have been rewritten and reference to record has been removed.
	D2.3.3, Change to "aggregate interruptions at a single facility." Companies with many	See response at 2.2.

facilities should not be penalized for this by adding together the interruptions from each facility. As currently worded, a company with one facility that has interruptions of systems or data availability for thirty days and a company with 15 facilities that has lost only 2 days of data at each facility would be at the same level on non-compliance.	See response, above.

006-C2,4

CIP-006 Drafting Team Responses to Comments

Commentor	Gary Campbell	
Entity Name	MAIN	
Ready to Ballot:	No	
General Comments	address items below	
006-R1		
006-R2		
006-R3		
006-R4		
006-R5		
006-R6	Retaining records for 90 days seems short when maybe an intrusion may not be detected right a way.	The drafting team received many comments on the length of time for retention of access logs. Some commenters believed 30 days was sufficient, some said 90 days was too short. When considering these comments, the drafting team agreed that a 30 day time period is too short due to the risk of losing data that may be required in an investigation. More than 90 days would be difficult and potentially very expensive. Ultimately the Drafting Team agreed 90 days is a reasonable period for forensic purposes to allow for potential delay in discovery or investigation of an event. The Drafting Team would like to point out that Responsible Entities may choose to keep logs longer 90 days if they deem appropriate. Additional concerns were voiced with regards to the difficulty of keeping video for 90 days. With modern DVR (digital video recording) systems, retaining video has become much more cost effective. Additionally, wording on the timeliness of review of unauthorized access attempts has been clarified, and moved into R4.
006-R7		
006-M1		
006-M2		
006-M3		
006-M4		
006-M5		
006-M6		

CIP-006 Drafting Team Responses to Comments

006-M7		
006-C1,1		
006-C1,2		
006-C1,3		
006-C1,4		
006-C2,1	2.1.1 Delete "Required Documenatation" use " The Physcial Security Plan" More Specific 2.1.2 Do not use aggreagate, delete.	The criteria for non-compliance have been changed from aggregate interruptions to percentage of physical security perimeters not controlled, monitored, and logged.
006-C2,2	2.2.1 Delete "Required Documenatation" use " The Physcial Security Plan" More Specific	See response, above.
006-C2,3	2.3.2 Delete "Required Documenatation" use " The Physcial Security Plan" More Specific	See response, above.
006-C2,4	2.4.2 Change to read " All (or some portion of them) physical security system have not been tested with in the previous calendar year.	See response, above.

CIP-006 Drafting Team Responses to Comments

Commentor	Roger Champagne	
Entity Name	Hydro-Québec TransÉnergie	
Ready to Ballot:	No	
General Comments	Physical security for access modem from home or from the vendor's site are still too confused or not strong enough.	If the Responsible Entity defines the equipment at a user's home or vendor site as a critical cyber asset, then the asset must be protected per this standard.
006-R1	Requirement R1.4 is too prescriptive. R3 covers several possible access devices. Recommend that any device inside any electronic perimeter should also be inside at least one physical perimeter	Please see responses to Ray A'Brial, Central Hudson Gas & Electric Corp.
006-R2		
006-R3	R3 should read, "the Responsible Entity shall document and implement ....". Otherwise, M 3 establishes a new requirement not identified in the Requirements section of the Standard. As we do in cyber security, clearly say if we need to log access in and out or only in, what is done in most of the cases. R3.1 - R3.4 are too prescriptive. They should be removed. R3 changes to "Physical Access Controls - The Responsible Entity shall document and implement the organizational, operational and procedural controls to manage physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day , seven days a week."	
006-R4	R4 should read, "the Responsible Entity shall document and implement ....". Otherwise, M 4 establishes a new requirement not identified in the Requirements section of the Standard. R4.1 - R4.3 are too prescriptive. They should be removed. R4 should read "Monitoring Physical Access - The Responsible Entity shall document and implement the organizational, technical and procedural controls for monitoring physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day , seven days a week."	
006-R5	R5 should read, "the Responsible Entity shall document and implement ....". Otherwise, M5 establishes a new requirement not identified in the Requirements section of the Standard. R5.1 - R5.3 are too prescriptive. They should be removed. R5 should read "Logging Physical Access - The Responsible Entity shall document and implement the organizational, technical and procedural mechanisms for logging and reviewing physical access at all access points to the Physical Security Perimeter(s). Methods shall record sufficient information to uniquely identify individuals and datetime stamps."	

CIP-006 Drafting Team Responses to Comments

006-R6 We recommend changing from "at least 90 calendar days" to "at least 30 calendar days". The log should be reviewed before it is dropped. Also, retaining video can be very be expensive with little benefit.
The statement "Unauthorized access attempts shall be reviewed every two months.", doesn't appear to be accomplishing the desired objective of being cognizant, in a timely manner, of attempted unauthorized access. The drafting team should discuss and clarify their intent or remove the statement.

006-R7

006-M1

006-M2

006-M3

006-M4

006-M5

006-M6

006-M7

006-C1,1

006-C1,2

006-C1,3 To remain consistent with R6, this "ninety days" should change to "30 days".

006-C1,4

006-C2,1

006-C2,2

006-C2,3 In Compliance statement 2.3.1, please clarify what is meant by “record”. If the reference is really to a “document”, then Compliance statement 2.3.1 appears to contradict Compliance statement 2.4.3 in cases where one of the missing documents is the security plan. Note also that no non-compliance level has been defined for cases where one required document (or record) is missing unless that document is the security plan.

006-C2,4

CIP-006 Drafting Team Responses to Comments

Commentor Larry Conrad

Entity Name ECAR Critical Infrastructure Protection Panel

Ready to Ballot: No

General Comments	Add additional exemption: A 4.2.4 (new) -- Applicability: The committee feels than an exemption should be noted under this section for dial-up modems within the Electronic Security Perimeter that do not utilize a routable protocol for external communications. This exemption would apply only to the physical security requirements of this section, not to electronic access control requirements as specified elsewhere in the standards.	D1.44 has been added to address this issue.
	We believe this entire section needs additional work before it can be successfully balloted. In response to Draft II concerns were expressed about the far reaching implications and tremendous costs of implementing the physical security measures mandated in CIP 006, particularly at substation locations. Comments cited issues such as how impractical the prescriptive measures are to implement at remote substation locations, the low risk of a cyber attack initiated via physical access to a remote substation location, the questionable benefit of manual logging at such unattended locations, the overhead required to implement the requirements, etc. Although the comments were extensive, there was little change in this section. While the level of physical security controls contained in CIP 006 may be appropriate for System Operations Centers, we do not believe this prescriptive level of physical security is appropriate for remote locations such as substations. We recommend that the language in CIP 006 be modified so that a distinction is made between system operations centers, generation facilities, and substations. The Requirements prescribed by CIP 006 should not necessarily apply to substations. Please consider using the NERC Physical Security -- Substations Guidelines for physical controls at substations.	The risk assessment as required in CIP-002 applies to Critical Assets, not Cyber Assets. If your risk assessment determines an asset is not critical, then the requirements of this standard do not apply.
006-R1		
006-R2		
006-R3		
006-R4		
006-R5		
006-R6		
006-R7		
006-M1		
006-M2		

006-M3

006-M4

006-M5

006-M6

006-M7

006-C1,1

006-C1,2

006-C1,3

006-C1,4

006-C2,1

006-C2,2

006-C2,3

006-C2,4

CIP-006 Drafting Team Responses to Comments

Commentor	Larry Conrad	
Entity Name	Cinergy	
Ready to Ballot:	No	
General Comments	Cinergy believes this entire section needs additional work before it can be successfully balloted. In response to Draft II Cinergy, and many others, expressed concerns about the far reaching implications and tremendous costs of implementing the physical security measures mandated in CIP 006, particularly at substation locations. Comments from Cinergy, and others, cited issues such as how impractical the prescriptive measures are to implement at remote substation locations, the low risk of a cyber attack initiated via physical access to a remote substation location, the questionable benefit of manual logging at such unattended locations, the overhead required to implement the requirements, etc. Although the comments were extensive, there was little change in this section in response to the comments. While the level of physical security controls contained in CIP 006 may be appropriate for System Operations Centers, we do not believe this prescriptive level of physical security is appropriate for remote locations such as substations. We recommend that the language in CIP 006 be modified so that a distinction is made between system operations centers, generation facilities, and substations. The Requirements prescribed by CIP 006 should not necessarily apply to substations. Separate language should be created for substations which directly links the risks to the prescribed protection. As an alternative, physical security at substations could continue to be guided by the NERC Physical Security -- Substations Guidelines. Exemptions Section: The FAQ's for Section 002 in Draft III state that "Critical Cyber Assets with dial up access not using a routable protocol must meet the Electronic Security Perimeter requirements for the remote access to that device but are not required to meet the requirements for Physical Security Perimeter..." If dial up devices which do not use a routable protocol are exempt from the CIP 006-1 Physical Security requirements, then the CIP 006-1 should list and exemption for dial up devices which do not use a routable protocol in CIP 006 A.4.2. While FAQ's may explain requirements as stated in the CIP document, it does not seem appropriate to use the FAQ's for the purpose of defining exemptions which should be listed in the NERC CIP 006 document.	The risk assessment as required in CIP-002 applies to Critical Assets, not Cyber Assets. If your risk assessment determines an asset is not critical, then the requirements of this standard do not apply.
006-R1		
006-R2		
006-R3	If the participant performs a risk assessment and the risk of launching a cyber attack from physically infiltrating a substation is determined to be low, then does the participant need to implement the physical security measures described?	The entity must perform a risk-based analysis as described in CIP-002. If that analysis identifies Critical Cyber Assets, regardless of where they reside, then the requirements of this standard apply.

006-R4		
006-R5		
006-R6	These standards include numerous and extensive documentation and review requirements. In general annual reviews are required, with updates required within 90 days of the change occurring. Several required timeframes are presently shorter than this and should be increased so that all timeframes throughout the standard are consistent and reasonable, and to make compliance more manageable: R4.1 -- Review unauthorized (physical) access attempts every 2 months. -- This is the only activity in the standard with a 2 month frequency. To make compliance review schedules more easily managed, the frequency of this review should match the review frequency for electronic unauthorized electronic access attempts, which is specified by CIP-005- R3.3 at 90 days.	The drafting team received many comments on the length of time for retention of access logs. Some commenters believed 30 days was sufficient, some said 90 days was too short. When considering these comments, the drafting team agreed that a 30 day time period is too short due to the risk of losing data that may be required in an investigation. More than 90 days would be difficult and potentially very expensive. Ultimately the Drafting Team agreed 90 days is a reasonable period for forensic purposes to allow for potential delay in discovery or investigation of an event. The Drafting Team would like to point out that Responsible Entities may choose to keep logs longer 90 days if they deem appropriate. Additional concerns were voiced with regards to the difficulty of keeping video for 90 days. With modern DVR (digital video recording) systems, retaining video has become much more cost effective. Additionally, wording on the timeliness of review of unauthorized access attempts has been clarified, and moved into R4.
006-R7		
006-M1		
006-M2		
006-M3		
006-M4		
006-M5		
006-M6		
006-M7		
006-C1,1		
006-C1,2		
006-C1,3		
006-C1,4	D1.4.3 Additional Compliance information: This section gets very prescriptive to the point of directing the physical securing of control rooms at generating stations. Regardless of the practicality of securing the physical perimeter for safety or non-safety reasons, Cinergy still does not understand why generating control rooms that are only connected to the critical cyber asset by way of the operating consoles should be included in the electronic perimeter and subject to a physical perimeter requirement. While the console may manipulate the logic of the cyber hardware cabinets, there is little risk of any other cyber access and should be addressed appropriately through a risk assessment.	The intent of this section was to allow for situations where equipment may not be secured for safety reasons. However, access to the console provides the opportunity to operate and manipulate the cyber assets, therefore physical security of the console is critical to maintaining adequate security.

From that standpoint, operation of a console is no different than the physical manipulation of a unit component in the field which would potentially take a unit off line. Physical security at this level should be governed by overall plant physical security requirements exclusive of this standard. The responsible entity should then have the leeway to address physical security through their evaluation and not prescribed to the level of detail required in CIP-006-1

Cinergy recommends that Additional Compliance Information item D 1.4.3 be removed from the standard.

006-C2,1

006-C2,2

006-C2,3

006-C2,4

CIP-006 Drafting Team Responses to Comments

Commentor	Theodore Creedon, P.E.
Entity Name	Creedon Engineering
Ready to Ballot:	Yes
General Comments	
006-R1	
006-R2	
006-R3	
006-R4	
006-R5	
006-R6	
006-R7	
006-M1	
006-M2	
006-M3	
006-M4	
006-M5	
006-M6	
006-M7	
006-C1,1	
006-C1,2	
006-C1,3	
006-C1,4	
006-C2,1	
006-C2,2	
006-C2,3	
006-C2,4	

CIP-006 Drafting Team Responses to Comments

Commentor	Joel De Granda	
Entity Name	Florida Power and Light	
Ready to Ballot:	Yes	
General Comments		
006-R1		
006-R2		
006-R3		
006-R4		
006-R5		
006-R6	What exactly is meant by this statement: "Unauthorized access attempts shall be reviewed every two months." Shouldn't unauthorized access be reviewed immediately? What constitute an unauthorized access attempt?	Wording on the timeliness of review of unauthorized access attempts has been modified, and moved into R4.
006-R7		
006-M1		
006-M2		
006-M3		
006-M4		
006-M5		
006-M6		
006-M7		
006-C1,1		
006-C1,2		
006-C1,3		
006-C1,4		
006-C2,1		
006-C2,2		
006-C2,3		

006-C2,4

Commentor	Richard Engelbrecht
Entity Name	RGE
Ready to Ballot:	No

General Comments

006-R1	Requirement R1.4 is too prescriptive. R3 covers several possible access devices.	Please see responses to Ray A'Brial, Central Hudson Gas & Electric Corp.
006-R2		
006-R3	R3 should read, "the Responsible Entity shall document and implement ....". Otherwise, M 3 establishes a new requirement not identified in the Requirements section of the Standard. R3.1 - R3.4 are too prescriptive. They should be removed. R3 changes to "Physical Access Controls - The Responsible Entity shall document and implement the organizational, operational and procedural controls to manage physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day , seven days a week."	
006-R4	R4 should read, "the Responsible Entity shall document and implement ....". Otherwise, M 4 establishes a new requirement not identified in the Requirements section of the Standard. R4.1 - R4.3 are too prescriptive. They should be removed. R4 should read "Monitoring Physical Access - The Responsible Entity shall document and implement the organizational, technical and procedural controls for monitoring physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day , seven days a week."	
006-R5	R5 should read, "the Responsible Entity shall document and implement ....". Otherwise, M5 establishes a new requirement not identified in the Requirements section of the Standard. R5.1 - R5.3 are too prescriptive. They should be removed. R5 should read "Logging Physical Access - The Responsible Entity shall document and implement the organizational, technical and procedural mechanisms for logging and reviewing physical access at all access points to the Physical Security Perimeter(s). Methods shall record sufficient information to uniquely identify individuals and datetime stamps."	
006-R6	We recommend changing from "at least 90 calendar days" to "at least 30 calendar days". The log should be reviewed before it is dropped. Also, retaining video can be very be expensive with little benefit. The statement "Unauthorized access attempts shall be reviewed every two months.", doesn't	

appear to be accomplishing the desired objective of being cognizant, in a timely manner, of attempted unauthorized access. The drafting team should discuss and clarify their intent or remove the statement.

006-R7

006-M1

006-M2

006-M3

006-M4

006-M5

006-M6

006-M7

006-C1,1

006-C1,2

006-C1,3 To remain consistent with R6, this "ninety days" should change to "30 days".

006-C1,4

006-C2,1

006-C2,2

006-C2,3 In Compliance statement 2.3.1, please clarify what is meant by “record”. If the reference is really to a “document”, then Compliance statement 2.3.1 appears to contradict Compliance statement 2.4.3 in cases where one of the missing documents is the security plan. Note also that no non-compliance level has been defined for cases where one required document (or record) is missing unless that document is the security plan.

006-C2,4

CIP-006 Drafting Team Responses to Comments

Commentor	Ken Fell	
Entity Name	New York ISO	
Ready to Ballot:	No	
General Comments		
006-R1	equirement R1.4 is too prescriptive. R3 covers several possible access devices.	Please see responses to Ray A'Brial, Central Hudson Gas & Electric Corp.
006-R2		
006-R3	R3 should read, "the Responsible Entity shall document and implement ....". Otherwise, M 3 establishes a new requirement not identified in the Requirements section of the Standard. R3.1 - R3.4 are too prescriptive. They should be removed. R3 changes to "Physical Access Controls - The Responsible Entity shall document and implement the organizational, operational and procedural controls to manage physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day , seven days a week."	
006-R4	R4 should read, "the Responsible Entity shall document and implement ....". Otherwise, M 4 establishes a new requirement not identified in the Requirements section of the Standard. R4.1 - R4.3 are too prescriptive. They should be removed. R4 should read "Monitoring Physical Access - The Responsible Entity shall document and implement the organizational, technical and procedural controls for monitoring physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day , seven days a week."	
006-R5	R5 should read, "the Responsible Entity shall document and implement ....". Otherwise, M5 establishes a new requirement not identified in the Requirements section of the Standard. R5.1 - R5.3 are too prescriptive. They should be removed. R5 should read "Logging Physical Access - The Responsible Entity shall document and implement the organizational, technical and procedural mechanisms for logging and reviewing physical access at all access points to the Physical Security Perimeter(s). Methods shall record sufficient information to uniquely identify individuals and datetime stamps."	
006-R6	We recommend changing from "at least 90 calendar days" to "at least 30 calendar days". The log should be reviewed before it is dropped. Also, retaining video can be very be expensive with little benefit. The statement "Unauthorized access attempts shall be reviewed every two months.", doesn't	

	appear to be accomplishing the desired objective of being cognizant, in a timely manner, of attempted unauthorized access. The drafting team should discuss and clarify their intent or remove the statement.
006-R7	
006-M1	
006-M2	
006-M3	
006-M4	
006-M5	
006-M6	
006-M7	
006-C1,1	
006-C1,2	
006-C1,3	To remain consistent with R6, this "ninety days" should change to "30 days".
006-C1,4	
006-C2,1	
006-C2,2	
006-C2,3	In Compliance statement 2.3.1, please clarify what is meant by “record”. If the reference is really to a “document”, then Compliance statement 2.3.1 appears to contradict Compliance statement 2.4.3 in cases where one of the missing documents is the security plan. Note also that no non-compliance level has been defined for cases where one required document (or record) is missing unless that document is the security plan.
006-C2,4	

CIP-006 Drafting Team Responses to Comments

Commentor Francis Flynn

Entity Name National Grid USA

Ready to Ballot: No

General Comments

006-R1 Requirement R1.4 is too prescriptive. R3 covers several possible access devices.

Please see responses to Ray A'Brial, Central Hudson Gas & Electric Corp.

006-R2

006-R3 R3 should read, "the Responsible Entity shall document and implement ....". Otherwise, M 3 establishes a new requirement not identified in the Requirements section of the Standard.

R3.1 - R3.4 are too prescriptive. They should be removed.

R3 changes to "Physical Access Controls - The Responsible Entity shall document and implement the organizational, operational and procedural controls to manage physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day , seven days a week."

006-R4 R4 should read, "the Responsible Entity shall document and implement ....". Otherwise, M 4 establishes a new requirement not identified in the Requirements section of the Standard.

R4.1 - R4.3 are too prescriptive. They should be removed.

R4 should read "Monitoring Physical Access - The Responsible Entity shall document and implement the organizational, technical and procedural controls for monitoring physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day , seven days a week."

006-R5 R5 should read, "the Responsible Entity shall document and implement ....". Otherwise, M5 establishes a new requirement not identified in the Requirements section of the Standard.

R5.1 - R5.3 are too prescriptive. They should be removed.

R5 should read "Logging Physical Access - The Responsible Entity shall document and implement the organizational, technical and procedural mechanisms for logging and reviewing physical access at all access points to the Physical Security Perimeter(s). Methods shall record sufficient information to uniquely identify individuals and datetime stamps."

006-R6 We recommend changing from "at least 90 calendar days" to "at least 30 calendar days". The log should be reviewed before it is dropped. Also, retaining video can be very be expensive with little benefit.
The statement "Unauthorized access attempts shall be reviewed every two months.", doesn't

appear to be accomplishing the desired objective of being cognizant, in a timely manner, of attempted unauthorized access. The drafting team should discuss and clarify their intent or remove the statement.

006-R7

006-M1

006-M2

006-M3

006-M4

006-M5

006-M6

006-M7

006-C1,1

006-C1,2

006-C1,3 To remain consistent with R6, this "ninety days" should change to "30 days".

006-C1,4

006-C2,1

006-C2,2

006-C2,3 In Compliance statement 2.3.1, please clarify what is meant by “record”. If the reference is really to a “document”, then Compliance statement 2.3.1 appears to contradict Compliance statement 2.4.3 in cases where one of the missing documents is the security plan. Note also that no non-compliance level has been defined for cases where one required document (or record) is missing unless that document is the security plan.

006-C2,4

CIP-006 Drafting Team Responses to Comments

Commentor	Greg Fraser	
Entity Name	Manitoba Hydro	
Ready to Ballot:	No	
General Comments	Either CIP-006 or CIP-004 should clearly state that access is only for authorized personnel and that all access by others must escorted.	This has been clarified in CIP-006, Requirement R1.6
006-R1	Suggest changing R1.2. to the following to specifically exclude the dial-up access from requiring the Physical Security Perimeter and all the local access requirements. "R1.2 Measures to control access at all access points of the perimeter(s), and to protect the Critical Cyber Assets within them. For dial-up accessible Critical Cyber Assets that use non-routable protocols, the Responsible Entity shall not require a Physical Security Perimeter for that single access point at the dial-up device."	Modifications have been made to the additional compliance section to address this point, and the FAQ has been updated.
	In R1.5, what is the required review period? R6 indicates 2 months for unauthorized attempts while other review periods in the cyber security standards are longer.	Requirement R1.5 has been modified to align with the access review requirements of CIP-004. Review requirements for R6 have been removed.
006-R2	Since R2 refers to the security plan, this requirement would be better included as part of R1. As written it really does not refer to a documentation review but rather a security plan review.	This has been moved under R1 as suggested.
006-R3	In R3.3 "24 hours a day" should be moved into the general statement of R3 as this requirement really refers to all options or combination of options in R3 (see the wording in R4).	Modifications have been made to the additional compliance section to address this and the FAQ has been updated.
006-R4	Suggest adding "real-time" to clarify the intent e.g. "...real-time monitoring of physical access..."	Human observation has been added to R3.2.
006-R5	Again suggest adding "24 hours a day" as worded in R4.	This change has been made.
	Remove "and reviewing" moving the review requirement in R6. Then R5 refers only to the logging function.	The review requirement has been moved to R6..
006-R6	The requirement to keep video records for 90 days is too long a period for so much data. Suggest 30 calendar days. As in 1200 suggest the review of access logs be at least every 90 days. Unauthorized attempt monitoring should be part of monitoring physical access in R4 as waiting two months is far too long. Then the two month review of unauthorized attempts could be part of the 90 calendar day review.	The drafting team received many comments on the length of time for retention of access logs. Some commenters believed 30 days was sufficient, some said 90 days was too short. When considering these comments, the drafting team agreed that a 30 day time period is too short due to the risk of losing data that may be required in an investigation. More than 90 days would be difficult and potentially very expensive. Ultimately the Drafting Team agreed 90 days is a reasonable period for forensic purposes to allow for potential delay in discovery or investigation of an event. The Drafting Team would like to point out that Responsible Entities may choose to keep logs longer 90 days if they deem appropriate. Additional concerns were voiced with regards to the difficulty of keeping video for 90 days. With modern DVR (digital video recording) systems, retaining video has become much more cost effective. Additionally,

		wording on the timeliness of review of unauthorized access attempts has been clarified, and moved into R4.
006-R7		
006-M1	Suggest wording "Document of the physical security plan as outlined in R1."	Measures have been rewritten to refer back to the requirements.
006-M2	"Documentation of the review and any update of the physical security plan, as required in R2." Suggest wording similar to M3.	Measures have been rewritten to refer back to the requirements.
006-M3		
006-M4		
006-M5		
006-M6		
006-M7		
006-C1,1		
006-C1,2		
006-C1,3		
006-C1,4		
006-C2,1	In 2.1.2 "Aggregate interruptions" is not defined as to whether this in the summation of multi-interruptions per year or the same interruption for multi-devises or both. Tracking the interruptions for the devices is not part of the requirements.	The criteria for non-compliance have been changed from aggregate interruptions to percentage of physical security perimeters not controlled, monitored, and logged.
006-C2,2		
006-C2,3		
006-C2,4	2.4.1 Suggest wording of: "Required access control, monitoring or logging of access does not exist."	The criteria for non-compliance have been changed from aggregate interruptions to percentage of physical security perimeters not controlled, monitored, and logged.

CIP-006 Drafting Team Responses to Comments

Commentor	Jerry Freese	
Entity Name	American Electric Power	
Ready to Ballot:	No	
General Comments	Based on the expanded scope set forth in CIP-002 R1 for the Critical Assets and the subsequently expanded scope of the Critical Cyber Assets and the Electronic Security Perimeter, it would be impractical and infeasible to meet the obligations set forth in this requirement.	CIP-006 applies to Critical Cyber Assets associated with Critical Assets. CIP-002 has been changed to recognize a risk-based approach to identifying Critical Assets. The drafting team also has removed much of the prescriptive language from these standards.
006-R1	Based on the scope of what is deemed as Critical Assets and subsequent Critical Cyber Assets in this standard, there would be a significant requirement to have six-walled boundary or other mentioned security enclosures for the Critical Cyber Assets within many substations, generation facilities and other locations. This is not feasible nor practical in many substation or plant environment.	CIP-002 and the definition of Critical Asset address this concern. For those cyber assets that are considered critical, the six-wall boundary is the most appropriate protection method and is required. This boundary may be satisfied through the use of an alternative measure, such as a security enclosure. Additionally, in situations where an entity is unable to meet it's cyber security policy, a provision has been made in the additional compliance information section to allow for approved exceptions, which will not result in non-compliance.
006-R2		
006-R3		
006-R4	We are in the process of planning telecommunications infrastructure requirements for supporting a massive SCADA expansion effort over the next 5-10 years. This section provides a couple of options, one of which is a SCADA-based options (e.g. remotely monitor gate and door entry alarms). I assume that this would be a primary means of compliance(?). However, as an alternative, the standard allows for closed-circuit television or video surveillence......I assume that the telecommunications bandwidth to support video is very significant. Therefore, to proactively plan the AEP telecomm infrastructure to support your compliance strategy, it would be important to get a forecast from your group sometime in 2005 or early 2006 of the types of stations that might eventually need to have video capability (e.g. some 765kv facilities? all 765kv facilities, unmanned generation station outlets? etc). In that way we could plan/size the telecomm data link to meet video bandwidth requirements while we execute the SCADA expansion efforts.	Specific references to video monitoring have been removed from this requirement; however, video monitoring is an alternative that could meet the requirement if a Responsible Entity so chooses. Regardless, the facilities for which monitoring is required is driven by the Responsible Entity's risk assessment and identification of Critical Assets under CIP-002.
006-R5		
006-R6		
006-R7		
006-M1		
006-M2		
006-M3		

006-M4

006-M5

006-M6

006-M7

006-C1,1

006-C1,2

006-C1,3

006-C1,4

006-C2,1

006-C2,2

006-C2,3

006-C2,4

CIP-006 Drafting Team Responses to Comments

Commentor	Edwin C. Goff III	
Entity Name	Progress Energy	
Ready to Ballot:	No	
General Comments	Log/data retention is not addressed consistently between the physical and electronic security standards. In the electronic standard there is a data retention section in the compliance area. In the physical security standard there is a requirement (CIP-006-1 R6).	
006-R1		
006-R2		
006-R3		
006-R4		
006-R5		
006-R6		
006-R7		
006-M1		
006-M2		
006-M3		
006-M4		
006-M5		
006-M6		
006-M7		
006-C1,1		
006-C1,2		
006-C1,3		
006-C1,4		
006-C2,1	2.1.2 & 2.2.2-- These items indicate non-compliance for "aggregate interruptions in the system or data availability over a full calendar year exist for more than seven calendar days(2.2.1)...for more than thirty calendar days(2.2.2)" There is no previously stated requirement for keeping up with the availability of the access monitoring systems. This	The criteria for non-compliance have been changed from aggregate interruptions to percentage of physical security perimeters not controlled, monitored, and logged.

	appears to create a requirement for logging the availability of the monitoring systems.	Retention of outage records regarding access controls, logging and monitoring has been added to R6.3.
006-C2,2	2.1.2 & 2.2.2-- These items indicate non-compliance for "aggregate interruptions in the system or data availability over a full calendar year exist for more than seven calendar days(2.2.1)...for more than thirty calendar days(2.2.2)" There is no previously stated requirement for keeping up with the availability of the access monitoring systems. This appears to create a requirement for logging the availability of the monitoring systems.	The criteria for non-compliance have been changed from aggregate interruptions to percentage of physical security perimeters not controlled, monitored, and logged. Retention of outage records regarding access controls, logging and monitoring has been added to R6.3.
006-C2,3		
006-C2,4		

CIP-006 Drafting Team Responses to Comments

Commentor	Kenneth Goldsmith	
Entity Name	Alliant Energy	
Ready to Ballot:	No	
General Comments	It is evident form the answers in the FAQ (see #4, for example) that the intention is for all critical cyber assets to be within a Ohysical Security Perimeter (or a cage). However, the language of the Requirements themselves does not appear to explicitly state this requirement. This should be corrected.	This is clearly stated in the definition of physical security perimeter and, therefore, it should not be necessary to repeat the definition in the requirements.
006-R1		
006-R2		
006-R3		
006-R4		
006-R5		
006-R6		
006-R7		
006-M1		
006-M2		
006-M3		
006-M4		
006-M5		
006-M6		
006-M7		
006-C1,1		
006-C1,2		
006-C1,3		
006-C1,4		
006-C2,1		

006-C2,2

006-C2,3

006-C2,4

CIP-006 Drafting Team Responses to Comments

Commentor	Kathleen Goodman	
Entity Name	ISO New England Inc	
Ready to Ballot:	No	
General Comments	We believe that CIP002 through CIP009 be beyond the intended scope of the original SAR for 1300. The final SAR for 1300, dated March 8, 2004, clearly states that the U/A 1200 is the basis for development of a permanent standard to replace it. The intent of both U/A 1200 and SAR 1300 is to establish a minimum set of cyber security best practices as a standard baseline for general cyber protection of a reliable BES. In establishing such a baseline, all care should be taken to aviod dictating particular tools, technologies, and/or methodologies. Where such are referenced, those references should be removed.	The Drafting Team has modified these standards to the extent practical to remove references to specific technologies. However, where appropriate, certain accepted methodologies and security-practice specific terms are still referenced; examples are passwords, access controls and access logs.
006-R1	Recommend that any device inside any electronic perimeter should also be inside at least one physical perimeter.	By definition, the Physical Security Perimeter houses all Critical Cyber Assets.
	R1.1 Change to "deploy remedial measures appropriate to physical environment...". Remove "(a cage/safe/cabinet system that control physical access to the critical cyber assets)."	R1.1 has been modified to address processes to identify and document that all Cyber Assets within the Electronic Security Perimeter also reside within an identified Physical Security Perimeter.
	R1.3 Change to "to monitor and authorize physical access."	This requirement has been modified to allow for the use of an alternative measure, such as a security enclosure. Examples of security enclosures have been removed.
006-R2		
006-R3	R3 Remove the word "Organizational."	Removed.
	R3.1 & R3.4 remove as too limiting by reference and does not leave room for more advanced tools, technologies, and/or methodologies.	Change has been made to allow for equivalent technology.
006-R4	R4 should read "Monitoring Physical Access - The Responsible Entity shall document and implement the organizational, technical, and procedural controls for monitoring physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week." R4.1 & R4.3 remove, these are too prescriptive.	R4 has been reworded. Modifications to the subrequirements have been made to provide greater latitude regarding methods of monitoring as long as either human notification or observation is in place.
006-R5	R5 should read "Logging Physical Access - The Responsible Entity shall document and implement the organizational, technical, and procedural mechanisms for logging and reviewing physical access at all access points to the Physical Security Perimeter(s). Methods shall record sufficient information to uniquely identify individuals and date/time stamps."	This requirement has been modified. R5 has been modified to allow for other equivalent logging methods.

	R5.1 & R5.3 remove, these are too prescriptive.	
006-R6	We recommend changing from "at least 90 calendar days" to "at least 30 calendar days. The log should be reviewed before it is dropped . Also, retaining a video can be very expensive with little benefit. Remove two-month reviews; it is being monitored, why review?	The drafting team received many comments on the length of time for retention of access logs. Some commenters believed 30 days was sufficient, some said 90 days was too short. When considering these comments, the drafting team agreed that a 30 day time period is too short due to the risk of losing data that may be required in an investigation. More than 90 days would be difficult and potentially very expensive. Ultimately the Drafting Team agreed 90 days is a reasonable period for forensic purposes to allow for potential delay in discovery or investigation of an event. The Drafting Team would like to point out that Responsible Entities may choose to keep logs longer 90 days if they deem appropriate. Additional concerns were voiced with regards to the difficulty of keeping video for 90 days. With modern DVR (digital video recording) systems, retaining video has become much more cost effective. Additionally, wording on the timeliness of review of unauthorized access attempts has been clarified, and moved into R4.
006-R7	R7.2 Remove "(from time of discovery to time of repair)."	This change has been made.
006-M1	Not a measurement statement.	Measures have been rewritten to refer back to the requirements. They have been reviewed by NERC Compliance Enforcement program personnel and no objections were raised.
006-M2	Not a measurement statement.	See above.
006-M3	Not a measurement statement.	See above.
006-M4	Not a measurement statement.	See above.
006-M5	Not a measurement statement.	See above.
006-M6	Not a measurement statement.	See above.
006-M7	Not a measurement statement.	See above.
006-C1,1		
006-C1,2		
006-C1,3	It is not clear when you mean documents, records, or data. These are three distinct items and should not be referenced interchangeably. Please clarify.	The Drafting Team has revised the standards for consistency. Please see FAQs.
	TO be consistent with R6, 90 days should be changed to 30 days.	Please see responses to R6.
006-C1,4	1.4.1 This is a requirement statement - remove it.	This statement clearly refers to noncompliance.
006-C2,1		
006-C2,2		
006-C2,3	In compliance statement 2.3.1, please clarify what is meant by "record." If the reference is	The levels of noncompliance have been rewritten and reference to

	really to a "document," then compliance statement 2.3.1 appears to contradict compliance statement 2.4.3 in cases where onle of the missing documents is the security plan. Note also that no non-compliance level has been defined for cases where one required document (or record) is missing unless that document is the security plan.	record has been removed.
006-C2,4		

CIP-006 Drafting Team Responses to Comments

Commentor	Tim Hattaway
Entity Name	Alabama Electric Cooperative
Ready to Ballot:	Yes
General Comments	
006-R1	
006-R2	
006-R3	
006-R4	
006-R5	
006-R6	
006-R7	
006-M1	
006-M2	
006-M3	
006-M4	
006-M5	
006-M6	
006-M7	
006-C1,1	
006-C1,2	
006-C1,3	
006-C1,4	
006-C2,1	
006-C2,2	
006-C2,3	
006-C2,4	

Commentor	Jerry Heeren
Entity Name	MEAG Power
Ready to Ballot:	Yes
General Comments	
006-R1	
006-R2	
006-R3	
006-R4	
006-R5	
006-R6	
006-R7	
006-M1	
006-M2	
006-M3	
006-M4	
006-M5	
006-M6	
006-M7	
006-C1,1	
006-C1,2	
006-C1,3	
006-C1,4	
006-C2,1	
006-C2,2	
006-C2,3	
006-C2,4	

CIP-006 Drafting Team Responses to Comments

Commentor	Peter Henderson	
Entity Name	Independent Electricity System Operator (IESO)	
Ready to Ballot:	No	
General Comments		
006-R1	Requirement R1.4 is too prescriptive. R3 covers several possible access devices.	Please see responses to Ray A'Brial, Central Hudson Gas & Electric Corp.
006-R2		
006-R3	1. R3 should read, "the Responsible Entity shall document and implement ....". Otherwise, M 3 establishes a new requirement not identified in the Requirements section of the Standard.	
006-R4	1. R4 should read, "the Responsible Entity shall document and implement ....". Otherwise, M 4 establishes a new requirement not identified in the Requirements section of the Standard.	
006-R5	1. R5 should read, "the Responsible Entity shall document and implement ....". Otherwise, M 5 establishes a new requirement not identified in the Requirements section of the Standard. 2. R5.1 - R5.3 are too prescriptive. They should be removed.	
006-R6		
006-R7		
006-M1		
006-M2		
006-M3		
006-M4		
006-M5		
006-M6		
006-M7		
006-C1,1		
006-C1,2		

006-C1,3 2. R3.1 - R3.4 are too prescriptive. They should be removed. 2. R4.1 - R4.3 are too prescriptive. They should be removed.

006-C1,4

006-C2,1

006-C2,2

006-C2,3 In Compliance statement 2.3.1, please clarify what is meant by “record”. If the reference is really to a “document”, then Compliance statement 2.3.1 appears to contradict Compliance statement 2.4.3 in cases where one of the missing documents is the security plan. Note also that no non-compliance level has been defined for cases where one required document (or record) is missing unless that document is the security plan.

006-C2,4

CIP-006 Drafting Team Responses to Comments

Commentor	E. Nick Henery	
Entity Name	SMUD	
Ready to Ballot:	Yes	
General Comments	The Drafting Team will need to go through the Standard and assign responsibility to each function from the functional model like the Version 0 STD. For this Standard to enforceable the generic use of Responsible Entity is the same as the generic use of Control Area. Even if the Standard lists the different functions it leaves open the possibility of misinterpretation as to which function is truly responsible.	The Responsible Entities are clearly enumerated in the standard Section A, item 4.
006-R1		
006-R2		
006-R3		
006-R4		
006-R5		
006-R6		
006-R7		
006-M1		
006-M2		
006-M3		
006-M4		
006-M5		
006-M6		
006-M7		
006-C1,1		
006-C1,2		
006-C1,3		
006-C1,4		
006-C2,1		

006-C2,2

006-C2,3

006-C2,4

CIP-006 Drafting Team Responses to Comments

Commentor	Jack Hobbick	
Entity Name	Consumers Energy	
Ready to Ballot:	No	
General Comments	Consumers Energy has also submitted comments via the ECAR CIPP.	Please see responses to Larry Conrad, ECAR CIPP.
006-R1		
006-R2		
006-R3		
006-R4		
006-R5		
006-R6		
006-R7		
006-M1		
006-M2		
006-M3		
006-M4		
006-M5		
006-M6		
006-M7		
006-C1,1		
006-C1,2		
006-C1,3		
006-C1,4		
006-C2,1		
006-C2,2		
006-C2,3		
006-C2,4		

CIP-006 Drafting Team Responses to Comments

Commentor	Richard Kafka	
Entity Name	Pepco Holdings, Inc.	
Ready to Ballot:	No	
General Comments		
006-R1	6 floor - reasonability? FAQ14 could include drop ceiling and/or raised floor if in secure area? R.1.4 appears to be in conflict with R3. R1.4 requires card access.	The consensus industry opinion, based on comments received, is that the requirement for a six-wall boundary is reasonable. Furthermore, additional verbiage has been added to clarify the boundary as completely enclosed. R1.4 has been modified to include all access controls in R3.
006-R2	Any modification to any components?	It is not the intent of this requirement to be overbroad but to update the security plan with changes of a significant nature only. The wording within this requirement has been changed to add clarity, and the requirement has been moved under R1. Additionally an FAQ has been added to describe the intent of this requirement.
006-R3	Replace "may" with "example".	Change has been made to allow for equivalent technology.
006-R4		
006-R5		
006-R6		
006-R7		
006-M1		
006-M2		
006-M3		
006-M4		
006-M5		
006-M6		
006-M7		
006-C1,1		
006-C1,2		

CIP-006 Drafting Team Responses to Comments

006-C1,3		
006-C1,4		
006-C2,1	C2.1.2 -- The term "aggregate" is unclear. Does it cover all perimeters, or the aggregate for each perimeter? Also, the seven-day criterion is not consistent with the six-hour criterion for Electronic Security Perimeters specified in CIP-005-C2.1.2. Seven days is the more reasonable period, particularly considering frequent, short interruptions such as are caused by lightening.	The criteria for non-compliance have been changed from aggregate interruptions to percentage of physical security perimeters not controlled, monitored, and logged.
006-C2,2		
006-C2,3		
006-C2,4		

CIP-006 Drafting Team Responses to Comments

Commentor	Tony Kroskey	
Entity Name	Brazos Electric Power Cooperative	
Ready to Ballot:	No	
General Comments		
006-R1	R1., suggest changing text "create, document, and maintain a physical security plan" to "create, document, and maintain a physical security plan to protect Critical Cyber Assets. R1.1, change word "indentified" to "identifies".	R1 has been changed as suggested.
006-R2	Suggest changing text "of any modification to any components" to "of modification to any components effecting physical security"	It is not the intent of this requirement to be overbroad but to update the security plan with changes of a significant nature only. The wording within this requirement has been changed to add clarity, and the requirement has been moved under R1. Additionally an FAQ has been added to describe the intent of this requirement.
006-R3		
006-R4		
006-R5		
006-R6		
006-R7		
006-M1		
006-M2		
006-M3		
006-M4		
006-M5		
006-M6		
006-M7		
006-C1,1		
006-C1,2		
006-C1,3		
006-C1,4		

CIP-006 Drafting Team Responses to Comments

006-C2,1

006-C2,2

006-C2,3

006-C2,4

CIP-006 Drafting Team Responses to Comments

Commentor	Carol Krysevig	
Entity Name	Allegheny Energy Supply Co. LLC	
Ready to Ballot:	Yes	
General Comments	The answer to FAQ 11 (regarding CIP-002) contains information that should be clearly stated within the body of the standard. The following information should be added under section D 1.4: a. 'Critical Cyber Assets with dial-up access not using a routable protocol must meet the Electronic Security Perimeter requirements for the remote access to that device but does not require a Physical Security Perimeter or local Electronic Security Perimeter for the actual Critical Cyber Asset. Secure remote access meets the intent of the Cyber Security Standards to provide a minimum level of security.'	D1.4.4 was added to address dial-up accessible Critical Cyber Assets that use non-routable protocols.
	D1.4.3. - This information should be included as a Requirement, not as 'Additional Compliance Information.' Also, please clarify that we are not expected to physically secure a control room if it does not contain a Critical Cyber Asset. Also, there should be room for en examption if physically securing a control room is determined to be a safety hazard.	The purpose of D1.4.3 (renumbered to D1.4.5) is to address a specific situation that may exist where a Critical Cyber Asset is within an Electronic Security Perimeter, but is out in the open in an area that cannot be physically secured without impacting safety. It defines for Responsible Entities the minimum they must do in those special cases.
	D2.1.1 -- Specify exactly what documents NERC is looking for. D2.2.1 -- Specify exactly what documents NERC is looking for. D2.3.1. - 'More than one required record does not exist...' Need clarification on what required record you are referring to. D2.3.2 -- Specify exactly what documents NERC is looking for.	The levels of noncompliance have been rewritten.
006-R1	R1.1. -- What ultimately determines when a security enclosure is required for field devices connected to a critical cyber asset? Does the field device have to provide an interactive access point to the asset?	R1.1 If the field device is identified as a Critical Cyber Asset or is within the Electronic Security Perimeter, it will require a completely enclosed border.
	R1.3. -- How do you expect entities to monitor field device enclosures for physical access if lock & key is the enclosure's security measure?	R1.3 The Responsible Entity retains the flexibility to determine how to implement the requirements of this standard using reasonable business judgment.
	R1.4. -- Revise the term 'piggybacking' to 'tailgating'.	R1.4 The term piggybacking has been removed.
006-R2		
006-R3	R3. - AE continues to have an concern with physically securing the generating station control rooms, per this standard, due to the numerous personnel and activities that occur in the control room on a daily basis, and more importantly, during outage periods.	The drafting team recognizes this concern, however, the need to physically secure the control room is key to protecting critical cyber assets.
	R3.3. -- Revise the phrase 'twenty-four hours per day' since some entities may choose to use a combination of security personnel and electronic security to control access at different times of the day.	R3.3 The 24-hour requirement has been removed.

006-R4	R4.3. -- Revise the term 'security personnel' to 'authorized on-site personnel'.	Requirement modified as suggested.
006-R5	R5. -- The logging requirement is problematic for field devices within the six walled enclosures. How can an accurate log be maintained for an enclosure sitting in the middle of a substation or power station?	Technical and procedural controls are to be used for logging. If the device is within the six-wall enclosure, then the logging at access points through that enclosure would be sufficient. If an enclosure is used, the expectation is that some sort of alarm system or human observation with manual logging will be used.
006-R6		
006-R7		
006-M1		
006-M2		
006-M3		
006-M4		
006-M5		
006-M6		
006-M7		
006-C1,1		
006-C1,2		
006-C1,3		
006-C1,4		
006-C2,1		
006-C2,2		
006-C2,3		
006-C2,4		

Commentor	John Lim
Entity Name	Con Edison
Ready to Ballot:	No

General Comments

006-R1	Requirement R1.4 is too specific. Access cards may or may not be the technology used. R3 covers several possible access devices.	Please see responses to Ray A'Brial, Central Hudson Gas & Electric Corp.
006-R2		
006-R3	R3 should read, "the Responsible Entity shall document and implement ....". Otherwise, M 3 establishes a new requirement not identified in the Requirements section of the Standard. R3.1 - R3.4 are too prescriptive and technology specific. They should be removed. R3 changes to "Physical Access Controls - The Responsible Entity shall document and implement the organizational, operational and procedural controls to manage physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day , seven days a week."	
006-R4	R4 should read, "the Responsible Entity shall document and implement ....". Otherwise, M 4 establishes a new requirement not identified in the Requirements section of the Standard. R4.1 - R4.3 are too specific: monitoring methods may change. They should be removed. R4 should read "Monitoring Physical Access - The Responsible Entity shall document and implement the organizational, technical and procedural controls for monitoring physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day , seven days a week."	
006-R5	R5 should read, "the Responsible Entity shall document and implement ....". Otherwise, M5 establishes a new requirement not identified in the Requirements section of the Standard. R5.1 - R5.3 are too prescriptive. They should be removed. R5 should read "Logging Physical Access - The Responsible Entity shall document and implement the organizational, technical and procedural mechanisms for logging and reviewing physical access at all access points to the Physical Security Perimeter(s). Methods shall record sufficient information to uniquely identify individuals and datetime stamps."	
006-R6	We recommend changing from "at least 90 calendar days" to "at least 30 calendar days". The log should be reviewed before it is dropped. Also, retaining video can be very be expensive with little benefit. The statement "Unauthorized access attempts shall be reviewed every two months.", doesn't appear to be accomplishing the desired objective of being cognizant, in a timely manner, of	

	attempted unauthorized access. The drafting team should discuss and clarify their intent or remove the statement.	
006-R7		
006-M1		
006-M2		
006-M3		
006-M4		
006-M5		
006-M6		
006-M7		
006-C1,1		
006-C1,2		
006-C1,3	To remain consistent with R6, this "ninety days" should change to "30 days".	Please refer to response to comment on R6.
006-C1,4		
006-C2,1		
006-C2,2		
006-C2,3		
006-C2,4		

CIP-006 Drafting Team Responses to Comments

Commentor	Deborah Linke	
Entity Name	Bureau of Reclamation	
Ready to Ballot:	No	
General Comments	Given the extremely broad definition of Critical Cyber Assets in the first standard to include supporting systems, Reclamation is particularly concerned about the requirement that all Critical Cyber Assets be enclosed within six surfaces. This would mean virtually all equipment would have to be inside an enclosure, which is probably not practical. Equipment that is only dial-up accessible should be exempted from these physical security controls.	Multiple Critical Cyber Assets may reside within a common 6-wall enclosure, such as a computer room or a control room. Where a Responsible Entity is unable to meet the requirement to place equipment in an enclosure, it can write an exception to its own security policies that implement this requirement (see CIP-003). A Responsible Entity's duly authorized exception will not result in non-compliance, as noted in the Additional Compliance section of this standard. Critical Cyber Assets that do not use routable protocols and are dial-up accessible are addressed in the additional compliance section.
006-R1	R1.1: If the Critical Cyber Assets definition is refined, then this section may need to be reworded to specifically state that the physical security perimeter is to enclose all Critical Cyber Assets.	By definition, the Physical Security Perimeter houses all Critical Cyber Assets. R1.1 has been modified to address processes to identify and document that all Cyber Assets within the Electronic Security Perimeter also reside within an identified Physical Security Perimeter.
006-R2		
006-R3	The definition of "access points" is not established or differentiated between doors and windows. This requirement dictates special locks and authentication for "all access points." It would probably be more reasonable to require these controls only at access points normally used for physical access.	Although not normally used for entry, windows are physical access points. They are potential points of entry into a facility just like doors and should not be differentiated in this respect.
006-R4	R4.2: The term "without authorization" implies that the door, window and gate alarms, and motion sensors, must be able to differentiate between authorized and unauthorized access.	Sensors may be able to determine authorized access based upon the receipt of an authorized code, via a cardkey or entered at a keypad, for example. In the case where they cannot, such as when an entity installs an alarm system without a local authentication mechanism, then procedural controls at the monitoring station must be in place to authenticate access.
006-R5		
006-R6		
006-R7		
006-M1		
006-M2		

006-M3

006-M4

006-M5

006-M6

006-M7

006-C1,1

006-C1,2

006-C1,3

006-C1,4

006-C2,1

006-C2,2

006-C2,3

006-C2,4

CIP-006 Drafting Team Responses to Comments

Commentor	Greg Mason
Entity Name	Dynegy Generation
Ready to Ballot:	Yes
General Comments	
006-R1	
006-R2	
006-R3	
006-R4	
006-R5	
006-R6	
006-R7	
006-M1	
006-M2	
006-M3	
006-M4	
006-M5	
006-M6	
006-M7	
006-C1,1	
006-C1,2	
006-C1,3	
006-C1,4	
006-C2,1	
006-C2,2	
006-C2,3	
006-C2,4	

CIP-006 Drafting Team Responses to Comments

Commentor	Paul McClay	
Entity Name	Tampa Electric	
Ready to Ballot:	No	
General Comments	Shouldn't the cyber assets used in the control and monitoring of Physical Security have a similar requirement as those used in the control and monitoring of Electronic Security (i.e. similar to a hopefully, more specifically, reworded R1.5 in CIP-005-1 for card key system, etc.)?	Please see responses to Linda Campbell, FRCC.
006-R1		
006-R2		
006-R3		
006-R4		
006-R5		
006-R6	Depending on the size of the organization, the review of all unauthorized access attempts could be very onerous. It is unclear from this requirement what the expectations and disposition of results of a review of unauthorized access are? What's the point of the review? This requirement should be more specific. This requirement contains data retention time of logs; that is also covered in the compliance section, D1.3.1. Probably should delete here to be consistent with other standards.	
006-R7		
006-M1		
006-M2		
006-M3		
006-M4		
006-M5		
006-M6		
006-M7		
006-C1,1		
006-C1,2		

006-C1,3	
006-C1,4	
006-C2,1	D2.1.2 Change to "aggregate interruptions at a single facility." Companies with many facilities should not be penalized for this by adding together the interruptions from each facility. As currently worded, a company with one facility that has interruptions of systems or data availability for thirty days and a company with 15 facilities that has lost only 2 days of data at each facility would be at the same level of non-compliance.
006-C2,2	D2.2.2 Change to "aggregate interruptions at a single facility." Companies with many facilities should not be penalized for this by adding together the interruptions from each facility. As currently worded, a company with one facility that has interruptions of systems or data availability for thirty days and a company with 15 facilities that has lost only 2 days of data at each facility would be at the same level of non-compliance
006-C2,3	D2.3.3 Change to “aggregate interruptions at a single facility.” Companies with many facilities should not be penalized for this by adding together the interruptions from each facility. As currently worded, a company with one facility that has interruptions of systems or data availability for thirty days and a company with 15 facilities that has lost only 2 days of data at each facility would be at the same level of non-compliance
006-C2,4	

CIP-006 Drafting Team Responses to Comments

Commentor	David McCoy	
Entity Name	Great Plains Energy/Kansas City Power & Light	
Ready to Ballot:	No	
General Comments		
006-R1		
006-R2	The words "any modification to any componets." should be removed. It is unreasonable to force updates of physical security plans for every equipment modification or wiring change.	It is not the intent of this requirement to be overbroad but to update the security plan with changes of a significant nature only. The wording within this requirement has been changed to add clarity, and the requirement has been moved under R1. Additionally an FAQ has been added to describe the intent of this requirement.
006-R3	The words "non-reproducable keys" should be changed to "difficult to reproduce keys." No keys are non reproducable.	The term has been changed to restricted key system. Refer to the FAQ.
006-R4		
006-R5		
006-R6		
006-R7		
006-M1		
006-M2		
006-M3		
006-M4		
006-M5		
006-M6		
006-M7		
006-C1,1		
006-C1,2		
006-C1,3		
006-C1,4		

CIP-006 Drafting Team Responses to Comments

006-C2,1

006-C2,2

006-C2,3

006-C2,4

CIP-006 Drafting Team Responses to Comments

Commentor	Patrick Miller	
Entity Name	PacifiCorp	
Ready to Ballot:	No	
General Comments		
006-R1	For R1.4, consider adding language that includes access mechanisms other than "access cards" such as physical keys, biometrics, etc.	R1.4 has been modified to include all access controls in R3.
006-R2		
006-R3		
006-R4		
006-R5		
006-R6		
006-R7		
006-M1		
006-M2		
006-M3		
006-M4		
006-M5		
006-M6		
006-M7		
006-C1,1		
006-C1,2		
006-C1,3		
006-C1,4		
006-C2,1		
006-C2,2		

006-C2,3

006-C2,4

CIP-006 Drafting Team Responses to Comments

Commentor	Don Miller
Entity Name	First Energy Corp
Ready to Ballot:	Yes
General Comments	
006-R1	
006-R2	
006-R3	
006-R4	
006-R5	
006-R6	
006-R7	
006-M1	
006-M2	
006-M3	
006-M4	
006-M5	
006-M6	
006-M7	
006-C1,1	
006-C1,2	
006-C1,3	
006-C1,4	
006-C2,1	
006-C2,2	
006-C2,3	
006-C2,4	

CIP-006 Drafting Team Responses to Comments

Commentor	Jeff Mitchell
Entity Name	ECAR
Ready to Ballot:	Yes
General Comments	
006-R1	
006-R2	
006-R3	
006-R4	
006-R5	
006-R6	
006-R7	
006-M1	
006-M2	
006-M3	
006-M4	
006-M5	
006-M6	
006-M7	
006-C1,1	
006-C1,2	
006-C1,3	
006-C1,4	
006-C2,1	
006-C2,2	
006-C2,3	
006-C2,4	

CIP-006 Drafting Team Responses to Comments

Commentor	Scott Mix	
Entity Name	KEMA, Inc	
Ready to Ballot:	No	
General Comments		
006-R1	While implied, Requirement R1 does not require ALL Critical Cyber Assets to be within the defined 6-wall boundary. This should be clearly stated. There should be a requirement in the Security Plan dealing with escorted access within the physical security perimeter.	By definition, the Physical Security Perimeter houses all Critical Cyber Assets. R1.1 has been modified to address processes to identify and document that all Cyber Assets within the Electronic Security Perimeter also reside within an identified Physical Security Perimeter. A sub-requirement has been added to R1 to address escorted access.
006-R2		
006-R3		
006-R4		
006-R5		
006-R6	Add "unless required as part of a Cyber Security Incident report as required in CIP-008 R2" to the end of the first sentence. Is a 2-month review cycle sufficient to detect and investigate an intrusion?	The requirement has been changed as suggested. Wording on the timeliness of review of unauthorized access attempts has been modified, and moved into R4.
006-R7		
006-M1		
006-M2		
006-M3		
006-M4		
006-M5		
006-M6		
006-M7		
006-C1,1		
006-C1,2		

CIP-006 Drafting Team Responses to Comments

006-C1,3

006-C1,4

006-C2,1

006-C2,2

006-C2,3

006-C2,4

CIP-006 Drafting Team Responses to Comments

Commentor	Darrick Moe	
Entity Name	WAPA	
Ready to Ballot:	No	
General Comments	It is evident from the answers in the FAQ (see #4, for example) that the intention is for all critical cyber assets to be within a Physical Security Perimeters (or a cage). However, the language of the Requirements themselves does not appear to explicitly state this requirement; this should be corrected.	By definition, the Physical Security Perimeter houses all Critical Cyber Assets. R1.1 has been modified to address processes to identify and document that all Cyber Assets within the Electronic Security Perimeter also reside within an identified Physical Security Perimeter.
006-R1	It should be clarified that dial-up cyber assets should be exempt from the Physical Security requirements (that is, from all of CIP-006). It is not clear what the current intention is, and the FAQs seem to add to the confusion; the desire is that cyber assets that are only dial-up accessible should be clearly exempt from Physical Security Requirements. To achieve this, modify R1.2. to read: "Measures to control access at all access points of the perimeter(s), and to protect the Critical Cyber Assets within them. For dial-up accessible Critical Cyber Assets that use non-routable protocols, the Responsible Entity shall not require a Physical Security Perimeter for that single access point at the dial-up device."	Modifications have been made to the additional compliance section to address this point.
006-R2		
006-R3		
006-R4		
006-R5		
006-R6		
006-R7		
006-M1		
006-M2		
006-M3		
006-M4		
006-M5		
006-M6		
006-M7		
006-C1,1		

CIP-006 Drafting Team Responses to Comments

006-C1,2

006-C1,3

006-C1,4

006-C2,1

006-C2,2

006-C2,3

006-C2,4

CIP-006 Drafting Team Responses to Comments

Commentor	Selby Mohr	
Entity Name	Sacramento Municipal Utility District	
Ready to Ballot:	Yes	
General Comments		
006-R1		
006-R2	within ninety days of any modifications to the physical security plan or any of its components. This wording will make it consistent with other similar references, such as Page 6 of 7 Section 2.1.1	The wording within this requirement has been changed to add clarity. Additionally, the requirement has been moved under R1.
006-R3		
006-R4		
006-R5	Page 4 of 7 - Section R5 - Last Sentence "Methods shall record sufficient information to uniquely identify individuals: Section R5.1 - Provide more clear guidance or words on expectations to comply, such as Individual's First Name, Last Name, Employee Number, ID verification, etc. Section R5.2 - Provide more clear guidance or words on expectations to comply, such as entry/exit time, Individual's First Name, Last Name, Employee Number, ID verification, etc. Be more explicit on compliance...name, etc. Section R5.3 - Add words to say "Video Recording: Electronic capture of video images that are of good quality and may be used for an investigation....	R5.The requirement is to obtain sufficient information to uniquely identify the individual. It is up to the Responsible Entity to determine the specific information required. R5.3 has been renumbered to R4.2 and now states video of sufficient quality to identify the individual.
006-R6	Page 5 of 7- Section R6 - Unauthorized access attempts shall be reviewed every two months. What do you do after the review? Is there some expected action? Maybe a Root Cause Analysis, preventive measures, and corrective actions, etc... It seems pretty slow/kick back to wait two months...It should be more timely like 1- 5 working days.	Wording on the timeliness of review of unauthorized access attempts has been modified, and moved into R4.
006-R7		
006-M1		
006-M2		
006-M3		
006-M4		
006-M5		

006-M6		
006-M7		
006-C1,1		
006-C1,2		
006-C1,3		
006-C1,4		
006-C2,1		
006-C2,2		
006-C2,3	Page 6 of 7- Section 2.3.2 - Add at the end of the sentence of a modification to the physical security plan or any of its components; or	The levels of noncompliance have been rewritten.
006-C2,4		

CIP-006 Drafting Team Responses to Comments

Commentor	Kurt Muehlbauer	
Entity Name	Exelon	
Ready to Ballot:	No	
General Comments	The documentation and processes around the responsible entity s tasks are too prescriptive. The industry needs to be extremely careful to avoid the creation of purely documentation-based non-compliances. With increasing legal requirements for compliance, and the associated penalties for noncompliance, noncompliance should be reserved for real security issues. It is simply too easy to make a mistake in documentation in light of the constantly evolving cyber environment. Each entity should develop its own processes in support of the requirements, and these processes should be required to contain provisions for periodic review and approval applicable to each requirement. The processes should also be required to produce reasonable documentation to demonstrate compliance. However, it is not necessary to specify the details of the documentation or review periods. The above approach can be met by removing references to documentation from the requirements section. Then, in the measures section require each entity to reasonably document programs and processes that support the security requirements and to produce reasonable documentation required to demonstrate compliance to the security requirements. Please refer to our overall comments on defining reasonable. If the above approach is taken, it will be possible to delete many of the sub-bullet points under each requirement (because the details will be specified by each entity in their program or process, as applicable). This will also ensure that documentation and excessive low-value administrative tasks are removed from the requirements.	The Drafting Team has reviewed the standards and removed prescription where possible. The prescriptiveness that remains is necessary to provide the clarity requested by a majority of commenters. The documentation required by these standards allow Responsible Entities to demonstrate that the policies, processes, and procedures that they have implemented consistently comply with the requirements of these standards.
006-R1	R1.1 Clarify wording to and all physical access points to Critical Cyber Assets R1.5 -- remove reviewing access authorization requests, revocation of access authorization, and which duplicates R4 of CIP-004 Might then need to reword or clarify the remaining portion of R1.5.	The requirement R1.5 has been clarified to indicate that the access authorization should be done in accordance with CIP-004. Please see the FAQs.
006-R2		
006-R3	R3. -- Delete the second sentence and delete R3.1 -- 3.3. Per the general comments to this standard, these sub points are too prescriptive. The entity should implement access controls consistent with its physical security plan.	Change has been made to allow for equivalent technology.
006-R4	R4.1 -- 4.3 Per general comments, these sub points are too prescriptive and should be removed. The entity should implement monitoring consistent with its physical security plan	Modifications to this section have been made to provide greater latitude regarding methods of monitoring as long as either human notification or observation is in place.
006-R5	R5.1 -- 5.3 Per general comments, these sub points are too prescriptive and should be	Change has been made to allow for equivalent technology.

	removed. The entity should implement logging consistent with its physical security plan	
006-R6	Delete R6. Please see the general comments to this standard for our rationale. In place of this statement, we recommend adding a general measure in the measures section to the affect, Each entity shall retain access logs for a period sufficient for auditing and investigations, and will	Please see response to General Comments, above.
006-R7	Remove R7.1 -- R7.3. Testing and maintenance of physical security components is the responsibility of each entity and should be consistent with their security program.	The current wording does not prohibit a Responsible Entity from implementing a maintenance and testing program consistent with its security plan. The intent is to define a set of minimum requirements for testing and for retention of documentation. An entity can decide to perform such testing more frequently if that meets the requirements of its security program as long as the security plan meets the minimum requirements of the standard.
006-M1	Refer to general, overall comments submitted on CIP-002 through CIP-009 regarding revision of the measures and compliance specification.	See response to General Comments, above.
006-M2	Refer to general, overall comments submitted on CIP-002 through CIP-009 regarding revision of the measures and compliance specification.	
006-M3	Refer to general, overall comments submitted on CIP-002 through CIP-009 regarding revision of the measures and compliance specification.	
006-M4	Refer to general, overall comments submitted on CIP-002 through CIP-009 regarding revision of the measures and compliance specification.	
006-M5	Refer to general, overall comments submitted on CIP-002 through CIP-009 regarding revision of the measures and compliance specification.	
006-M6	Refer to general, overall comments submitted on CIP-002 through CIP-009 regarding revision of the measures and compliance specification.	
006-M7	Refer to general, overall comments submitted on CIP-002 through CIP-009 regarding revision of the measures and compliance specification.	
006-C1,1	Refer to general, overall comments submitted on CIP-002 through CIP-009 regarding revision of the measures and compliance specification.	
006-C1,2	Refer to general, overall comments submitted on CIP-002 through CIP-009 regarding revision of the measures and compliance specification.	
006-C1,3	Refer to general, overall comments submitted on CIP-002 through CIP-009 regarding revision of the measures and compliance specification.	
006-C1,4	Refer to general, overall comments submitted on CIP-002 through CIP-009 regarding revision of the measures and compliance specification.	
006-C2,1	Refer to general, overall comments submitted on CIP-002 through CIP-009 regarding revision of the measures and compliance specification.	
006-C2,2	Refer to general, overall comments submitted on CIP-002 through CIP-009 regarding revision of the measures and compliance specification.	

CIP-006 Drafting Team Responses to Comments

006-C2,3 Refer to general, overall comments submitted on CIP-002 through CIP-009 regarding revision of the measures and compliance specification.

006-C2,4 Refer to general, overall comments submitted on CIP-002 through CIP-009 regarding revision of the measures and compliance specification.

CIP-006 Drafting Team Responses to Comments

Commentor	Jeffrey Mueller	
Entity Name	PSEG Companies	
Ready to Ballot:	No	
General Comments	The PSEG Companies have reviewed and share the concerns expressed in the Comments of PJM and EEI. Accordingly, the PSEG Companies support the comments of PJM and EEI, and request that the concerns expressed in those comments be properly addressed in the next version of the draft standard.	Please see responses to Laurence W. Brown, Edison Electric Institute.
006-R1		
006-R2		
006-R3		
006-R4		
006-R5		
006-R6		
006-R7		
006-M1		
006-M2		
006-M3		
006-M4		
006-M5		
006-M6		
006-M7		
006-C1,1		
006-C1,2		
006-C1,3		
006-C1,4		
006-C2,1		

006-C2,2

006-C2,3

006-C2,4

CIP-006 Drafting Team Responses to Comments

Commentor	Mitchell Needham	
Entity Name	Tennessee Valley Authority	
Ready to Ballot:	No	
General Comments		
006-R1		
006-R2		
006-R3		
006-R4		
006-R5	Using Video recording would be difficult as an entity would have to retain all such video for at least 90 days.	A 30 day time period is too short due to the risk of losing data that may be required in an investigation. 90 days is a reasonable period for forensic purposes to allow for potential delay in discovery or investigation of an event. An entity may also choose to keep such logs longer as they deem appropriate. Additional concerns were voiced with regards to the difficulty of keeping video for 90 days, however with modern DVR (digital video recording) systems retaining video has become much more cost effective.
006-R6		Please see response in CIP-007.
006-R7		
006-M1		
006-M2		
006-M3		
006-M4		
006-M5		
006-M6		
006-M7		
006-C1,1		
006-C1,2		
006-C1,3		

CIP-006 Drafting Team Responses to Comments

006-C1,4

006-C2,1

006-C2,2

006-C2,3

006-C2,4

CIP-006 Drafting Team Responses to Comments

Commentor	Dave Norton	
Entity Name	Entergy Transmission	
Ready to Ballot:	No	
General Comments		
006-R1		
006-R2		
006-R3	R3 and R4: Since each Responsible Entity is required to "implement one of more of the following ...", shouldn't R3.1 -- R3.4 really just be bullets? They are not individual sub-requirements, but rather are options.	The format of the standard requires these to be numbered.
006-R4	R3 and R4: Since each Responsible Entity is required to "implement one of more of the following ...", shouldn't R3.1 -- R3.4 really just be bullets? They are not individual sub-requirements, but rather are options.	The format of the standard requires these to be numbered.
006-R5		
006-R6		
006-R7		
006-M1		
006-M2		
006-M3		
006-M4		
006-M5		
006-M6		
006-M7		
006-C1,1		
006-C1,2		
006-C1,3		
006-C1,4		
006-C2,1		

006-C2,2

006-C2,3

006-C2,4

CIP-006 Drafting Team Responses to Comments

Commentor	Doug Orlofske
Entity Name	Wisconsin Public Power Inc
Ready to Ballot:	Yes
General Comments	
006-R1	
006-R2	
006-R3	
006-R4	
006-R5	
006-R6	
006-R7	
006-M1	
006-M2	
006-M3	
006-M4	
006-M5	
006-M6	
006-M7	
006-C1,1	
006-C1,2	
006-C1,3	
006-C1,4	
006-C2,1	
006-C2,2	
006-C2,3	
006-C2,4	

CIP-006 Drafting Team Responses to Comments

Commentor	Kevin Perry	
Entity Name	Southwest Power Pool	
Ready to Ballot:	No	
General Comments		
006-R1	R1.1: The six-wall boundary should be clarified to mean "concrete-to-concrete" with no gaps, such as a wall terminating at the false ceiling.	Please refer to FAQs for discussion of six-wall border.
006-R2		
006-R3		
006-R4	Does R4.1 imply that a human is constantly monitoring the output of the video cameras 24x7? In FAQ that accompanied the draft standards, the comment is made that the video feed can be displayed at a dispatcher desk. While there is a human working at that desk, it is unreasonable to expect that the disatcher will be paying close attention, if any attention, to the video monitor. The only alternative is to have a security station with a guard in duty 24x7 to constantly monitor the video camera feed. For small entities, this may be unreasonably expensive. R4.2 requires that a card access controlled door must not only be badged to get in, but also to exit. Otherwise, there is not way to distinguish between an authorized and unauthorized door opening. This violates fire code standards in many locales in that the requirement is to provide easy, unimpeded egress from a room or building in an emergency. The mitigation would be to install alarmed crash bars on all secured doors, and possibly replace the existing security systems due to incompatability with crash bars. This would be an expensive proposition, especially with the requirement to alarm back to a central monitoring station.	Specific requirements for video monitoring have been removed. However, if an entity chooses to use video for 24x7 monitoring, then it is reasonable to assume it will be adequately monitored. The alarm system is meant to alert on forced entry, or entry without corresponding authentication. Typically, exit is assumed to be authorized. Sensors may be able to determine authorized access based upon the receipt of an authorized code, via a cardkey or entered at a keypad, for example. In the case where they cannot, such as when an entity installs an alarm system without a local authentication mechanism, then procedural controls at the monitoring station must be in place to authenticate access.
006-R5		
006-R6	The requirement to review unauthorized attempts every two months is not reasonable for sites with proximity card readers. The mere act of walking past a sensor often logs an "attempt" whether or not there was a real attempt to enter the controlled space, authorized or not. Likewise, reviewing two months of video tapes is an unreasonable burden on most entities. If the requirement is for 24x7 human monitoring of the physical access control points, then a secondary review is unnecessary.	Wording on the timeliness of review of unauthorized access attempts has been modified, and moved into R4.
006-R7	R7.1: Testing of physical access controls should take place much more frequently than once per year.	The current wording does not prohibit a Responsible Entity from implementing a maintenance and testing program consistent with its security plan. The intent is to define a set of minimum requirements for testing and for retention of documentation. An entity can decide to perform such testing more frequently if that meets the requirements of its security program as long as the security plan meets the minimum requirements of the standard.

006-M1		
006-M2		
006-M3		
006-M4		
006-M5		
006-M6		
006-M7		
006-C1,1		
006-C1,2		
006-C1,3		
006-C1,4	Approval of exceptions to the requirements should not be delegated.	Exceptions cannot be taken to NERC standards. It is up to Responsible Entities to define policies, exception handling, and delegation authority.
006-C2,1	C2.1.2: As logs are to be kept only for 90 days, there is no way to verify compliance with this requirement.	Record keeping related to the loss of logging data has been added to requirement R6 to allow for compliance measurement with this section.
006-C2,2	C2.2.2: As logs are to be kept only for 90 days, there is no way to verify compliance with this requirement.	Record keeping related to the loss of logging data has been added to requirement R6 to allow for compliance measurement with this section.
006-C2,3	C2.3.3: As logs are to be kept only for 90 days, there is no way to verify compliance with this requirement.	Record keeping related to the loss of logging data has been added to requirement R6 to allow for compliance measurement with this section.
006-C2,4		

CIP-006 Drafting Team Responses to Comments

Commentor Tom Pruitt

Entity Name Duke Power Company

Ready to Ballot: No

General Comments	A.4.1 -- Given the critical role of the PSE, why are these standards not applicable to that entity? A.4.2.2 -- Appears to be inconsistent with definition of "Cyber Asset". A.5 -- This should reference the proposed Implementation Plan. Alternatively, the compliance implementation plan should be referenced in the compliance sections for all of CIP002 thru CIP 009.	The standards reflect the Standard Authorization Request (SAR), which excluded PSEs. The drafting team must respect the scope of the SAR and not extend it during standards development. The SAR reflects industry consensus on the scope of the standard to be developed. The SAR also specifically excluded communication links. Although reviewed and voted upon by the industry, the Implementation Plan is not part of the standard and cannot be referenced therein.
006-R1	R1 -- Clarify that this response plan must be approved by a level of management. R1.1 -- Use of "boundary" is inconsistent terminology. Previous wording is "border" in definition of terms above. "Boundary" should be the preferred term.	R1 requires that the physical security plan must be approved by a senior manager. The terminology has been changed to match the definition.
006-R2		
006-R3		
006-R4		
006-R5		
006-R6	R6 -- Suggest changing review of unauthorized access attempt to every 90 days to align with other requirements through out CIP 002-009.	Wording on the timeliness of review of unauthorized access attempts has been modified, and moved into R4.
006-R7		
006-M1		
006-M2		
006-M3		
006-M4		
006-M5		
006-M6		
006-M7		

CIP-006 Drafting Team Responses to Comments

006-C1,1		
006-C1,2		
006-C1,3		
006-C1,4	1.4.1 -- Provide clarification as to when an entity may allow an exemption. For instance, would an event as described in R7.2 constitute an exemption event? Add senior management approval of plan to R1.	Exceptions cannot be taken to NERC standards. It is up to Responsible Entities to define policies and exception handling. See Additional Compliance Information, Section D1.4.2.
006-C2,1		
006-C2,2		
006-C2,3		
006-C2,4		

CIP-006 Drafting Team Responses to Comments

Commentor	Duane Radzwion
Entity Name	Consumers Energy
Ready to Ballot:	Yes
General Comments	
006-R1	
006-R2	
006-R3	
006-R4	
006-R5	
006-R6	
006-R7	
006-M1	
006-M2	
006-M3	
006-M4	
006-M5	
006-M6	
006-M7	
006-C1,1	
006-C1,2	
006-C1,3	
006-C1,4	
006-C2,1	
006-C2,2	
006-C2,3	
006-C2,4	

CIP-006 Drafting Team Responses to Comments

Commentor	Howard Rulf	
Entity Name	We Energies	
Ready to Ballot:	No	
General Comments	R1-7 (Most Sections) Due to the nature of a plant's Distributed Control System (DCS) component placement it will be very costly to physically secure all system devices on multiple DCS networks if they employ routable protocol.	Instances where a Responsible Entity is unable to meet the requirement to place equipment in an enclosure as required, it can write an exception to its own security policies (see CIP-003). A Responsible Entity's duly authorized exception will not result in non-compliance, as noted in the Additional Compliance section of this standard.
006-R1	R1.6: There needs to be an allowance for unauthorized visitors to be admitted under the escort of an authorized person. Add the following to R1.6: R1.6 A means for logging the identification, approval, entry and exit of an unauthorized visitor who is under the escort of an authorized individual. Such escorted visitors may be admitted only for a business purpose and their manipulation of critical cyber assets must be prevented, unless their presence is for the purpose of intervention with the critical cyber assets in an emergency condition on behalf of an authorized individual.	Escorted access has been incorporated into R1.6.
006-R2		
006-R3		
006-R4		
006-R5		
006-R6		
006-R7		
006-M1		
006-M2		
006-M3		
006-M4		
006-M5		
006-M6		
006-M7		
006-C1,1		

CIP-006 Drafting Team Responses to Comments

006-C1,2

006-C1,3

006-C1,4

006-C2,1

006-C2,2

006-C2,3

006-C2,4

CIP-006 Drafting Team Responses to Comments

Commentor	Randy Schimka
Entity Name	San Diego Gas and Electric Co.
Ready to Ballot:	Yes
General Comments	
006-R1	
006-R2	
006-R3	
006-R4	
006-R5	
006-R6	
006-R7	
006-M1	
006-M2	
006-M3	
006-M4	
006-M5	
006-M6	
006-M7	
006-C1,1	
006-C1,2	
006-C1,3	
006-C1,4	
006-C2,1	
006-C2,2	
006-C2,3	
006-C2,4	

CIP-006 Drafting Team Responses to Comments

Commentor	Lyman Shaffer	
Entity Name	PG&E	
Ready to Ballot:	Yes	
General Comments		
006-R1		
006-R2		
006-R3		
006-R4		
006-R5		
006-R6	The standard states that "unauthorized access attempts shall be reviewed every two months." This seems burdensome to check that many card swipes.	Wording on the timeliness of review of unauthorized access attempts has been modified, and moved into R4.
006-R7		
006-M1		
006-M2		
006-M3		
006-M4		
006-M5		
006-M6		
006-M7		
006-C1,1		
006-C1,2		
006-C1,3		
006-C1,4		
006-C2,1		
006-C2,2		

006-C2,3

006-C2,4

CIP-006 Drafting Team Responses to Comments

Commentor	Neil Shockey
Entity Name	Southern California Edison
Ready to Ballot:	Yes
General Comments	
006-R1	
006-R2	
006-R3	
006-R4	
006-R5	
006-R6	
006-R7	
006-M1	
006-M2	
006-M3	
006-M4	
006-M5	
006-M6	
006-M7	
006-C1,1	
006-C1,2	
006-C1,3	
006-C1,4	
006-C2,1	
006-C2,2	
006-C2,3	
006-C2,4	

CIP-006 Drafting Team Responses to Comments

Commentor	William Smith	
Entity Name	Allegheny Power	
Ready to Ballot:	No	
General Comments	1.--The answer to FAQ 11 contains information that should be clearly stated within the body of the standard. Furthermore, the lack of a requirement for a physical security perimeter for dial-up Critical Cyber Assets, such as a relay at a substation, should be extended to IP-based Critical Cyber Assets installed in substations in the case where the local electronic security perimeter and it’s associated access points (substation firewalls) fall completely within the 6 wall boundary comprised of the substation control building. The following information should be added under section D 1.4: a.--"Critical Cyber Assets with dial-up access not using a routable protocol must meet the Electronic Security Perimeter requirements for the remote access to that device but does not require a Physical Security Perimeter or local Electronic Security Perimeter for the actual Critical Cyber Asset. Secure remote access meets the intent of the Cyber Security Standards to provide a minimum level of security." b.--"Critical Cyber Assets located at substations in which the local electronic security perimeter and its associated electronic access points are completely contained within the substation control building must meet the Electronic Security Perimeter requirements for remote access to the Critical Cyber Assets, but not the requirements for a Physical Security Perimeter. Secure remote access meets the intent of the Cyber Security Standards to provide a minimum level of security."	1.a. The suggestion is reflected in changes to the Additional Compliance Section. 1.b. In this case the Physical Security Perimeter must be in place, and the substation control building becomes the Physical Security Perimeter through which access must be controlled.
006-R1	R1.1. -- What ultimately determines when a security enclosure is required for field devices connected to a critical cyber asset? Does the field device have to provide an interactive access point to the asset? R1.3. -- How do you expect entities to monitor field device enclosures for physical access if lock & key is the enclosure’s security measure? R1.4. -- Revise the term "piggybacking" to "tailgating".	R1.1 If the field device is identified as a Critical Cyber Asset or is within the Electronic Security Perimeter, it will require a completely enclosed border. R1.3 The Responsible Entity retains the flexibility to determine how to implement the requirements of this standard using reasonable business judgment. R1.4 The term piggybacking has been removed.
006-R2		
006-R3		
006-R4		
006-R5		
006-R6		

CIP-006 Drafting Team Responses to Comments

006-R7

006-M1

006-M2

006-M3

006-M4

006-M5

006-M6

006-M7

006-C1,1

006-C1,2

006-C1,3

006-C1,4

006-C2,1

006-C2,2

006-C2,3

006-C2,4

CIP-006 Drafting Team Responses to Comments

Commentor	Paul Sorenson
Entity Name	Open Access Technology International
Ready to Ballot:	Yes
General Comments	
006-R1	
006-R2	
006-R3	
006-R4	
006-R5	
006-R6	
006-R7	
006-M1	
006-M2	
006-M3	
006-M4	
006-M5	
006-M6	
006-M7	
006-C1,1	
006-C1,2	
006-C1,3	
006-C1,4	
006-C2,1	
006-C2,2	
006-C2,3	
006-C2,4	

CIP-006 Drafting Team Responses to Comments

Commentor	Robert Strauss	
Entity Name	NYSEG	
Ready to Ballot:	No	
General Comments		
006-R1	Requirement R1.4 is too prescriptive. R3 covers several possible access devices.	Please see responses to Ray A'Brial, Central Hudson Gas & Electric Corp.
006-R2		
006-R3	R3 should read, "the Responsible Entity shall document and implement ....". Otherwise, M 3 establishes a new requirement not identified in the Requirements section of the Standard. R3.1 - R3.4 are too prescriptive. They should be removed. R3 changes to "Physical Access Controls - The Responsible Entity shall document and implement the organizational, operational and procedural controls to manage physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day , seven days a week."	
006-R4	R4 should read, "the Responsible Entity shall document and implement ....". Otherwise, M 4 establishes a new requirement not identified in the Requirements section of the Standard. R4.1 - R4.3 are too prescriptive. They should be removed. R4 should read "Monitoring Physical Access - The Responsible Entity shall document and implement the organizational, technical and procedural controls for monitoring physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day , seven days a week."	
006-R5	R5 should read, "the Responsible Entity shall document and implement ....". Otherwise, M5 establishes a new requirement not identified in the Requirements section of the Standard. R5.1 - R5.3 are too prescriptive. They should be removed. R5 should read "Logging Physical Access - The Responsible Entity shall document and implement the organizational, technical and procedural mechanisms for logging and reviewing physical access at all access points to the Physical Security Perimeter(s). Methods shall record sufficient information to uniquely identify individuals and datetime stamps."	
006-R6	We recommend changing from "at least 90 calendar days" to "at least 30 calendar days". The log should be reviewed before it is dropped. Also, retaining video can be very be expensive with little benefit. The statement "Unauthorized access attempts shall be reviewed every two months.", doesn't	

	appear to be accomplishing the desired objective of being cognizant, in a timely manner, of attempted unauthorized access. The drafting team should discuss and clarify their intent or remove the statement.	
006-R7		
006-M1		
006-M2		
006-M3		
006-M4		
006-M5		
006-M6		
006-M7		
006-C1,1		
006-C1,2		
006-C1,3	To remain consistent with R6, this "ninety days" should change to "30 days".	Please refer to response to comment on R6.
006-C1,4		
006-C2,1		
006-C2,2		
006-C2,3	In Compliance statement 2.3.1, please clarify what is meant by “record”. If the reference is really to a “document”, then Compliance statement 2.3.1 appears to contradict Compliance statement 2.4.3 in cases where one of the missing documents is the security plan. Note also that no non-compliance level has been defined for cases where one required document (or record) is missing unless that document is the security plan.	
006-C2,4		

CIP-006 Drafting Team Responses to Comments

Commentor	Karl Tammar	
Entity Name	IRC	
Ready to Ballot:	No	
General Comments		
006-R1		
006-R2		
006-R3	R3 should read, "the Responsible Entity shall document and implement ....". Otherwise, M 3 establishes a new requirement not identified in the Requirements section of the Standard.	The requirement has been modified as suggested.
006-R4	R4 should read, "the Responsible Entity shall document and implement ....". Otherwise, M 4 establishes a new requirement not identified in the Requirements section of the Standard.	The requirement has been modified as suggested.
006-R5	R5 should read, "the Responsible Entity shall document and implement ....". Otherwise, M 5 establishes a new requirement not identified in the Requirements section of the Standard.	The requirement has been modified as suggested.
006-R6		
006-R7		
006-M1		
006-M2		
006-M3		
006-M4		
006-M5		
006-M6		
006-M7		
006-C1,1		
006-C1,2		
006-C1,3		
006-C1,4		
006-C2,1		

CIP-006 Drafting Team Responses to Comments

006-C2,2		
006-C2,3	4.In Compliance statement 2.3.1, please clarify what is meant by “record”. If the reference is really to a “document”, then Compliance statement 2.3.1 appears to contradict Compliance statement 2.4.3 in cases where one of the missing documents is the security plan. Note also that no non-compliance level has been defined for cases where one required document (or record) is missing unless that document is the security plan.	The levels of noncompliance have been rewritten and reference to record has been removed.
006-C2,4	4.--In Compliance statement 2.3.1, please clarify what is meant by "record". If the reference is really to a "document", then Compliance statement 2.3.1 appears to contradict Compliance statement 2.4.3 in cases where one of the missing documents is the security plan. Note also that no non-compliance level has been defined for cases where one required document (or record) is missing unless that document is the security plan.	The levels of noncompliance have been rewritten and reference to record has been removed.

CIP-006 Drafting Team Responses to Comments

Commentor	Todd Thompson	
Entity Name	PJM Interconnection	
Ready to Ballot:	No	
General Comments		
006-R1		
006-R2		
006-R3	R3 should read, "the Responsible Entity shall document and implement ....". Otherwise, M 3 establishes a new requirement not identified in the Requirements section of the Standard.	The requirement has been modified as suggested.
006-R4	R4 should read, "the Responsible Entity shall document and implement ....". Otherwise, M 4 establishes a new requirement not identified in the Requirements section of the Standard.	The requirement has been modified as suggested.
006-R5	R5 should read, "the Responsible Entity shall document and implement ....". Otherwise, M 5 establishes a new requirement not identified in the Requirements section of the Standard.	The requirement has been modified as suggested.
006-R6		
006-R7		
006-M1		
006-M2		
006-M3		
006-M4		
006-M5		
006-M6		
006-M7		
006-C1,1		
006-C1,2		
006-C1,3		
006-C1,4		
006-C2,1		

006-C2,2		
006-C2,3	In Compliance statement 2.3.1, please clarify what is meant by “record”. If the reference is really to a “document”, then Compliance statement 2.3.1 appears to contradict Compliance statement 2.4.3 in cases where one of the missing documents is the security plan. Note also that no non-compliance level has been defined for cases where one required document (or record) is missing unless that document is the security plan.	The levels of noncompliance have been rewritten and reference to record has been removed.
006-C2,4		

CIP-006 Drafting Team Responses to Comments

Commentor	Steven Townsend	
Entity Name	Consumers Energy Co.	
Ready to Ballot:	No	
General Comments	Consumers Energy has also submitted comments via the ECAR CIPP.	Please see responses to Larry Conrad, ECAR CIPP.
006-R1		
006-R2		
006-R3		
006-R4		
006-R5		
006-R6		
006-R7		
006-M1		
006-M2		
006-M3		
006-M4		
006-M5		
006-M6		
006-M7		
006-C1,1		
006-C1,2		
006-C1,3		
006-C1,4		
006-C2,1		
006-C2,2		
006-C2,3		
006-C2,4		

CIP-006 Drafting Team Responses to Comments

Commentor	Martin Trence
Entity Name	Xcel Energy - Northen States Power (NSP)
Ready to Ballot:	No

General Comments

006-R1	Installations exist that due to NESC (National Electric Safety Code) issues preclude a "six wall" approach to identifying a Physical Security Perimeter. Though the requirement has a caveat for the inability to create a six wall boundary, it is incomplete in regards to identification and verbage where such caveats exercised would be in compliance with this requirement and subsequently the standard. The requirement should be revised accordingly.	The drafting team expects that any implementation of these standards will take into consideration all applicable safety codes and does not feel that these requirements will preclude compliance.
006-R2		
006-R3	R3.2 Please rephrase the first part to read: "These may include mechanical locks, as part of door hardware or padlocks with non-reproducible keys as long as they have restricted key ways and classified as lick or tamper resistant". In the last part of the requirement, the concept of a man-trap in regards to double locks is misleading, assuming a padlock scheme, since the premise is that one door (or gate) must be closed before the oher door (or gate) can be opened. Please correct the language in the requirement as stated. R3.3 - On-site and centrally monitored are not equivalents in this requirement. Centrally monitored station personnel require additional infrastructure to effectively perform the function intended by this requirement, but is not stated as such in the requirement. Please correct this deficiency. R3.4 - Overlaps with R3.1 as Card Keys are a form of personnel authentication. The folllowing is recommended to replace R3.1: "An electronic access control system where access rights of the cardholder are predefined in a computer database. Access rights may differ from one perimeter to another. Means of authentications include, but are not limited to an access card(proximity, magnetic stripe, wiegand wire, contactless smart card etc.) or biometrics (fingerprint, hand geometry, etc), keypads or other devices that are used to authenticate." R3.4 should then be deleted. An additional recommendation may be to consider 2 factor authentication (e.g. Card + Pin number) especially when dealing with remote sites. The requirement as presently written appears to accept 1 factor authentication at this time	The requirement has been changed to refer to restricted key systems, which is further explained in the FAQs. It is not the intent of this requirement to force Responsible Entities to create additional infrastructure to allow for central monitoring. From a control standpoint, these methods (on-site vs central) are equivalent. It is a Responsible Entity's responsibility to decide which to implement based upon its own infrastructure requirements. Card keys are listed separately because they are the most common form of controlling physical access. The requirement relating to Other Authentication Devices provides for alternatives. Dual authentication meets this requirement, however, the drafting team feels that it is up individual entities to determine if they wish to implement this level of control.
006-R4		
006-R5	Reformat R5.1, R5.2, and R5.3 to align with R4.1, R4.2, and R4.3, as they are related to each other, and would provide greater clarity.	Modifications have been made.
006-R6		
006-R7		

CIP-006 Drafting Team Responses to Comments

006-M1

006-M2

006-M3

006-M4

006-M5

006-M6

006-M7

006-C1,1

006-C1,2

006-C1,3

006-C1,4

006-C2,1

006-C2,2

006-C2,3

006-C2,4

CIP-006 Drafting Team Responses to Comments

Commentor	Rick Vermeers
Entity Name	Avistacorp
Ready to Ballot:	Yes
General Comments	
006-R1	
006-R2	
006-R3	
006-R4	
006-R5	
006-R6	
006-R7	
006-M1	
006-M2	
006-M3	
006-M4	
006-M5	
006-M6	
006-M7	
006-C1,1	
006-C1,2	
006-C1,3	
006-C1,4	
006-C2,1	
006-C2,2	
006-C2,3	
006-C2,4	

CIP-006 Drafting Team Responses to Comments

Commentor	Robert C. Webb	
Entity Name	Instrumentation, Systems and Automation Society	
Ready to Ballot:	No	
General Comments	1. Who is ISA and Why is ISA commenting on CIP-002 through CIP-009?	Regarding comment #2a, the exclusionary language concerning generation assets has been removed with the exception of nuclear generation which is excluded by the SAR. Because distribution assets are not considered part of the Bulk Electric System, these resources remain excluded as well. Regarding comment #2b, much of the prescriptive language on how certain security measures should be applied has been removed. For example, the requirement for port scans in CIP 005, R4.2 has been replaced by a requirement to review only ports and services required for operations are enabled. In addition, the Drafting Team has removed most references to "how" security measures should be applied throughout the Standards unless it is required for compliance purposes. Regarding comment #2c, language has been added to reflect the fact that some security solutions that are available today were not available when some legacy systems were designed and put into service. CIP-003, CIP- 004, CIP-005, and CIP-006 contain language addressing exceptions to their policies that may be required to deal with legacy systems and facilities where modern security solutions are not technically possible. In these cases, the Responsible Entities must identify and document the exception and describe the mitigating steps they are taking to secure the assets in lieu of the modern solution. Regarding the comments #3, #4, and #5 related to scope, the Standard reflects the Standard Authorization Request which excluded distribution, nuclear generation, and telecommunication infrastructure. The Drafting Team cannot exceed the scope of the SAR. A SAR reflects the industry consensus on the scope of any particular standard to be developed. Once SAR has been approved for standards drafting, the scope cannot be changed. The NERC Reliability Standards process would require new SARs to address these scope issues.

CIP-006 Drafting Team Responses to Comments

006-R1

006-R2

006-R3

006-R4

006-R5

006-R6

006-R7

006-M1

006-M2

006-M3

006-M4

006-M5

006-M6

006-M7

006-C1,1

006-C1,2

006-C1,3

006-C1,4

006-C2,1

006-C2,2

006-C2,3

006-C2,4

CIP-006 Drafting Team Responses to Comments

Commentor Laurent Webber

Entity Name Western Area Power Administration

Ready to Ballot: No

General Comments	Critical Cyber Assets that are only dial-up accessible should be exempted from these physical security controls.	Critical Cyber Assets that do not use routable protocols and are dial-up accessible are addressed in the additional compliance section.
006-R1	R1.1: This never specifically states that the physical security perimeter is to enclose all Critical Cyber Assets. Reword to say "Clearly identified Physical Security Perimeter(s) around all Critical Cyber Assets and all physical access points to such perimeters."	By definition, the Physical Security Perimeter houses all Critical Cyber Assets. R1.1 has been modified to address processes to identify and document that all Cyber Assets within the Electronic Security Perimeter also reside within an identified Physical Security Perimeter.
006-R2		
006-R3	R3: The definition of "access points" is not established or differentiated between doors and windows. This requirement dictates special locks and authentication for "all access points." It is unreasonable to require such controls at windows or other access points not normally used for physical access.	Although not normally used for entry, windows are physical access points. They are potential points of entry into a facility just like doors and should not be differentiated in this respect.
006-R4	R4.2: The term "without authorization" implies that the door and gate alarms must differentiate between authorized and unauthorized access. This is not always possible and your examples, "door contacts, window contacts, and motion sensors", cannot differentiate between authorized and unauthorized access. Remove the term "without authorization."	Sensors may be able to determine authorized access based upon the receipt of an authorized code, via a cardkey or entered at a keypad, for example. In the case where they cannot, such as when an entity installs an alarm system without a local authentication mechanism, then procedural controls at the monitoring station must be in place to authenticate access.
006-R5		
006-R6		
006-R7		
006-M1		
006-M2		
006-M3		
006-M4		
006-M5		
006-M6		
006-M7		

CIP-006 Drafting Team Responses to Comments

006-C1,1

006-C1,2

006-C1,3

006-C1,4

006-C2,1

006-C2,2

006-C2,3

006-C2,4

Commentor	Michal Zeithammel	
Entity Name	Brascan Power	
Ready to Ballot:	No	
General Comments	Assuming that we had 3 buildings (6 wall physical security perimeter) within a fenced in (5 wall physical security perimeter with monitoring, access control, etc), all three buildings with critical cyber equipment that needs to be interconnected. The way we read the standard, we would need to have a firewall-like device at the electronic access point to every building. Is this the intent of the standard? If it is in fact NERC's intent, Brascan Power recommends that the wording be clarified to specifically say that all critical cyber assets and all the other cyber assets on the same routable network segment (i.e., within an electronic security perimeter) must fully be located within one 6-wall physical security perimeter.	It is not the intent to require Responsible Entities to install multiple firewalls: The ESP can cross multiple physical locations and have just one access control device. Nor is it the intent to require Responsible Entities to implement a single Physical Security Perimeter.
006-R1		
006-R2		
006-R3		
006-R4		
006-R5		
006-R6		
006-R7		
006-M1		
006-M2		
006-M3		
006-M4		
006-M5		
006-M6		
006-M7		
006-C1,1		
006-C1,2		
006-C1,3		

CIP-006 Drafting Team Responses to Comments

006-C1,4

006-C2,1

006-C2,2

006-C2,3

006-C2,4

CIP-006 Drafting Team Responses to Comments

Commentor	Guy Zito	
Entity Name	NPCC	
Ready to Ballot:	No	
General Comments		
006-R1	Requirement R1.4 is too prescriptive. R3 covers several possible access devices.	Please see responses to Ray A'Brial, Central Hudson Gas & Electric Corp.
006-R2		
006-R3	R3 should read, "the Responsible Entity shall document and implement ....". Otherwise, M 3 establishes a new requirement not identified in the Requirements section of the Standard. R3.1 - R3.4 are too prescriptive. They should be removed. R3 changes to "Physical Access Controls - The Responsible Entity shall document and implement the organizational, operational and procedural controls to manage physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day , seven days a week."	
006-R4	R4 should read, "the Responsible Entity shall document and implement ....". Otherwise, M 4 establishes a new requirement not identified in the Requirements section of the Standard. R4.1 - R4.3 are too prescriptive. They should be removed. R4 should read "Monitoring Physical Access - The Responsible Entity shall document and implement the organizational, technical and procedural controls for monitoring physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day , seven days a week."	
006-R5	R5 should read, "the Responsible Entity shall document and implement ....". Otherwise, M5 establishes a new requirement not identified in the Requirements section of the Standard. R5.1 - R5.3 are too prescriptive. They should be removed. R5 should read "Logging Physical Access - The Responsible Entity shall document and implement the organizational, technical and procedural mechanisms for logging and reviewing physical access at all access points to the Physical Security Perimeter(s). Methods shall record sufficient information to uniquely identify individuals and datetime stamps."	
006-R6	We recommend changing from "at least 90 calendar days" to "at least 30 calendar days". The log should be reviewed before it is dropped. Also, retaining video can be very be expensive with little benefit. The statement "Unauthorized access attempts shall be reviewed every two months.", doesn't	

appear to be accomplishing the desired objective of being cognizant, in a timely manner, of attempted unauthorized access. The drafting team should discuss and clarify their intent or remove the statement.

006-R7

006-M1

006-M2

006-M3

006-M4

006-M5

006-M6

006-M7

006-C1,1

006-C1,2

006-C1,3 To remain consistent with R6, this "ninety days" should change to "30 days".

006-C1,4

006-C2,1

006-C2,2

006-C2,3 In Compliance statement 2.3.1, please clarify what is meant by "record". If the reference is really to a "document", then Compliance statement 2.3.1 appears to contradict Compliance statement 2.4.3 in cases where one of the missing documents is the security plan. Note also that no non-compliance level has been defined for cases where one required document (or record) is missing unless that document is the security plan.

006-C2,4

CIP-007 Drafting Team Responses to Comments

Name	Raymond A'Brial	
Entity	Central Hudson Gas & Electric Corp	
Ready to Ballot	No	
General Comments	Remove the first sentence of the purpose since it is redundant with the rest of the purpose. We prefer the second and third sentence of the purpose.	The purpose has been reworded.
	For consistency, this Standard should include an Applicability 4.2.3, "Responsible Entities that, in compliance with CIP-002, identify that they have no Critical Cyber Assets."	Applicability section 4.2.3 has been added.
007-R1	The wording of R1 requires clarification given that some requirements in this standard refer specifically to Critical Cyber Assets rather than to the more generic "cyber assets". For instance, R8 requires data destruction or removal prior to disposal of a Critical Cyber Asset. On one hand, the wording of R1 could be taken to mean that one should replace the words "Critical Cyber Assets" by the words "Critical and Non-Critical Cyber Assets" when interpreting the standard. Under this interpretation, the Responsible Entity should wipe data on all assets prior to disposal. Alternatively, one could argue that the wording of R8 explicitly excludes non-critical cyber assets, and therefore failure to consider wipe data from non-critical cyber assets does not give rise to non-compliance. Please clarify.	The drafting team has clarified that all requirements in CIP-007 apply to both Critical and non-critical Cyber Assets in the Electronic Security Perimeter.
007-R2	Request clarification on R2. Does this Standard apply to Critical Cyber Assets or Cyber Assets?	The drafting team has clarified that all requirements in CIP-007 apply to both Critical and non-critical Cyber Assets within the Electronic Security Perimeter.
	For clarification, change to "security patches, cumulative service packs, vendor releases, or version upgrades as applied to operating systems, applications, database platforms, or other third-party software or firmware."	R2 has been renumbered to R1 and reworded for clarity as suggested.
007-R3		
007-R4		
007-R5		
007-R6	R6.1.5 is not clear. This should be rewritten or removed	R6 has been rewritten and renumbered to R5.
007-R7		
007-R8		
007-R9		
007-R10		
007-M1		

007-M2	Measures M2.1, M2.2 and M2.3 should be rephrased as measures	The measures have been rewritten to reference back to the requirements. NERC Compliance Enforcement Program personnel have reviewed the measures and found them to be sufficient.
007-M3		
007-M4		
007-M5		
007-M6		
007-M7		
007-M8		
007-M9		
007-M10		
007-C1,1		
007-C1,2		
007-C1,3		
007-C1,4		
007-C2,1		
007-C2,2		
007-C2,3		
007-C2,4		

CIP-007 Drafting Team Responses to Comments

Name	Ori Artman	
Entity	Teltone	
Ready to Ballot	Yes	
General Comments		
007-R1		
007-R2		
007-R3		
007-R4		
007-R5		
007-R6	R6.3.3 changing password annually (even where risk is low) is too long. How about suggesting a range and a default of two weeks?	The consensus of commenters is that annually is a minimal acceptable time frame. The standard does not preclude the Responsible Entity from changing passwords more frequently.
007-R7		
007-R8		
007-R9		
007-R10		
007-M1		
007-M2		
007-M3		
007-M4		
007-M5		
007-M6		
007-M7		
007-M8		
007-M9		

CIP-007 Drafting Team Responses to Comments

007-M10

007-C1,1

007-C1,2

007-C1,3

007-C1,4

007-C2,1

007-C2,2

007-C2,3

007-C2,4

CIP-007 Drafting Team Responses to Comments

Name	Steve Badgett
Entity	Riverside Public Utilitities
Ready to Ballot	Yes
General Comments	
007-R1	
007-R2	
007-R3	
007-R4	
007-R5	
007-R6	
007-R7	
007-R8	
007-R9	
007-R10	
007-M1	
007-M2	
007-M3	
007-M4	
007-M5	
007-M6	
007-M7	
007-M8	
007-M9	
007-M10	

CIP-007 Drafting Team Responses to Comments

007-C1,1

007-C1,2

007-C1,3

007-C1,4

007-C2,1

007-C2,2

007-C2,3

007-C2,4

CIP-007 Drafting Team Responses to Comments

Name	Terry Baker
Entity	Platte River Power Authority
Ready to Ballot	Yes
General Comments	
007-R1	
007-R2	
007-R3	
007-R4	
007-R5	
007-R6	
007-R7	
007-R8	
007-R9	
007-R10	
007-M1	
007-M2	
007-M3	
007-M4	
007-M5	
007-M6	
007-M7	
007-M8	
007-M9	
007-M10	

CIP-007 Drafting Team Responses to Comments

007-C1,1

007-C1,2

007-C1,3

007-C1,4

007-C2,1

007-C2,2

007-C2,3

007-C2,4

CIP-007 Drafting Team Responses to Comments

Name	Terry Bilke
Entity	Midwest ISO
Ready to Ballot	No
General Comments	
007-R1	
007-R2	
007-R3	
007-R4	
007-R5	
007-R6	
007-R7	
007-R8	
007-R9	
007-R10	
007-M1	
007-M2	
007-M3	
007-M4	
007-M5	
007-M6	
007-M7	
007-M8	
007-M9	
007-M10	

CIP-007 Drafting Team Responses to Comments

007-C1,1

007-C1,2

007-C1,3

007-C1,4

007-C2,1

007-C2,2

007-C2,3

007-C2,4

CIP-007 Drafting Team Responses to Comments

Name	Pat Bourassa	
Entity	Wisconsin Public Service Corporation	
Ready to Ballot	No	
General Comments		
007-R1	Non critical assets should not be included.	CIP-007 has been clarified to state that all requirements in CIP-007 apply to both Critical and non-critical Cyber Assets in the Electronic Security Perimeter. Protecting non-critical cyber assets residing within the same Electronic Security Perimeter as Critical Cyber Assets is essential because the non-critical cyber assets introduce vulnerabilities exposing the Critical Cyber Assets to threats that must be protected against. However, The drafting team has removed the requirement to list non-critical Cyber Assets within the Electronic Security Perimeter because this requirement is in CIP-005.
007-R2	R2.3 Records of test results for 1 year have no value if the source is not also available to recreate the results. What value does this provide?	The records demonstrate compliance.
007-R3		
007-R4		
007-R5		
007-R6		
007-R7		
007-R8		
007-R9		
007-R10		
007-M1		
007-M2		
007-M3		
007-M4		
007-M5		
007-M6		

CIP-007 Drafting Team Responses to Comments

007-M7

007-M8

007-M9

007-M10

007-C1,1

007-C1,2

007-C1,3

007-C1,4

007-C2,1

007-C2,2

007-C2,3

007-C2,4

CIP-007 Drafting Team Responses to Comments

Name	Laurence W. Brown	
Entity	Edison Electric Institute	
Ready to Ballot	No	
General Comments	Applicability paragraph A4.2.3 is missing.	Applicability section 4.2.3 has been added.
007-R1	If the suggestion, made at CIP-005-R1.4, to move reference to "covered" non-critical assets is adopted, this Requirement may no longer be necessary. Certainly, it is unnecessarily inconvenient, and even somewhat confusing, that a full determination of the responsibilities regarding such assets cannot be ascertained without reference both to CIP-005 and this Standard.	CIP-007 has been clarified to state that all requirements in CIP-007 apply to both Critical and non-critical Cyber Assets in the Electronic Security Perimeter. Protecting non-critical cyber assets residing within the same Electronic Security Perimeter as Critical Cyber Assets is essential because the non-critical cyber assets introduce vulnerabilities exposing the Critical Cyber Assets to threats that must be protected against. However, The drafting team has removed the requirement to list non-critical Cyber Assets within the Electronic Security Perimeter because this requirement is in CIP-005.
007-R2		
007-R3	This duplicates the requirements of CIP-005 at R2.1.1 and R2.1.2, and at R4.2, as well as to require an individual accounting of each and every single port and service, and thus is overly burdensome. One company has estimated that this requirement, port for port, line by line, would produce 6.4-million data points. Producing and maintaining documentation on each individual port and service is futile because many services are dynamic, bringing themselves up and taking themselves down as needed, many services use dynamic port numbers, and there is some thought that port-number information is not really crucial, since they are represented by a data field in the packet header that can be manipulated. For all of these considerations, no reasonable entity would attempt such detailed accounting, and such records could not be audited within a reasonable time frame or budget. Thus the Standard must be clarified to indicate that some form of grouping or class accounting is permitted, such as documenting standard ports and configurations, and reserving greater detail for any exceptions thereto. SEE ALSO M3, below. Suggested Alternative Wording: "Ports and Services — >Where< unused ports and services cannot be disabled> as required by CIP-005<, the Responsible Entity shall use and document >reasonable< compensating measure(s) to help mitigate risk exposure." (The above suggested wording also reinforces that the requirement may appropriately be moved to CIP-005; SEE comment at CIP-005-R2.1, above.)	CIP-005 refers to devices on the Electronic Security Perimeter and CIP-007 refers to devices within the Electronic Security Perimeter. The standard no longer requires the documentation of the configuration and status of all ports and services inside the Electronic Security Perimeter.
007-R4	R4.2 appears to require an individual accounting of each and every single patch, and thus is overly burdensome. No reasonable entity would attempt such detailed accounting, and thus the standard must be clarified to indicate that some form of grouping or class accounting is permitted. Also, it is not clear that detailed documentation is necessary where updates are automatically applied.	The requirement has been clarified. It does not explicitly define how patches are to be applied. Responsible Entities are expected to use reasonable business judgment when implementing the requirements of these standards.

	Suggested Alternative Wording: "… >Where patches are< not installed, the Responsible Entity shall document >reasonable< compensating measure(s) >taken< or >the assessment leading to its< acceptance of risk."	
007-R5	R5.2 appears to require an individual accounting of each and every single such tool, and thus is overly burdensome. No reasonable entity would attempt such detailed accounting, and thus the standard must be clarified to indicate that some form of grouping or class accounting is permitted. Also, it is not clear that detailed documentation is necessary where updates are automatically applied.	Tools and processes used to detect, prevent, deter, and mitigate the introduction of malware must be documented. The application of each individual signature does not.
	Suggested Alternative Wording: "… not installed, the Responsible Entity shall document >reasonable< compensating measure(s) >taken< or >the assessment leading to its< acceptance of risk."	
007-R6	R6.1.3 -- The concluding phrase "at any moment in time" appears unnecessarily, and perhaps unintentionally, overbroad. We suggest appending the following phrase to close out the sentence: "within the previous full calendar year."	Draft 3 R6 has been rewritten and renumbered to R5. Reference to "any moment in time" has been removed.
007-R7		
007-R8		
007-R9	Consistent with the above comment at R3, conducting an assessment every year on every item (especially if line by line, and port by port) is dramatically burdensome, completely unnecessary, and would produce such massive amounts of material that record-retention alone would be overly burdensome, and audits would become essentially unmanageable. We suggest modifying this Requirement to cover only 1/5 of the assets in any one year, or to permit pro-forma assessments, for example only assessing changes and otherwise indicating "no change."	Please see response at R3.
	In addition, this Requirement should cover only "Critical" Cyber Assets, since other covered assets are addressed in R1. Even if R1 is moved, or otherwise becomes unnecessary, due to acceptance of our comments on that Requirement, covered non-critical assets would still be adequately addressed only referring to Critical Cyber Assets here.	CIP-007 has been clarified to state that all requirements in CIP-007 apply to both Critical and non-critical Cyber Assets in the Electronic Security Perimeter. Protecting non-critical cyber assets residing within the same Electronic Security Perimeter as Critical Cyber Assets is essential because the non-critical cyber assets introduce vulnerabilities exposing the Critical Cyber Assets to threats that must be protected against.
007-R10	Consistent with several comments above, reference to "any modification" is overbroad. Instead, the phrase should be replaced with the phrase "a reasonably critical modification."	The requirement has been clarified.
007-M1		
007-M2		
007-M3	See above comment regarding R3.	See response at R3. Measures have been reworded.
	Suggested Alternative Wording: "Records documenting the status/configuration of >< ports and services on Critical Cyber Assets inside the Electronic Security Perimeter(s), >to the extent not already recorded pursuant to CIP-005-R4.2,< as well as >< compensating measures taken>, as identified in R3."	

007-M4	The term "business records" is used here, when "records" alone is used in similar measures such as M3, and in M5 through M9. We suggest deleting the unnecessary word "business" in this Measure.	Reference to business has been removed.
007-M5		
007-M6		
007-M7		
007-M8		
007-M9	NERC and or the Regions need to address the protection of sensitive information, both regarding auditors themselves and regarding litigation "discovery" and use. SEE General Comment 3, below.	All documentation required in this standard will remain in the possession of the Responsible Entity. It is the up to the Responsible Entity to protect sensitive information by Non-disclosure Agreements (NDA) or similar documents at all times, including audits. Information protection is addressed in CIP-003.
007-M10		
007-C1,1		
007-C1,2		
007-C1,3		
007-C1,4		
007-C2,1		
007-C2,2		
007-C2,3		
007-C2,4		

CIP-007 Drafting Team Responses to Comments

Name	Peter Burke	
Entity	American Transmission Company	
Ready to Ballot	No	
General Comments	American Transmission Company concurs with the comments submitted separately by the Edison Electric Institute and by the Midwest Reliability Organization.	Please see responses to Laurence W. Brown, Edison Electric Institute.
007-R1	American Transmission Company concurs with the comments submitted separately by the Edison Electric Institute.	
007-R2		
007-R3	American Transmission Company concurs with the comments submitted separately by the Edison Electric Institute and by the Midwest Reliability Organization.	
007-R4	American Transmission Company concurs with the comments submitted separately by the Edison Electric Institute.	
007-R5	American Transmission Company concurs with the comments submitted separately by the Edison Electric Institute.	
007-R6	American Transmission Company concurs with the comments submitted separately by the Edison Electric Institute and by the Midwest Reliability Organization.	
007-R7		
007-R8		
007-R9	American Transmission Company concurs with the comments submitted separately by the Edison Electric Institute and by the Midwest Reliability Organization.	
007-R10	American Transmission Company concurs with the comments submitted separately by the Edison Electric Institute and by the Midwest Reliability Organization.	
007-M1		
007-M2		
007-M3	American Transmission Company concurs with the comments submitted separately by the Edison Electric Institute.	
007-M4	American Transmission Company concurs with the comments submitted separately by the Edison Electric Institute.	
007-M5		
007-M6		
007-M7		

CIP-007 Drafting Team Responses to Comments

007-M8

007-M9 American Transmission Company concurs with the comments submitted separately by the Edison Electric Institute.

007-M10

007-C1,1

007-C1,2

007-C1,3

007-C1,4

007-C2,1

007-C2,2

007-C2,3

007-C2,4

CIP-007 Drafting Team Responses to Comments

Name	Marc Butts	
Entity	Southern Company	
Ready to Ballot	No	
General Comments	The 4.2.3 exemption for those entities with "no critical assets" is missing.	Applicability section 4.2.3 has been added.
007-R1	Replace the words "this standard" with "CIP-007" to maintain clarity. The purpose statement of all the standards says that CIP-002 through CIP-009 should be taken as a group so clarification is required if a subset of the group is meant.	The standard has been updated to specify CIP-007.
007-R2		
007-R3		
007-R4		
007-R5	We suggest dropping the 5.1 and 5.2 sub-requirements. It is sufficient to require that antivirus software be utilized but it is too onerous to require every signature update to be assessed for applicability or to do full change management on every signature update. Signatures are released almost constantly and can be released several times per day.	Tools and processes used to detect, prevent, deter, and mitigate the introduction of malware must be documented. The application of each individual signature does not.
007-R6	R6.1.3 We suggest changing "at any moment in time" which is open-ended to "within the previous full calendar year" which is the data retention period specified later in this standard.	Draft 3 R6 has been rewritten and renumbered to R5. Reference to "any moment in time" has been removed.
007-R7		
007-R8		
007-R9		
007-R10		
007-M1		
007-M2		
007-M3		
007-M4		
007-M5		
007-M6		
007-M7		
007-M8		

CIP-007 Drafting Team Responses to Comments

007-M9

007-M10

007-C1,1

007-C1,2

007-C1,3

007-C1,4

007-C2,1

007-C2,2

007-C2,3

007-C2,4

CIP-007 Drafting Team Responses to Comments

Name	Gary Campbell	
Entity	MAIN	
Ready to Ballot	No	
General Comments	address items below	
007-R1		
007-R2		
007-R3		
007-R4	What does "of availability" mean?	The intent of "of availability" was to define the assessment of the patches relative to the vendor's notification of availability. However, this term is subject to the Responsible Entity's reasonable business judgment.
007-R5		
007-R6	6.1.2 This should be a requirement of CIP-003 R5 if that is where the list resides. 6.1.5 This should be a requirement of CIP-003 and CIP-004 if that is where the information resides. 6.2.2 What does this statement mean? Remember to be specific.	The requirement in CIP-007 is to ensure the settings on Cyber Assets match access rights defined in CIP-003. The requirement has been rewritten and renumbered to R5.
007-R7		
007-R8		
007-R9		
007-R10		
007-M1		
007-M2		
007-M3		
007-M4		
007-M5		
007-M6		
007-M7		
007-M8		

007-M9		
007-M10		
007-C1,1		
007-C1,2		
007-C1,3		
007-C1,4		
007-C2,1	2.1.1 & 2.1.3 I do not think these two requirement should be the same level. Actual change toa control system I think be more critical.	The levels of noncompliance have been rewritten to reflect changes to requirements and measures as well as severity of infraction.
007-C2,2	2.2.4 What does "of availability" mean?. In looking at logs it needs to be defined on how far back the aduitor should look.	Please see response to R4, above.
007-C2,3		
007-C2,4		

Name	Linda Campbell	
Entity	FRCC	
Ready to Ballot	No	
General Comments	Applicability Section is missing the 4.2.3 wording found in other standards	Applicability section 4.2.3 has been added.
	Applicability 4.2.4 should be added to exclude non-critical cyber assets which reside within the physical perimeter, are not used for any electronic or physical control and are not in the electronic perimeter.	The standard only applies to Cyber Assets within the Electronic Security Perimeter, and, as a result, Cyber Assets outside of the Electronic Security Perimeter, but inside the Physical Security Perimeter, are excluded.
007-R1	R1 Non critical assets should be subject to the requirements of this standard with the exception of R2 (if not critical, it is not going to affect systems that can cause reliability problems, so testing while possibly still prudent, should not be required to be documented for these assets) and R8 (If the asset is non-critical, why do you care about its disposition or redeployment?)	
007-R2		
007-R3	R3 In the last sentence, where the Responsible Entity must document unused ports and services that cannot be disabled, it this documented as an exception? If yes, then explicitly state that. Scanning should not be required, so delete the reference to CIP-005	Provided that the compensating measure or acceptance of risk is documented, it is not an exception. R3 has been renumbered to R2 and reference to CIP-005 removed.
007-R4	R.4.2 and R5.2 If cannot be installed, is this documented as an exception? If yes, then explicitly state that.	Provided that the compensating measure or acceptance of risk is documented, it is not an exception.
007-R5	Anti-Virus is a subset of mal-ware, and hence this requirement should be for mal-ware mitigation software, which includes anti-virus, host based IPS, key logger blockers, etc. and specifically state that the minimum mal-ware protection required is anti-virus.	The title has been changed to Malicious Software Prevention.
	R5. Should replace "technically feasible" with "practical", because anything can be technically feasible or not depending on an entity's budget. If the wording is not changed the requirement could force the Responsible Entity to implement an exception.	If the use of anti-virus and other malware prevention tools is technically feasible, it must be implemented using reasonable business judgment. Refer to the FAQ for a discussion of technical feasibility.
	R.4.2 and R5.2 If cannot be installed, is this documented as an exception? If yes, then explicitly state that.	Provided that the compensating measure or acceptance of risk is documented, it is not an exception.
007-R6	R6.1.3 Please define what "detail" is being requested. It may not be practical to track all activities of a user. This would lead to very large and unmanageable logs. The statement "at any moment in time" is too ambiguous. Suggested wording: "The responsible Entity shall establish methods, processes and procedures that generate logs of sufficient detail to provide an audit trail of an individual user account access activity."	The Responsible Entity must determine the appropriate amount of logging for its environment. Logging should be sufficient to respond appropriately to incidents as referenced in CIP-008. Reference to "any moment in time" has been removed.
	R6.1.5 I don't see any review checklists defined in CIP-003 or 004 -- what is "review checklists" referring to?? If truly an example, and not required, perhaps this belongs in the FAQs.	This requirement has been reworded and the reference to checklists removed.
	R6.3 Should replace "technically feasible" with "practical", because anything can be technically	

	feasible or not depending on an entity's budget. If the wording is not changed the requirement could force the Responsible Entity to implement an exception.	See response regarding tehcnical feasibility, above.
007-R7	R7 Should replace "as technically feasible" with "as practical", because anything can be technically feasible or not depending on an entity's budget. If the wording is not changed the requirement could force the Responsible Entity to implement an exception.	See response regarding tehcnical feasibility, above.
	R7.3 This requirement is not specific enough. How would you measure that the events are there in "sufficient detail to enable a root-cause analysis" There is no requirement to perform a root-cause analysis, so why do you need the detailed information? Suggested wording:" The Responsible Entity shall maintain logs of system events related to cyber security in sufficient detail to enable a root-cause analysis, if possible." It may not be possible in all cases to get a root-cause.	The requirement has been updated to address your comment. The requirement now requires maintaining logs of events to support investigation of cyber events referenced in CIP-008.
	R7.4 Does this belong in section D1.3 with other data retention?	The requirement is listed in R7 as it is a part of Security Status Monitoring. It is reiterated in D1.3.
	R7.5, This is first use of the term "business records" in the standard. What constitutes a "business record" and how does it differ from measures in previous sections of the standards from "data", "document" or "documentation."	Reference to "business record" has been removed.
007-R8	R8.2 Simply erasing data does not prevent it from being retrieved. You must cleanse the data media with a multi-pass write-delete process.	The requirement says "to prevent retrieval of critical cyber security or reliability data". Erasures that do not prevent retrieval do not meet the requirement.
	R8.2 If a critical cyber asset is being redeployed, only stored data related to the critical cyber asset or reliability of the grid should be required to be erased or destroyed, not all data storage on the asset. If an employee's workstation or a server with no critical information is being moved outside the cyber perimeter (redeployed), there is no cause to delete information on that equipment. Change 8.2 to Prior to redeployment of Critical Cyber Assets, the Responsible Entity shall at a minimum evaluate the data stored on the asset, and erase any data that should not be accessed by unauthorized personnel.	Reference to business records has been removed.
	R8.3, This is first use of the term "business records" in the standard. What constitutes a "business record" and how does it differ from measures in previous sections of the standards from "data", "document" or "documentation."	
007-R9		
007-R10		
007-M1		
007-M2	M2.3 Is this referencing the approval specified in R6.2 in CIP-003-1? If so they are accepting the "testing results" rather than the "successful completion of changes." There is no requirement specified for the acceptance of the successful completion of changes.	The measures have been rewritten to refer back to the requirements.
007-M3		
007-M4	M4 How do documentation and business records differ? Clarify the measure if there is a difference	Reference to business has removed. The measures have been rewritten

	or use only documentation.	to refer back to the requirements.
007-M5	M5. Change Anti-virus to Mal-ware. M5 through M9 How do documentation and records differ? Clarify the measure if there is a difference or use only documentation.	Reference to business has removed. The measures have been rewritten to refer back to the requirements.
007-M6	M5 through M9 How do documentation and records differ? Clarify the measure if there is a difference or use only documentation.	Reference to business has removed. The measures have been rewritten to refer back to the requirements.
007-M7	M5 through M9 How do documentation and records differ? Clarify the measure if there is a difference or use only documentation.	Reference to business has removed. The measures have been rewritten to refer back to the requirements.
007-M8	Reference to business has removed. The measures have been rewritten to refer back to the requirements.	Reference to business has removed. The measures have been rewritten to refer back to the requirements.
007-M9	M5 through M9 How do documentation and records differ? Clarify the measure if there is a difference or use only documentation.	Reference to business has removed. The measures have been rewritten to refer back to the requirements.
007-M10		
007-C1,1	In the applicability section 4.1.10 and 4.1.11, RRO's and NERC are included. Who has the monitoring responsibility for a RRO or NERC? Add Self-Certification and Audit information to this section. Proposed language would be: 1.1. Complaince Monitoring Responsibility Regional Reliability Organization. 1.1.1. The Compliance Monitor will request a self-certification annually. 1.1.2. The Compliance Monitor will perform an audit at least once every three (3) calendar years.	NERC will monitor the RROs and a third party without vested interest in the outcome will monitor NERC. Self-certification has been added under "Additional Compliance Information." Data retention has been modified to match requirements.
007-C1,2		
007-C1,3	D1.3.1 Should this exclude logs from R7.4 and R6.1.3 or specifically mention here only 90 days for those? What is the reason to keep Individual User Account Activity Logs (R6.1.3) which can be extremely large for the previous calendar year?	This section has been reworded.
007-C1,4		
007-C2,1		
007-C2,2		
007-C2,3		
007-C2,4		

Name	Roger Champagne	
Entity		
Ready to Ballot	No	
General Comments	Remove the first sentence of the purpose since it is redundant with the rest of the purpose. We prefer the second and third sentence of the purpose. For consistency, this Standard should include an Applicability 4.2.3, "Responsible Entities that, in compliance with CIP-002, identify that they have no Critical Cyber Assets."	Please see responses to Ray A'Brial, Central Hudson Gas & Electric Corp.
007-R1	The wording of R1 requires clarification given that some requirements in this standard refer specifically to Critical Cyber Assets rather than to the more generic "cyber assets". For instance, R8 requires data destruction or removal prior to disposal of a Critical Cyber Asset. On one hand, the wording of R1 could be taken to mean that one should replace the words "Critical Cyber Assets" by the words "Critical and Non-Critical Cyber Assets" when interpreting the standard. Under this interpretation, the Responsible Entity should wipe data on all assets prior to disposal. Alternatively, one could argue that the wording of R8 explicitly excludes non-critical cyber assets, and therefore failure to consider wipe data from non-critical cyber assets does not give rise to non-compliance. Please clarify. Change; Non-critical Cyber Assets as well as the Critical Cyber Assets defined in CIP-002 within the Electronic Security Perimeter(s) defined in CIP-005 shall be subject to the requirements of this standard. to; Cyber Assets associated with the Critical Cyber Assets defined in CIP-002 within the Electronic Security Perimeter(s) defined in CIP-005 shall be subject to the requirements of this standard.	
007-R2	Request clarification on R2. Does this Standard apply to Critical Cyber Assets or Cyber Assets? For clarification, change to "security patches, cumulative service packs, vendor releases, or version upgrades as applied to operating systems, applications, database platforms, or other third-party software or firmware."	
007-R3		
007-R4		
007-R5		

007-R6	R6.1.5 is not clear. This should be rewritten or removed	R6 has been rewritten and renumbered to R5.
	R6.3.1 replace six by eight caracters R6.3.2 …combinaison of at least one alpha, one numeris, one … if possible. Rational	Not all control systems support eight characters. It is the consensus of commenters that six characters is acceptable. This does not preclude the entity from using eight. The requirement calls for the use of a
007-R7		
007-R8		
007-R9		
007-R10		
007-M1		
007-M2	Measures M2.1, M2.2 and M2.3 should be rephrased as measures	
007-M3		
007-M4		
007-M5		
007-M6		
007-M7		
007-M8		
007-M9		
007-M10		
007-C1,1		
007-C1,2		
007-C1,3		
007-C1,4		
007-C2,1		
007-C2,2		
007-C2,3		
007-C2,4		

CIP-007 Drafting Team Responses to Comments

Name	Larry Conrad	
Entity	ECAR Critical Infrastructure Protection Panel	
Ready to Ballot	No	
General Comments	The introduction section needs to be made consistent with the other standards, the following language was not included in CIP-007 exemptions and needs to be added: 4.2.3 Responsible Entities that, in compliance with Standard CIP-002, identify that they have no Critical Cyber Assets.	Applicability section 4.2.3 has been added.
007-R1		
007-R2		
007-R3		
007-R4		
007-R5		
007-R6		
007-R7		
007-R8		
007-R9		
007-R10		
007-M1		
007-M2		
007-M3		
007-M4		
007-M5		
007-M6		
007-M7		
007-M8		
007-M9		

CIP-007 Drafting Team Responses to Comments

007-M10

007-C1,1

007-C1,2

007-C1,3

007-C1,4

007-C2,1

007-C2,2

007-C2,3

007-C2,4

CIP-007 Drafting Team Responses to Comments

Name	Larry Conrad	
Entity	Cinergy	
Ready to Ballot	No	
General Comments	Exemptions The following language was not included in CIP 007 exemptions and needs to be added: 4.2.3. Responsible Entities that, in compliance with Standard CIP-002, identify that they have no Critical Cyber Assets. This exemption appears in the other standards, but not in CIP 007.	Applicability section 4.2.3 has been added.
007-R1		
007-R2		
007-R3		
007-R4	R4.1 -- Requires utilities to "document the assessment of security patches and upgrades for applicability within 30 calendar days of availability." This timeframe is too short, and should be extended to at least 90 days.	30 days reflects industry concensus.
007-R5	B.R5.1 -- Requires utilities to "document the assessment of anti-virus and integrity monitoring tool signatures for applicability within 30 calendar days of availability." This timeframe is too short, and should be extended to at least 90 days	30 days reflects industry concensus.
007-R6		
007-R7	B.R7.2 If automated alerts are required and implemented, do participants still need to perform the manual review of logs referenced in CIP 005 requirements?	CIP-005 addresses Critical Cyber Assets on the Electronic Security Perimeter. CIP-007 addresses Critical Cyber Assets within the Electronic Security Perimeter. The logs are different and must be reviewed as such.
007-R8		
007-R9		
007-R10		
007-M1		
007-M2		
007-M3		
007-M4		
007-M5		
007-M6		

CIP-007 Drafting Team Responses to Comments

007-M7

007-M8

007-M9

007-M10

007-C1,1

007-C1,2

007-C1,3

007-C1,4

007-C2,1

007-C2,2

007-C2,3

007-C2,4

CIP-007 Drafting Team Responses to Comments

Name	Theodore Creedon, P.E.	
Entity	Creedon Engineering	
Ready to Ballot	No	
General Comments	This section is inadequate and does not recognize the technical complexity of the task at hand.	These requirements represent a consensus of the industry, as gauged by comments the drafting team received. They are a set of minimum requirements that must be complied with to protect Critical Cyber Assets. Responsible Entities may exceed the minimum requirements if they deem it appropriate to do so.
007-R1		
007-R2		
007-R3		
007-R4		
007-R5	IP addressing is being used in all modern IED based systems. IED's use windows, embedded windows, linux and embedded linux as the basic operating systems. It has been discovered that firmware patches may themselves contain bugs that are discovered in the recalibration and test of protective relays. Require vendors to publish bug and patch information. Require that test data and test software be under engineering change control/configuration management.	Responsible Entities must manage the relationship with its vendors. The standards cannot require vendors to publish information or perform testing. However if vendors make available bug and patch information and test data, it is the Responsible Entity's responsibility to obtain and use such information.
007-R6		
007-R7		
007-R8		
007-R9		
007-R10		
007-M1		
007-M2		
007-M3		
007-M4		
007-M5		
007-M6		
007-M7		

CIP-007 Drafting Team Responses to Comments

007-M8

007-M9

007-M10

007-C1,1

007-C1,2

007-C1,3

007-C1,4

007-C2,1

007-C2,2

007-C2,3

007-C2,4

CIP-007 Drafting Team Responses to Comments

Name	Joel De Granda	
Entity	Florida Power and Light	
Ready to Ballot	No	
General Comments		
007-R1		
007-R2		
007-R3		
007-R4		
007-R5		
007-R6	R6.1.3 Please define what "detail" is being requested. It may not be practical to track all activities of a user. This would lead to very large and unmanageable logs. The statement "at any moment in time" is too ambiguous. Suggested wording: "The responsible Entity shall establish methods, processes and procedures that generate logs of sufficient detail to provide an audit trails of an individual user account access activity.	Please see responses to Linda Campbell, FRCC.
007-R7	R7 Should replace "as technically feasible" with "as practical", because anything can be technically feasible or not depending on an entity’s budget. R7.3 Suggested wording:" The Responsible Entity shall maintain logs of system events related to cyber security in sufficient detail to enable a root-cause analysis, if possible." It may not be possible in all cases to get a root-cause.	
007-R8		
007-R9		
007-R10		
007-M1		
007-M2		
007-M3		
007-M4		
007-M5		
007-M6		

CIP-007 Drafting Team Responses to Comments

007-M7

007-M8

007-M9

007-M10

007-C1,1

007-C1,2

007-C1,3

007-C1,4

007-C2,1

007-C2,2

007-C2,3

007-C2,4

CIP-007 Drafting Team Responses to Comments

Name	Richard Engelbrecht	
Entity	RGE	
Ready to Ballot	No	
General Comments	Remove the first sentence of the purpose since it is redundant with the rest of the purpose. We prefer the second and third sentence of the purpose. For consistency, this Standard should include an Applicability 4.2.3, "Responsible Entities that, in compliance with CIP-002, identify that they have no Critical Cyber Assets."	Please see responses to Ray A'Brial, Central Hudson Gas & Electric Corp.
007-R1	The wording of R1 requires clarification given that some requirements in this standard refer specifically to Critical Cyber Assets rather than to the more generic "cyber assets". For instance, R8 requires data destruction or removal prior to disposal of a Critical Cyber Asset. On one hand, the wording of R1 could be taken to mean that one should replace the words "Critical Cyber Assets" by the words "Critical and Non-Critical Cyber Assets" when interpreting the standard. Under this interpretation, the Responsible Entity should wipe data on all assets prior to disposal. Alternatively, one could argue that the wording of R8 explicitly excludes non-critical cyber assets, and therefore failure to consider wipe data from non-critical cyber assets does not give rise to non-compliance. Please clarify. Change; Non-critical Cyber Assets as well as the Critical Cyber Assets defined in CIP-002 within the Electronic Security Perimeter(s) defined in CIP-005 shall be subject to the requirements of this standard. to; Cyber Assets associated with the Critical Cyber Assets defined in CIP-002 within the Electronic Security Perimeter(s) defined in CIP-005 shall be subject to the requirements of this standard.	
007-R2	Request clarification on R2. Does this Standard apply to Critical Cyber Assets or Cyber Assets? For clarification, change to "security patches, cumulative service packs, vendor releases, or version upgrades as applied to operating systems, applications, database platforms, or other third-party software or firmware."	
007-R3		
007-R4		
007-R5		
007-R6	R6.1.5 is not clear. This should be rewritten or removed	
007-R7		

CIP-007 Drafting Team Responses to Comments

007-R8	
007-R9	
007-R10	
007-M1	
007-M2	Measures M2.1, M2.2 and M2.3 should be rephrased as measures
007-M3	
007-M4	
007-M5	
007-M6	
007-M7	
007-M8	
007-M9	
007-M10	
007-C1,1	
007-C1,2	
007-C1,3	
007-C1,4	
007-C2,1	
007-C2,2	
007-C2,3	
007-C2,4	

Name	Ken Fell	
Entity	New York ISO	
Ready to Ballot	No	
General Comments	Remove the first sentence of the purpose since it is redundant with the rest of the purpose. We prefer the second and third sentence of the purpose. For consistency, this Standard should include an Applicability 4.2.3, "Responsible Entities that, in compliance with CIP-002, identify that they have no Critical Cyber Assets."	Please see responses to Ray A'Brial, Central Hudson Gas & Electric Corp.
007-R1	The wording of R1 requires clarification given that some requirements in this standard refer specifically to Critical Cyber Assets rather than to the more generic "cyber assets". For instance, R8 requires data destruction or removal prior to disposal of a Critical Cyber Asset. On one hand, the wording of R1 could be taken to mean that one should replace the words "Critical Cyber Assets" by the words "Critical and Non-Critical Cyber Assets" when interpreting the standard. Under this interpretation, the Responsible Entity should wipe data on all assets prior to disposal. Alternatively, one could argue that the wording of R8 explicitly excludes non-critical cyber assets, and therefore failure to consider wipe data from non-critical cyber assets does not give rise to non-compliance. Please clarify. Change; Non-critical Cyber Assets as well as the Critical Cyber Assets defined in CIP-002 within the Electronic Security Perimeter(s) defined in CIP-005 shall be subject to the requirements of this standard. to; Cyber Assets associated with the Critical Cyber Assets defined in CIP-002 within the Electronic Security Perimeter(s) defined in CIP-005 shall be subject to the requirements of this standard.	
007-R2	Request clarification on R2. Does this Standard apply to Critical Cyber Assets or Cyber Assets? For clarification, change to "security patches, cumulative service packs, vendor releases, or version upgrades as applied to operating systems, applications, database platforms, or other third-party software or firmware."	
007-R3		
007-R4		
007-R5		
007-R6	R6.1.5 is not clear. This should be rewritten or removed	
007-R7		

CIP-007 Drafting Team Responses to Comments

007-R8	
007-R9	
007-R10	
007-M1	
007-M2	Measures M2.1, M2.2 and M2.3 should be rephrased as measures
007-M3	
007-M4	
007-M5	
007-M6	
007-M7	
007-M8	
007-M9	
007-M10	
007-C1,1	
007-C1,2	
007-C1,3	
007-C1,4	
007-C2,1	
007-C2,2	
007-C2,3	
007-C2,4	

CIP-007 Drafting Team Responses to Comments

Name	Francis Flynn	
Entity	National Grid USA	
Ready to Ballot	No	
General Comments	Remove the first sentence of the purpose since it is redundant with the rest of the purpose. We prefer the second and third sentence of the purpose. For consistency, this Standard should include an Applicability 4.2.3, "Responsible Entities that, in compliance with CIP-002, identify that they have no Critical Cyber Assets."	Please see responses to Ray A'Brial, Central Hudson Gas & Electric Corp.
007-R1	The wording of R1 requires clarification given that some requirements in this standard refer specifically to Critical Cyber Assets rather than to the more generic "cyber assets". For instance, R8 requires data destruction or removal prior to disposal of a Critical Cyber Asset. On one hand, the wording of R1 could be taken to mean that one should replace the words "Critical Cyber Assets" by the words "Critical and Non-Critical Cyber Assets" when interpreting the standard. Under this interpretation, the Responsible Entity should wipe data on all assets prior to disposal. Alternatively, one could argue that the wording of R8 explicitly excludes non-critical cyber assets, and therefore failure to consider wipe data from non-critical cyber assets does not give rise to non-compliance. Please clarify. Change; Non-critical Cyber Assets as well as the Critical Cyber Assets defined in CIP-002 within the Electronic Security Perimeter(s) defined in CIP-005 shall be subject to the requirements of this standard. to; Cyber Assets associated with the Critical Cyber Assets defined in CIP-002 within the Electronic Security Perimeter(s) defined in CIP-005 shall be subject to the requirements of this standard.	
007-R2	Request clarification on R2. Does this Standard apply to Critical Cyber Assets or Cyber Assets? For clarification, change to "security patches, cumulative service packs, vendor releases, or version upgrades as applied to operating systems, applications, database platforms, or other third-party software or firmware."	
007-R3		
007-R4		
007-R5		
007-R6	R6.1.5 is not clear. This should be rewritten or removed	
007-R7		

007-R9	This point needs clarification. National Grid believes this requirement should be deleted and is not required, since in CIP-005-1 Requirement R4, we are protecting the access points into the Electronic Security Perimeter and performing the vulnerability assessment on the access points. Within R9 National Grid believes that additional clarification is required regarding the definition of"Ports and Services" wherever these terms are used. Is the standard trying to address Physical Ports (i.e. ethernet ports on an IED?) or Virtual IP Logical Ports? If physical ports, is requirement R9.2 suggesting that an IED's unused physical ethernet ports be verified as being unused on an annual basis? If so, please clarify and explain what perceived threat is being addressed by this requirment.	It is appropriate to separately address the requirement to perform a vulnerability assessment of Cyber Assets within the Electronic Security Perimeter in CIP-007. CIP-005 defines requirements for Critical Cyber Assets on the perimeter. The assessment process and procedures may be quite different. The requirement is intended to address logical ports.
007-R10		
007-M1		
007-M2	Measures M2.1, M2.2 and M2.3 should be rephrased as measures	
007-M3		
007-M4		
007-M5		
007-M6		
007-M7		
007-M8		
007-M9		
007-M10		
007-C1,1		
007-C1,2		
007-C1,3		
007-C1,4		
007-C2,1		
007-C2,2		
007-C2,3		
007-C2,4		

CIP-007 Drafting Team Responses to Comments

Name	Greg Fraser	
Entity	Manitoba Hydro	
Ready to Ballot	No	
General Comments	Cyber Assets in CIP-005 R1.5 performing security access control should be mentioned in the paragraph R1 which mentions Critical Cyber Assets. It needs to be made very clear that all these Cyber Assets must be managed including documentation (lists), access controls, etc. Under Introduction add 4.2.3 which should read the same as in CIP-009-1: "Responsible Entities that, in compliance with Standard CIP-002, identify that they have no Critical Cyber Assets."	The drafting team has removed the requirement to list non-critical Cyber Assets within the Electronic Security Perimeter because this requirement is in CIP-005. The drafting team has also clarified that all requirements in CIP-007 apply to both Critical and non-critical Cyber Assets within the Electronic Security Perimeter. Applicability section 4.2.3 has been added.
007-R1		
007-R2	Remove "cyber security" as the test procedures should include more than just the security portion. Same comment in R2.1. All hardware and software testing as noted in CIP-003 R6 which creates an inconsistency between these standards. Remove the "security" from security patches as all patches should be managed. R2.1 2nd sentence change "...precludes adversely affecting the production system and operation." to "minimize the adverse impact to the production system and operation." Reducing the impact to zero is not always possible. Suggest combining R2.2 with R2.1 as it is really redundant.	The drafting team must respect the limits identified in the SAR, which says that the standards are for cyber security. The Responsible Entity may implement procedures beyond the scope of these requirements. The requirement has been changed to reflect the intent of the comment. R2.1 has been renumbered to R1.1 and R2.2 has been renumbered to 1.2. The first one refers to the potential adverse impact of the test; the second one refers to the test environment itself.
007-R3		
007-R4	Suggest that patch management apply to all patches and not just security related patches.	See response to R2, above.
007-R5	In R5.1 the 30 calendar days for the assessment period should be shortened since mass attacks usually come sooner than 30 days after announcement of vulnerability. Unless it is specifically the intent of this standard to have the 2nd layer of security defense behind the Electronic Security Perimeter as a lesser requirement, if so then an FAQ should be added detailing this intent.	30 days reflects industry consensus. Responsible Entities may shorten the assessment period as it deems appropriate.
007-R6		
007-R7	This requirement is more restrictive than CIP-005 R3 while cyber assets should be less vulnerable inside the Electronic Security Perimeter. Suggest coordinating these requirements in both standards.	The standards have been changed to clarify that the assets addressed CIP-005 are different than those addressed In CIP-007. The requirements reflect those differences.
007-R8	In addition to Critical Cyber Assets this requirement should include the assets identified in CIP-	The requirement has been reworded.

005 R1.4 and R1.5.

007-R9

007-R10

007-M1

007-M2

007-M3

007-M4

007-M5

007-M6

007-M7

007-M8

007-M9

007-M10

007-C1,1

007-C1,2

007-C1,3

007-C1,4

007-C2,1

007-C2,2

007-C2,3

007-C2,4

CIP-007 Drafting Team Responses to Comments

Name	Jerry Freese	
Entity	American Electric Power	
Ready to Ballot	No	
General Comments	Based on the expanded scope set forth in CIP-002 R1 for the Critical Assets and the subsequently expanded scope of the Critical Cyber Assets and the Electronic Security Perimeter, it would be impractical and infeasible to meet the obligations set forth in this requirement.	CIP-002 has been changed and the scope of assets to be considered critical modified.
007-R1	Futhermore, the Non-Critical Cyber Assets should be clearly defined in CIP-002 along with the Critical Cyber Assets.	The drafting team has removed the requirement to list non-critical Cyber Assets within the Electronic Security Perimeter because this requirement is in CIP-005. It must remain in CIP-005 rather than CIP-002 because the Electronic Security Perimeter must be identified before the non-critical Cyber Assets within the Electronic Security Perimeter can be identified.
007-R2		
007-R3	There is a true reliability risk of performing a full port-scan of the critical production systems.	The standard no longer requires the documentation of the configuration and status of all ports and services inside the Electronic Security Perimeter. R8.2. calls for a review to verify that only ports and services required for operation of the Cyber Assets within the Electronic Security Perimeter are enabled, not an active port scan. Please see the FAQs.
007-R4		
007-R5		
007-R6	Many legacy equipment that could be in-scope of this standard, might not allow for password scemas as desired in the standard.	The requirement calls for the use of passwords as technically feasible.
007-R7		
007-R8		
007-R9		
007-R10		
007-M1		
007-M2		
007-M3		

CIP-007 Drafting Team Responses to Comments

007-M4

007-M5

007-M6

007-M7

007-M8

007-M9

007-M10

007-C1,1

007-C1,2

007-C1,3

007-C1,4

007-C2,1

007-C2,2

007-C2,3

007-C2,4

CIP-007 Drafting Team Responses to Comments

Name	Edwin C. Goff III	
Entity	Progress Energy	
Ready to Ballot	No	
General Comments		
007-R1	This requirement is titled "Non-Critical Cyber" assets. The focus being Critical Cyber Assets…that should be the title. Suggest changing the wording to "Critical Cyber Assets defined…as well as non-critical cyber assets"	The drafting team has removed the requirement to list non-critical Cyber Assets within the Electronic Security Perimeter because this requirement is in CIP-005 and clarified that all requirements in CIP-007 apply to both Critical and non-critical Cyber Assets in the Electronic Security Perimeter.
007-R2		
007-R3		
007-R4		
007-R5	"where technically feasible" -- there is a FAQ (15) that states "available for the OS..." Is that the only criteria or meaning we are to use "where technically feasible"? How far do we have to go to make anti-virus software work? If anti-virus software is available for a particular OS, do we have to test and prove that it works or negatively impacts the operation of the host too much to tolerate? Can we rely just on vendor documentation that it can't be loaded? Another option could be the following: Anti-Virus Software - To detect, prevent, deter, and mitigate the introduction, exposure, and propagation of malicious software (mal-ware) on systems within all Electronic Security Perimeters, the responsible entity shall use anti-virus software and related file integrity monitoring tools. Anti-virus software and related file integrity monitoring tools may be run directly on the process control system components where technically feasible. Optionally, where technically feasible, anti-virus software and related file integrity monitoring tools can be run on installed security appliances located between the system and the network that provides a security perimeter. All outside connections to the process network shall be scanned and verified "clean" or non-destructive by the installed security appliances prior to connection to the process control networks or components.	If the vendor provides documentation, testing is not necessary. The standard, as written, does not prevent the use of a security appliance.
007-R6		
007-R7		
007-R8		
007-R9		
007-R10		

CIP-007 Drafting Team Responses to Comments

007-M1

007-M2

007-M3

007-M4

007-M5

007-M6

007-M7

007-M8

007-M9

007-M10

007-C1,1

007-C1,2

007-C1,3

007-C1,4

007-C2,1

007-C2,2

007-C2,3

007-C2,4

CIP-007 Drafting Team Responses to Comments

Name	Kenneth Goldsmith	
Entity	Alliant Energy	
Ready to Ballot	No	
General Comments	The standard should allow the Responsible Entity to determine the appropriate protection for non-critical assets, even if located in a critical area.	CIP-007 includes non-critical assets within the Electronic Security Perimeter, not the Physical Security Perimeter. Protecting non-critical cyber assets residing in the same Electronic Security Perimeter as Critical Cyber Assets is essential because the non-critical Cyber Assets introduce vulnerabilities exposing the Critical Cyber Assets to threats that must be protected against.
007-R1		
007-R2	R6 of CIP-003-1 does a good job of sufficiently covering the matter of testing. R2 of CIP-007-1should be deleted.	The testing requirement has been removed from 003 and consolidated in CIP-007. CIP-007 R2 addresses testing to verify that changes do not adversely affect security controls required in CIP-007.
007-R3	R3 is not sufficiently beneficial to mandate the costs; it should be left to each entity to weigh costs and benefits in this area. The corresponding requirement regarding devices on teh perimeter (CIP-005) is fine; this R3 should be deleted.	CIP-005 refers to devices on the Electronic Security Perimeter and CIP-007 refers to devices within the Electronic Security Perimeter. The standard no longer requires the documentation of the configuration and status of all ports and services inside the Electronic Security Perimeter.
007-R4		
007-R5		
007-R6	R6 should be deleted. R5 of CIP-003 covers it very well. The elements of R6 that are not explicitly covered in CIP-003 are better left to each Responsible Entity to define in their cyber security policies. The exception is R6.2.1, which should be integrated into R5 of CIP-003.	CIP-007 addresses the requirements for implementing the access rights defined in CIP-003. The requirement has been updated to reference CIP-003.
007-R7		
007-R8		
007-R9	R9 should be deleted. It is a repeat of R4 in CIP-005.	It is appropriate to separately address the requirement to perform a vulnerability assessment of Cyber Assets within the Electronic Security Perimeter in CIP-007. CIP-005 defines requirements for Critical Cyber Assets on the perimeter. The assessment process and procedures may be quite different.
007-R10		
007-M1		
007-M2		

007-M3

007-M4

007-M5

007-M6

007-M7

007-M8

007-M9

007-M10

007-C1,1

007-C1,2

007-C1,3

007-C1,4

007-C2,1

007-C2,2

007-C2,3

007-C2,4

CIP-007 Drafting Team Responses to Comments

Name	Kathleen Goodman	
Entity	ISO New England Inc	
Ready to Ballot	Yes	
General Comments	We believe that CIP002 through CIP009 be beyond the intended scope of the original SAR for 1300. The final SAR for 1300, dated March 8, 2004, clearly states that the U/A 1200 is the basis for development of a permanent standard to replace it. The intent of both U/A 1200 and SAR 1300 is to establish a minimum set of cyber security best practices as a standard baseline for general cyber protection of a reliable BES.	The Drafting Team has modified these standards to the extent practical to remove references to specific technologies. However, where appropriate, certain accepted methodologies and security-practice specific terms are still referenced; examples are passwords, access controls and access logs.
	In establishing such a baseline, all care should be taken to aviod dictating particular tools, technologies, and/or methodologies. Where such are referenced, those references should be removed.	The purpose has been modifed and A.4.2.3 added.
	Remove the first sentence of the purpose since it is redundant with the rest of the purpose. For consistency, this Standard should include an Applicability 4.2.3, "Responsible Entities that, in compliance with CIP-002, identify that they have no Critical Cyber Assets."	
007-R1	The wording of R1 requires clarification given that some requirements in this standard refer specifically to Critical Cyber Assets rather than to the more generic "cyber assets". For instance, R8 requires data destruction or removal prior to disposal of a Critical Cyber Asset. On one hand, the wording of R1 could be taken to mean that one should replace the words "Critical Cyber Assets" by the words "Critical and Non-Critical Cyber Assets" when interpreting the standard. Under this interpretation, the Responsible Entity should wipe data on all assets prior to disposal. Alternatively, one could argue that the wording of R8 explicitly excludes non-critical cyber assets, and therefore failure to consider wipe data from non-critical cyber assets does not give rise to non-compliance. Please clarify.	The drafting team has clarified that all requirements in CIP-007 apply to both Critical and non-critical Cyber Assets in the Electronic Security Perimeter.
007-R2	Request clarification on R2. Does this Standard apply to Critical Cyber Assets or Cyber Assets?	The drafting team has clarified that all requirements in CIP-007 apply to both Critical and non-critical Cyber Assets within the Electronic Security Perimeter.
	For clarification, change to "security patches, cumulative service packs, vendor releases, or version upgrades as applied to operating systems, applications, database platforms, or other third-party software or firmware."	R2 has been renumbered to R1 and reworded for clarity as suggested.
	R2.2 is redundent and should be removed.	R2.1 has been renumbered to R1.1 and R2.2 has been renumbered to 1.2. The first one refers to the potential adverse impact of the test; the second one refers to the test environment itself.
007-R3	Reference to test ports is either redundent and should be removed, or confusing and should be removed. How do you account for dymanic ports?	The standard no longer requires the documentation of the configuration and status of all ports and services inside the Electronic Security Perimeter.

007-R4	R4.1 suggest re-write to "...within 30 days of notification...". R4.2 suggest re-write to "...implementation od security patches...".	The intent of "of availability" was to define the assessment of the patches relative to the vendor's notification of availability. However, this term is subject to the Responsible Entity's reasonable business judgment.
007-R5	R5 Title should be "Integrity Software." Remove words, "related file."	The title has been changed to Malicious Software Prevention.
007-R6	R6.1 Remove references to administrator and system accounts in all instances throughout this requirement as being platform-specific. Acounts are either individual or shared, period. R6.1.1 Likewise, this is therefore confusing and needs clarification. R6.1.3 This is not technically feasible and should be removed. R6.1.5 is not clear. This should be rewritten or removed. R6.2 Should re-write to simply say, "The Responsible Entity shall implement a policy to manage the scope and acceptable use of account privileges." R6.2 should also corrilate with personnel changes. R6.3 Should re-write to say, "The Responsible Entity shall require and utilize strong authentication methods (e.g. use of multi-factor access controls, digital certificates, or bio-metrics). In the absence of strong authentication methods, the Responsible Entity shall require and utilize passwords as technically feasible.	R6 has been renumbered to R5 and its subrequirements clarified. For example, reference to "any given moment" has been removed, the correlation with CIP-004 has been added, and the reference to strong authentication methods removed.
007-R7	R7.3 Re-write to say, "The Responsible Entity shall maintain logs of system events to enable analysis." R7.5 Is not technically feasible and should be removed.	The requirement has been reworded. Technical feasibility is address in R7, which has been renumbered to R6.
007-R8	R8.3 Remove word "business."	Reference to business has been removed.
007-R9	R9 Should re-tilte as "Cyber Asset Security Controls" and re-write to say, "The Responsible Entity shall perform a cyber security controls assessment of Cyber Assets within the Electronic Security Perimeter at least annually. The assessment shall include, at a minimum, the following:" R9.1 Remove word "vulnerability."	R9 has been renumbered to R8. The title accurately reflects the intent of the requirement.
007-R10	R10 Change word "referenced" to "required."	The requirement has been updated.
007-M1		
007-M2	Measures M2.1, M2.2 & M2.3 should be rephrased as measures	
007-M3		
007-M4	Remove "...and business...".	Reference to business has been removed. The measures have been rewritten to refer back to the requirements.
007-M5		
007-M6		

007-M7		
007-M8		
007-M9		
007-M10		
007-C1,1		
007-C1,2		
007-C1,3	t is not clear when you mean documents, records, or data. These are three distinct items and should not be referenced interchangeably. Please clarify.	The Drafting Team has revised the standards for consistency and uses the terms as follows: DATA: information in a raw form. RECORDS: objective evidence that an activity has occurred. Records typically provide a snapshot in time of past actions and events, and can be used to demonstrate compliance. Records can only be modified or revised in compliance with proper and auditable trails. LOGS: Generally, collections of records of events that are generated automatically or by following a manual process. They identify who or what caused the event to be written and are time-stamped to indicate when the event occurred. DOCUMENTS: demonstrate what an organization does and plans to do and instruct employees how they should perform their tasks. Documents include but are not limited to policies, processes and procedures, specifications, drawings, maps, etc. A document can be in paper or electronic format.
007-C1,4		
007-C2,1	2.1.2 Re-write as, "Any one of the required documents has not been reviewed in the previous full calendar year;" 2.1.2 Re-write as, "Any one of the required documents has not been updated within 30 calendar days of any changes to the system security controls;" 2.1.4 b2 - Should be remove - seven days appear anywhere in the requirements. 2.1.4 b4 - Should be remove - requirement removed as too excessive.	The levels of noncompliance have been rewritten to reflect changes to requirements and measures as well as severity of infraction.
007-C2,2	2.2.2 Remove - 16 months is outside of one full calendar year. 2.2.3 Remove - 60 days does not appear in requirements. 2.2.4 b2 - Should be remove - seven days appear anywhere in the requirements. 2.2.4 b4 - Should be remove - requirement removed as too excessive.	The levels of noncompliance have been rewritten to reflect changes to requirements and measures as well as severity of infraction.
007-C2,3	2.3.2 Remove - 20 months is outside of one full calendar year.	The levels of noncompliance have been rewritten to reflect changes to

	2.3.4 b2 - Should be remove - seven days appear anywhere in the requirements. 2.3.4 b4 - Should be remove - requirement removed as too excessive.	requirements and measures as well as severity of infraction.
007-C2,4	2.4.4 b2 - Should be remove - seven days appear anywhere in the requirements. 2.4.4 b4 - Should be remove - requirement removed as too excessive.	The levels of noncompliance have been rewritten to reflect changes to requirements and measures as well as severity of infraction.

CIP-007 Drafting Team Responses to Comments

Name	Tim Hattaway
Entity	Alabama Electric Cooperative
Ready to Ballot	Yes
General Comments	
007-R1	
007-R2	
007-R3	
007-R4	
007-R5	
007-R6	
007-R7	
007-R8	
007-R9	
007-R10	
007-M1	
007-M2	
007-M3	
007-M4	
007-M5	
007-M6	
007-M7	
007-M8	
007-M9	
007-M10	

CIP-007 Drafting Team Responses to Comments

007-C1,1

007-C1,2

007-C1,3

007-C1,4

007-C2,1

007-C2,2

007-C2,3

007-C2,4

CIP-007 Drafting Team Responses to Comments

Name	Jerry Heeren	
Entity	MEAG Power	
Ready to Ballot	No	
General Comments		
007-R1		
007-R2		
007-R3		
007-R4		
007-R5		
007-R6	R6.2.2 The statement in this section needs to be clarified further - i.e., when supported, setting up multiple administrative accounts for accountability purposes is not always a good practice. Setting up multiple root equivalent accounts can make a UNIX based system more vulnerable.	R6 has been renumbered to R5 and reworded for clarity.
007-R7		
007-R8		
007-R9		
007-R10		
007-M1		
007-M2		
007-M3		
007-M4		
007-M5		
007-M6		
007-M7		
007-M8		
007-M9		

007-M10

007-C1,1

007-C1,2

007-C1,3

007-C1,4

007-C2,1

007-C2,2

007-C2,3

007-C2,4

CIP-007 Drafting Team Responses to Comments

Name	Peter Henderson	
Entity	Independent Electricity System Operator (IESO)	
Ready to Ballot	No	
General Comments	It is unreasonable to require that documents referenced in this standard should be revised within 30 days of a change to the systems or controls. Even minor changes to network configurations or the addition of a single hardware element could require updating the large number of documents specified in this standard. The sheer volume of work involved is very likely to take considerably more than 30 days. Furthermore, since this standard applies to all cyber assets within the electronic security perimeter, the frequency of change could be high for organizations with large numbers of assets within the security perimeter. It is conceivable that the documentation required would be under constant revision (hence making it effectively impossible to establish a measurable date on which the revision is complete). A requirement to update the documents at least annually would be more sensible. It is unclear in the Compliance section what is meant by the terms "system security controls" or "documented system security controls"since these terms are never defined in the standard. If the intent is to refer to M1 through M10, this should be clearly stated. Compliance levels in this Standard are not consistent with those established in CIP-005 and CIP-006 for similar levels of logging system unavailability. Remove the first sentence of the purpose since it is redundant with the rest of the purpose. We prefer the second and third sentence of the purpose.	The standard has been updated to require changes to procedures be updated within 90 calendar days of a change resulting from a modification. Ninety days reflects industry consensus. System security controls in the Compliance Section refer to the requirements of CIP-007. They have been reveiwed and modified for consistency with other cyber security standards. The purpose has been reworded.
007-R1	The wording of R1 requires clarification given that some requirements in this standard refer specifically to Critical Cyber Assets rather than to the more generic "cyber assets". For instance, R8 requires data destruction or removal prior to disposal of a Critical Cyber Asset. On one hand, the wording of R1 could be taken to mean that one should replace the words "Critical Cyber Assets" by the words "Critical and Non-Critical Cyber Assets" when interpreting the standard. Under this interpretation, the Responsible Entity should wipe data on all assets prior to disposal. Alternatively, one could argue that the wording of R8 explicitly excludes non-critical cyber assets, and therefore failure to consider wipe data from non-critical cyber assets does not give rise to non-compliance. Please clarify.	The drafting team has clarified that all requirements in CIP-007 apply to both Critical and non-critical Cyber Assets within the Electronic Security Perimeter.
007-R2	R2 requires that testing be done but it is unclear what that testing is to accomplish.	CIP-007 R2 addresses testing to verify that changes do not adversely affect security controls required in CIP-007.
007-R3		
007-R4		

007-R5	R5 requires that virus signatures must be explicitly assessed for applicability, installed under change management and configuration management control, and that all of this must be documented. This is overly prescriptive as it does not contemplate Responsible Entities employing auto-update services commonly offered by service providers.	The requirement has been reworded. The Responsible Entity is now required to document and implement a process for updating signatures. The process must address testing and installation.
007-R6	1. R6.1.1 should be reworded to state, "Wherever technically practical, ….. 2. There is a verb missing in R6.1.5. 3. R6.1.5 is redundant given the requirements of CIP-003 R5 and CIP-004 R4. R6.1.5 should be deleted. 4. There appears to be overlap between R6.2.2 and R6.1.1. To avoid confusion, the wording of R6.1 should be modified to include coverage of factory default accounts, and R6.2.2 deleted. 5. The requirement for an audit trail of account use in R6.2.4 overlaps the audit requirement in R6.2.5. These requirements should be combined in R6.2.4, and R6.2.5 deleted to avoid confusion. 6. In R6.3.2 -- the special character requirement should be removed. This is not enforceable on many systems including AD. (AD allows enforcement of only 3 of 4 items).	R6 has been renumbered to R5 and its subrequirements clarified. For example, reference to "any given moment" has been removed, the correlation with CIP-004 has been added, and the reference to strong authentication methods removed. R5 is subject to technical feasibility.
007-R7		
007-R8		
007-R9	R9 should read as Critical Cyber Assets throughout.	The drafting team intends the requirements to apply to all Cyber Assets within the Electronic Security Perimeter and has updated the standard to clarify this issue.
007-R10		
007-M1		
007-M2	1. Measure M2.1, as written, specifies a requirement. Requirements should be specified only in the Requirements section of the document. 2. Measure M2.3 establishes a requirement new to this standard -- to formally accept test results indicative of successful completion of changes to Critical Cyber Assets. This new requirement should not be established in the Measures section. Consider moving this measure to CIP-003 and associating it with R6.2 3. Measures M2.1, M2.2 and M2.3 should be rephrased as measures.	The measures have been rewritten to reference back to the requirements.
007-M3		
007-M4		
007-M5		

007-M6		
007-M7		
007-M8		
007-M9		
007-M10		
007-C1,1		
007-C1,2		
007-C1,3		
007-C1,4		
007-C2,1	Compliance statement 2.1.4 effectively establishes a new requirement for annual review of access privileges and authorization rights. If this is a requirement, it should be established in the Requirements section. Furthermore, this compliance statement should be reviewed for consistency against compliance statements 2.1.1 and 2.2.1 of CIP-004.	The levels of noncompliance have been rewritten to reflect changes to requirements and measures as well as severity of infraction.
007-C2,2		
007-C2,3		
007-C2,4		

CIP-007 Drafting Team Responses to Comments

Name	E. Nick Henery	
Entity	SMUD	
Ready to Ballot	Yes	
General Comments	The Drafting Team will need to go through the Standard and assign responsibility to each function from the functional model like the Version 0 STD. For this Standard to enforceable the generic use of Responsible Entity is the same as the generic use of Control Area. Even if the Standard lists the different functions it leaves open the possibility of misinterpretation as to which function is truly responsible.	The Responsible Entities are clearly enumerated in the standard Section A, item 4.
007-R1		
007-R2		
007-R3		
007-R4		
007-R5		
007-R6		
007-R7		
007-R8		
007-R9		
007-R10		
007-M1		
007-M2		
007-M3		
007-M4		
007-M5		
007-M6		
007-M7		
007-M8		
007-M9		

CIP-007 Drafting Team Responses to Comments

007-M10

007-C1,1

007-C1,2

007-C1,3

007-C1,4

007-C2,1

007-C2,2

007-C2,3

007-C2,4

CIP-007 Drafting Team Responses to Comments

Name	Jack Hobbick	
Entity	Consumers Energy	
Ready to Ballot	No	
General Comments	Consumers Energy has also submitted comments via the ECAR CIPP.	Please see responses to Larry Conrad, ECAR CIPP.
007-R1		
007-R2		
007-R3		
007-R4		
007-R5		
007-R6		
007-R7		
007-R8		
007-R9		
007-R10		
007-M1		
007-M2		
007-M3		
007-M4		
007-M5		
007-M6		
007-M7		
007-M8		
007-M9		
007-M10		

CIP-007 Drafting Team Responses to Comments

007-C1,1

007-C1,2

007-C1,3

007-C1,4

007-C2,1

007-C2,2

007-C2,3

007-C2,4

Name	Richard Kafka	
Entity	Pepco Holdings, Inc.	
Ready to Ballot	No	
General Comments	Is applicability paragraph A4.2.3 missing?	A4.2.3 has been added.
007-R1		
007-R2		
007-R3	This appears to duplicate the requirements of CIP-005 at R2.1.1 and R2.1.2, and at R4.2, as well as to require an individual accounting of each and every single port and service.	CIP-005 refers to devices on the Electronic Security Perimeter and CIP-007 refers to devices within the Electronic Security Perimeter. The standard no longer requires the documentation of the configuration and status of all ports and services inside the Electronic Security Perimeter.
007-R4	R4.2 appears to require an individual accounting of each and every single patch. Clarify in FAQ or in standard. Should patches be applied that break warranties? How is this audited? How can you determine?	The requirement has been clarified. It does not explicitly define how patches are to be applied. Responsible Entities are expected to use reasonable business judgment when implementing the requirements of these standards.
007-R5		
007-R6	Add within calendar year.	This comment does not have enough specificity to address.
007-R7		
007-R8		
007-R9	Ssuggest modifying this Requirement to cover only 1/5 of the assets in any one year, or to permit pro-forma assessments, for example only assessing changes and otherwise indicating "no change."	An annual assessment of Cyber Assets within the ESP is essential to protecting the Critical Cyber Assets.
	In addition, this Requirement should cover only "Critical" Cyber Assets, since other covered assets are addressed in R1.	Protecting non-critical cyber assets residing within the same Electronic Security Perimeter as Critical Cyber Assets is essential because the non-critical cyber assets introduce vulnerabilities exposing the Critical Cyber Assets to threats that must be protected against.
007-R10	How audit any modification?	Compliance auditors will review available documentation.
007-M1		
007-M2		
007-M3		
007-M4	The term "business records" is used here, when "records" alone is used in similar measures such as M3, and in M5 through M9. We suggest deleting the unnecessary word "business" in this Measure.	Reference to business has been removed. The measures have been rewritten to refer back to the requirements.

007-M5		
007-M6		
007-M7		
007-M8		
007-M9	NERC and or the Regions need to address the protection of sensitive information, both regarding auditors themselves and regarding litigation "discovery" and use.	All documentation required in this standard will remain in the possession of the Responsible Entity. It is the up to the Responsible Entity to protect sensitive information by Non-disclosure Agreements (NDA) or similar documents at all times, including audits. Information protection is addressed in CIP-003.
007-M10	Any documentation?	The requirement applies to all documentation required by the standard.
007-C1,1		
007-C1,2		
007-C1,3		
007-C1,4		
007-C2,1		
007-C2,2		
007-C2,3		
007-C2,4		

Name	Tony Kroskey	
Entity	Brazos Electric Power Cooperative	
Ready to Ballot	No	
General Comments	Subsection 4.2, remove the word "entities".	Reference to entities has been removed.
007-R1		
007-R2		
007-R3		
007-R4	R4., suggest changing text "installation of applicable cyber security software patches" to "installation of available cyber security software patches" or just delete the word "applicable".	The requirement has been clarified. It does not explicitly define how patches are to be applied. Responsible Entities are expected to use reasonable business judgment when implementing the requirements of these standards.
007-R5		
007-R6	R6.1.4, should this be moved to CIP005? Also should clarify what "field devices" are.	This requirement has been removed.
007-R7		
007-R8		
007-R9		
007-R10		
007-M1		
007-M2		
007-M3		
007-M4		
007-M5		
007-M6		
007-M7		
007-M8		
007-M9		

CIP-007 Drafting Team Responses to Comments

007-M10

007-C1,1

007-C1,2

007-C1,3

007-C1,4

007-C2,1

007-C2,2

007-C2,3

007-C2,4

Name	Carol Krysevig	
Entity	Allegheny Energy Supply Co. LLC	
Ready to Ballot	No	
General Comments	D1.3.1 -- Clarification needed on exactly what 'all data' refers to. D2.1.4, D2.2.4, D2.3.4 and D2.4.4 -- The second bullet in each section refers to a 7-day gap in 'any one log.' Previous version of standards specified which logs applied. The logs should be specifically defined. 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.' Some of the specific requirements in both sections appear to be duplicative. The Cyber Vulnerability Assessment requirement should be placed in one standard and be all-inclusive, or should be more clearly be cross-referenced.	D1.3.1 has been changed to documentation and records. It refers to the documentation and records identified in the requirements. Please see the FAQ. The logs are those identified in the requirements.
007-R1		
007-R2	R2. - 'significant change' seems to include any change to application software, 3rd party software, or firmware. This is a rather cumbersome requirement and should be clarified further.	The requirement has been reworded to clarify significant change.
007-R3		
007-R4	R4.1. - The requirement to document the assessment of security patches and upgrades for applicability within 30 calendar days of availability is too restrictive. Also, recognize that doing the assessment on a timely basis may not ensure application of the patch or upgrade shortly thereafter. In a power station, some patches or upgrades may need to wait for a unit outage. Also, certain patches or upgrades may not be installed if the vendor does not support them.	The 30 day requirement applies to assessment rather than implementation. The requirement has been clarified.
007-R5	R5.1. - 'The Responsible Entity shall document the assessment of anti-virus and integrity monitoring tool signatures for applicability within 30 calendar days of availability.' Same comment as R4.1 above.	The requirement has been reworded. The Responsible Entity is now required to document and implement a process for updating signatures. The process must address testing and installation.
007-R6	R6.1.4 -- The additional requirement of 'Field devices that do not enforce electronic access control must have physical protections to appropriately control access to said devices' is confusing and needs clarification. R6.2.2. - Change 'technically supported' to 'technically and operationally supported'. Sometimes when things are technically possible, that doesn't mean that they can be worked into an operational framework. This wording may be in several other places as well. R6.3.1-3 - These should be replaced with a generic statement about appropriate password construction.	This requirement has been removed. Please refer to the FAQ on technical feasibility. The requirements address industry comments asking for more specificity. The drafting team finds it more clear to describe password construction as a list of requirements rather than a single generic statement.
007-R7		
007-R8	R8.2. - Redeployment within the same kind of electronic and physical perimeter should be permitted without storage erasure. In other words, one should be able to move a computer from	Correct. If systems are deployed outside an Electronic Security Perimeter, however, the data should be erased.

	one secure area to another secure area without erasure -- when needed.	
007-R9		
007-R10		
007-M1		
007-M2		
007-M3		
007-M4	Specify exactly what documents and business records looking for.	The measures have been rewritten to refer back to the requirements.
007-M5	Specify exactly what documents and business records looking for.	The measures have been rewritten to refer back to the requirements.
007-M6	Specify exactly what documents and business records looking for.	The measures have been rewritten to refer back to the requirements.
007-M7	Specify exactly what documents and business records looking for.	The measures have been rewritten to refer back to the requirements.
007-M8	The measures have been rewritten to refer back to the requirements.	The measures have been rewritten to refer back to the requirements.
007-M9	Specify exactly what documents and business records looking for.	The measures have been rewritten to refer back to the requirements.
007-M10		
007-C1,1		
007-C1,2		
007-C1,3		
007-C1,4		
007-C2,1		
007-C2,2		
007-C2,3		
007-C2,4		

Name	John Lim	
Entity	Con Edison	
Ready to Ballot	No	
General Comments	Remove the first sentence of the purpose since it is redundant with the rest of the purpose. We prefer the second and third sentence of the purpose. For consistency, this Standard should include an Applicability 4.2.3, "Responsible Entities that, in compliance with CIP-002, identify that they have no Critical Cyber Assets."	Please see responses to Ray A'Brial, Central Hudson Gas & Electric Corp.
007-R1	The wording of R1 requires clarification given that some requirements in this standard refer specifically to Critical Cyber Assets rather than to the more generic "cyber assets". For instance, R8 requires data destruction or removal prior to disposal of a Critical Cyber Asset. On one hand, the wording of R1 could be taken to mean that one should replace the words "Critical Cyber Assets" by the words "Critical and Non-Critical Cyber Assets" when interpreting the standard. Under this interpretation, the Responsible Entity should wipe data on all assets prior to disposal. Alternatively, one could argue that the wording of R8 explicitly excludes non-critical cyber assets, and therefore failure to consider wipe data from non-critical cyber assets does not give rise to non-compliance. Please clarify. Change; Non-critical Cyber Assets as well as the Critical Cyber Assets defined in CIP-002 within the Electronic Security Perimeter(s) defined in CIP-005 shall be subject to the requirements of this standard. to; Non-critical Cyber Assets, and the Critical Cyber Assets defined in CIP-002, within the Electronic Security Perimeter(s) defined in CIP-005 shall be subject to the requirements of this standard.	
007-R2	Request clarification on R2. Does this Standard apply to Critical Cyber Assets or Cyber Assets? For clarification, change to "security patches, cumulative service packs, vendor releases, or version upgrades as applied to operating systems, applications, database platforms, or other third-party software or firmware."	
007-R3		
007-R4		
007-R5		
007-R6		
007-R7	Change R7.4 to:The Responsible Entity shall retain logs for 90 calendar days unless longer	

	retention is required pursuant to CIP-008-1, R2.
007-R8	
007-R9	
007-R10	
007-M1	
007-M2	Measures M2.1, M2.2 and M2.3 should be rephrased as measures.
007-M3	
007-M4	
007-M5	
007-M6	
007-M7	
007-M8	
007-M9	
007-M10	
007-C1,1	
007-C1,2	
007-C1,3	
007-C1,4	
007-C2,1	
007-C2,2	
007-C2,3	
007-C2,4	

CIP-007 Drafting Team Responses to Comments

Name	Deborah Linke	
Entity	Bureau of Reclamation	
Ready to Ballot	No	
General Comments	General Comment: Reclamation believes that a more sound approach would be to use a risk-based security management program. You may wish to consider a requirement to follow a risk management lifecycle process for mitigating risk to an acceptable level.	The cyber security standards embody the concept of risk management. The standards development process itself relies on industry consensus to identify minimum levels of acceptable risk. The intent of the standards is to provide a minimum level of consistency across the industry. As long as the requirements of these standards are met, the Responsible Entity is free to use its own risk assessment process to manage risk.
007-R1	R1: Reclamation is particularly concerned about the requirement to manage non-critical cyber assets the same way as Critical Cyber Assets. Responsible entities should be required to evaluate the threats, vulnerabilities, and risks associated with non-critical cyber assets and apply appropriate mitigation.	CIP-007 has been clarified to state that all requirements in CIP-007 apply to both Critical and non-critical Cyber Assets in the Electronic Security Perimeter. Protecting non-critical Cyber Assets residing within the same Electronic Security Perimeter as Critical Cyber Assets is essential because the non-critical Cyber Assets introduce vulnerabilities exposing the Critical Cyber Assets to threats that must be protected against.
007-R2	R2: The testing requirements in this section seem to be redundant of those required under CIP-003, R6. We suggest eliminating R2, R2.1, R2.2, and R2.3. R3: R3.9.2 appears to repeat the requirement in CIP-005, R2 which requires that all unnecessary ports and services be disabled. R6: R6 appears to repeat the requirements in CIP-003, R5. If these are removed, the measures need to be revised accordingly.	Testing has been removed from CIP-003. CIP-007 R2 addresses testing to verify that changes do not adversely affect security controls required in CIP-007. CIP-005 applies to devices on the Electronic Security Perimeter and CIP-007 applies to devices within the Electronic Security Perimeter. CIP-007 applies to access controls on Cyber Assets and has been updated to reference CIP-003.
007-R3		
007-R4	R4.1: States that upgrades must be assessed with 30 days. This should only apply to security related upgrades. Change wording to "security upgrades."	The requirement has been modified as suggested.
007-R5		
007-R6		
007-R7	R7.5: When using automated tools, as is encouraged in R7, it is unnecessary to review all logs. Reclamation suggests focusing on the review of alarms and events related to cyber security incidents.	The intent of the requirement is to alert and alarm, and review of logs. Those processes may be manual or automated as deemed appropriate by the Responsible Entity.
007-R8		
007-R9	R9: Given the very broad definition of Critical Cyber Assets, the requirement for cyber vulnerability assessments inside every Electronic Security Perimeter could become very burdensome. Focusing on control centers is more appropriate, with perimeter scans used for other	An annual assessment of Cyber Assets within the Electronic Security Perimeter is essential to protecting the Critical Cyber Assets.

	remote Electronic Security Perimeters.	
007-R10		
007-M1	M1: A list of non-critical Cyber Assets is unnecessary and will be time consuming and costly to maintain. Reclamation suggests removing this measure.	The measures have been rewritten to refer back to the requirements.
007-M2		
007-M3		
007-M4		
007-M5		
007-M6		
007-M7		
007-M8		
007-M9		
007-M10		
007-C1,1		
007-C1,2		
007-C1,3		
007-C1,4		
007-C2,1		
007-C2,2		
007-C2,3		
007-C2,4		

CIP-007 Drafting Team Responses to Comments

Name	Greg Mason
Entity	Dynegy Generation
Ready to Ballot	No
General Comments	
007-R1	
007-R2	
007-R3	
007-R4	
007-R5	
007-R6	
007-R7	
007-R8	
007-R9	
007-R10	
007-M1	Same comment as on R1 of CIP-005
007-M2	
007-M3	
007-M4	
007-M5	
007-M6	
007-M7	
007-M8	
007-M9	
007-M10	

CIP-007 Drafting Team Responses to Comments

007-C1,1

007-C1,2

007-C1,3

007-C1,4

007-C2,1

007-C2,2

007-C2,3

007-C2,4

Name	Paul McClay	
Entity	Tampa Electric	
Ready to Ballot	No	
General Comments	Applicability Section is missing the 4.2.3 wording found in other standards. Applicability 4.2.4 should be added to exclude non-critical cyber assets which reside within the physical perimeter, are not used for any electronic or physical control, and are not in the electronic perimeter	Please see responses to Linda Campbell, FRCC.
007-R1	Non critical assets should be subject to the requirements of this standard with the exception of R2 (if not critical, it is not going to affect systems that can cause reliability problems, so testing while possibly still prudent depending on the asset, should not be required to be documented for these assets) and R8 (If the asset is non-critical, why do you care about its disposition or redeployment?)	
007-R2		
007-R3	In the last sentence, where the Responsible Entity must document unused ports and services that cannot be disabled, it this documented as an exception? If yes, then explicitly state that. Scanning should not be required, so delete the reference to CIP-005.	
007-R4	R.4.2 If cannot be installed, is this documented as an exception? If yes, then explicitly state that.	
007-R5	R.5.2 If cannot be installed, is this documented as an exception? If yes, then explicitly state that.	
007-R6	R6.1.5 I don't see any review checklists defined in CIP-003 or 004 -- what is "review checklists" referring to?? If truly an example, and not required, perhaps this belongs in the FAQs. R6.3 This requirement as worded appears to prescribe all 3 sub-requirements if a password is technically possible. A password may be technically available, yet not have the capability to provide all three controls. We suggest clarifying the wording -- the responsible entity shall require and utilize passwords where technically available and the passwords shall be subject to the following controls as technically feasible:......	R6 has been renumbered to R5 and clarified. The requirements for passwords are subject to technical availabiity.
007-R7	Change the first sentence to "The Responsible Entity shall implement, as technically feasible, automated tools or organizational process controls to monitor the system cyber security events of Critical Cyber Assets within the electronic Security Perimeter. Cyber Assets don't "implement"; people do. R7.3 This requirement is not specific enough. How would you measure that the events are there in "sufficient detail to enable a root-cause analysis" There is no requirement to perform a root-cause analysis, so why do you need the detailed information? R7.4 Move this to section D1.3 with other data retention.	

	R7.5 What constitutes a "business record" and how does it differ from measures in previous sections of the standards from "data", "document" or "documentation."
007-R8	R8.2 If a critical cyber asset is being redeployed, only stored data related to the critical cyber asset or reliability of the grid should be required to be erased or destroyed, not all data storage on the asset. If an employee’s workstation or a server with no critical information is being moved outside the cyber perimeter (redeployed), there is no cause to delete information on that equipment. Change 8.2 to Prior to redeployment of Critical Cyber Assets, the Responsible Entity shall at a minimum evaluate the data stored on the asset, and erase any data that should not be accessed by unauthorized personnel. R8.3 What constitutes a "business record" and how does it differ from measures in previous sections of the standards from "data", "document" or "documentation."
007-R9	
007-R10	
007-M1	
007-M2	M2.3 Is this referencing the approval specified in R6.2 in CIP-003-1? If so they are accepting the "testing results" rather than the "successful completion of changes." There is no requirement specified for the acceptance of the successful completion of changes.
007-M3	
007-M4	M4 How do documentation and business records differ? Clarify the measure if there is a difference or use only documentation.
007-M5	How do documentation and records differ? Clarify the measure if there is a difference or use only documentation.
007-M6	How do documentation and records differ? Clarify the measure if there is a difference or use only documentation.
007-M7	How do documentation and records differ? Clarify the measure if there is a difference or use only documentation.
007-M8	
007-M9	How do documentation and records differ? Clarify the measure if there is a difference or use only documentation.
007-M10	
007-C1,1	
007-C1,2	
007-C1,3	D1.3.1 Should this exclude logs from R7.4 and R6.1.3 or specifically mention here only 90 days for those? What is the reason to keep Individual User Account Activity Logs (R6.1.3) which can be

	extremely large for the previous calendar year? Suggest deleting that retention schedule or shortening to 90 days.
007-C1,4	
007-C2,1	
007-C2,2	
007-C2,3	
007-C2,4	

CIP-007 Drafting Team Responses to Comments

Name	David McCoy	
Entity	Great Plains Energy/Kansas City Power & Light	
Ready to Ballot	No	
General Comments	Most of the other standards have a 4.2.3 provision. It appears that this was overlooked on this standard	A4.2.3 has been added.
007-R1		
007-R2		
007-R3	Documentation of "the status and configuration of all ports and services" is too onerous. This requirement should be eliminated.	The standard no longer requires the documentation of the configuration and status of all ports and services inside the Electronic Security Perimeter.
007-R4		
007-R5		
007-R6	After the words "at any moment in time" you should add the words "within the previous year."	Reference to "any point in time" has been removed.
007-R7		
007-R8		
007-R9		
007-R10		
007-M1		
007-M2		
007-M3		
007-M4		
007-M5		
007-M6		
007-M7		
007-M8		
007-M9		

CIP-007 Drafting Team Responses to Comments

007-M10

007-C1,1

007-C1,2

007-C1,3

007-C1,4

007-C2,1

007-C2,2

007-C2,3

007-C2,4

CIP-007 Drafting Team Responses to Comments

Name	Don Miller	
Entity	First Energy Corp	
Ready to Ballot	Yes	
General Comments		
007-R1	If non-critical and critical cyber assets are subject to this standard then we should just state all Cyber Assets within the perimeter are subject to the standard period.	The drafting team has clarified that all requirements in CIP-007 apply to both Critical and non-critical Cyber Assets in the Electronic Security Perimeter.
007-R2		
007-R3		
007-R4		
007-R5		
007-R6		
007-R7		
007-R8		
007-R9		
007-R10		
007-M1		
007-M2		
007-M3		
007-M4		
007-M5		
007-M6		
007-M7		
007-M8		
007-M9		

007-M10

007-C1,1

007-C1,2

007-C1,3

007-C1,4

007-C2,1

007-C2,2

007-C2,3

007-C2,4

Name	Patrick Miller	
Entity	PacifiCorp	
Ready to Ballot	No	
General Comments		
007-R1		
007-R2		
007-R3		
007-R4		
007-R5		
007-R6	For R6, consider adding language so that paragraph would read: "Account Management - The Responsible Entity shall establish, implement, and document account management methods that enforce access authentication and individual accountability of user activity where technically feasible, and minimize the risk of unauthorized system access.	R6 has been renumbered t o R5 and clarified.
	For R6.1.1, there is no mention of how "application accounts" are to be handled. This leaves open a potential loophole.	If the Responsible Entity implements access control at the application level, the requirements of this standard apply.
	For R6.3.1, six characters is below the standard best practice of eight.	Not all control systems support eight characters. It is the consensus of commenters that six characters is acceptable. This does not preclude the entity from using eight.
007-R7		
007-R8	For R8.x, there are no criteria for the destruction or erasing of the data storage media. Consider, at a minimum, adding language speaking to the concept that simple deletion is not sufficient for erasing.	The requirement says "to prevent retrieval of critical cyber security or reliability data". Erasures that do not prevent retrieval do not meet the requirement.
007-R9		
007-R10		
007-M1		
007-M2		
007-M3		
007-M4		

CIP-007 Drafting Team Responses to Comments

007-M5

007-M6

007-M7

007-M8

007-M9

007-M10

007-C1,1

007-C1,2

007-C1,3

007-C1,4

007-C2,1

007-C2,2

007-C2,3

007-C2,4

CIP-007 Drafting Team Responses to Comments

Name	Jeff Mitchell
Entity	ECAR
Ready to Ballot	Yes
General Comments	N/A
007-R1	
007-R2	
007-R3	
007-R4	
007-R5	
007-R6	
007-R7	
007-R8	
007-R9	
007-R10	
007-M1	
007-M2	
007-M3	
007-M4	
007-M5	
007-M6	
007-M7	
007-M8	
007-M9	
007-M10	

CIP-007 Drafting Team Responses to Comments

007-C1,1

007-C1,2

007-C1,3

007-C1,4

007-C2,1

007-C2,2

007-C2,3

007-C2,4

CIP-007 Drafting Team Responses to Comments

Name	Scott Mix	
Entity	KEMA, Inc	
Ready to Ballot	No	
General Comments	Since the standards have been split up into multiple standards, the titles should be made clearer so that they stand on their own. Therefore, I am resubmitting the request to change the title of this standard to "Critical Cyber Asset System Security Management".	The drafting team believes the title is adequate.
007-R1	The requirement to document the non-Critical Cyber Assets within the Electronic Security Perimeter is duplicated in CIP-005 Requirement R1.6. It should only be in one location (probably here).	
007-R2		
007-R3		
007-R4		
007-R5		
007-R6	There is no specific requirement to disable "unauthorized, invalidated, expired, or unused computer accounts" (a requirement of standard 1212).	These requirements are included in CIP-003 and CIP-004.
	Requirement 6 should include a technical feasibility clause for all the underlying requirements. For example, R6.1.3 may not be possible in substation IED equipment. Alternatively, a technically feasible clause should be inserted into requirements at least R6.1.3, R6.2.4, R6.2.5.	R6 has been renumbered to R5 and clarified. The requirement does not preclude manual processes to comply with these requirements.
007-R7		
007-R8		
007-R9	Requirements R9.2 should read "A non-invasive review and verification …"	The requirement has been reworded to "review to verify;" active port scanning is not required. Please see the FAQs.
007-R10		
007-M1		
007-M2		
007-M3		
007-M4		
007-M5		
007-M6		

CIP-007 Drafting Team Responses to Comments

007-M7

007-M8

007-M9

007-M10

007-C1,1

007-C1,2

007-C1,3

007-C1,4

007-C2,1

007-C2,2

007-C2,3

007-C2,4

CIP-007 Drafting Team Responses to Comments

Name	Darrick Moe	
Entity	WAPA	
Ready to Ballot	No	
General Comments		
007-R1		
007-R2	R6 of CIP-003-1 does a good job of sufficiently covering the matter of Testing. R2 of CIP-007-1 should be deleted. If R2 is not entirely eliminated, at least R2.2 should be deleted; it is covered sufficiently by R2.1.	Testing has been removed from CIP-003. CIP-007 R2 addresses testing to verify that changes do not adversely affect security controls required in CIP-007.
007-R3	Requiring that ports and services on the electronic perimeter is a must, and is already required CIP-005. Going beyond this is not sufficiently beneficial to mandate the costs; it should be left to each entity to weigh costs and benefits in this area. The corresponding requirement regarding devices on the perimeter (in CIP-005) is fine; this R3 should be deleted.	CIP-005 refers to devices on the Electronic Security Perimeter and CIP-007 refers to devices within the Electronic Security Perimeter. The standard no longer requires the documentation of the configuration and status of all ports and services inside the Electronic Security Perimeter.
007-R4		
007-R5		
007-R6	The topic of Account Management is sufficiently covered by R5 of CIP-003; R6 of CIP-007 should be deleted. The elements of R6 that are not explicitly covered in CIP-003 are better left to each responsible entity to define in their cyber security policies. The exception is R6.2.1; this requirement should be integrated into the existing R5 of CIP-003.	CIP-007 addresses the requirements for implementing the access rights defined in CIP-003. The standard has been updated to reference CIP-003.
007-R7		
007-R8		
007-R9	R9.2 should be reworded to say: "A review and verification that ports and services are configured in compliance with the entity's Cyber Security Policy(s)"	The requirement has been reworded to "review to verify;" active port scanning is not required. Please see the FAQs.
007-R10	R10 is too broad as currently worded, as it would be too difficult to know what change would require a review. The words "and shall update these documents within thirty calendar days of any modification of the systems or controls" should be deleted.	The requirement has been modified.
007-M1		
007-M2		
007-M3		
007-M4		
007-M5		

007-M6

007-M7

007-M8

007-M9

007-M10

007-C1,1

007-C1,2

007-C1,3

007-C1,4

007-C2,1

007-C2,2

007-C2,3

007-C2,4

CIP-007 Drafting Team Responses to Comments

Name	Selby Mohr
Entity	Sacramento Municipal Utility District
Ready to Ballot	Yes
General Comments	
007-R1	
007-R2	
007-R3	
007-R4	
007-R5	
007-R6	
007-R7	
007-R8	
007-R9	
007-R10	
007-M1	
007-M2	
007-M3	
007-M4	
007-M5	
007-M6	
007-M7	
007-M8	
007-M9	
007-M10	

CIP-007 Drafting Team Responses to Comments

007-C1,1

007-C1,2

007-C1,3

007-C1,4

007-C2,1

007-C2,2

007-C2,3

007-C2,4

CIP-007 Drafting Team Responses to Comments

Name	Kurt Muehlbauer	
Entity	Exelon	
Ready to Ballot	No	
General Comments	The documentation and processes around the responsible entity s tasks are too prescriptive. The industry needs to be extremely careful to avoid the creation of purely documentation-based non-compliances. With increasing legal requirements for compliance, and the associated penalties for noncompliance, noncompliance should be reserved for real security issues. It is simply too easy to make a mistake in documentation in light of the constantly evolving cyber environment. Each entity should develop its own processes in support of the requirements, and these processes should be required to contain provisions for periodic review and approval applicable to each requirement. The processes should also be required to produce reasonable documentation to demonstrate compliance. However, it is not necessary to specify the details of the documentation or review periods. The above approach can be met by removing references to documentation from the requirements section. Then, in the measures section require each entity to reasonably document programs and processes that support the security requirements and to produce reasonable documentation required to demonstrate compliance to the security requirements. Please refer to our overall comments on defining reasonable. If the above approach is taken, it will be possible to delete many of the sub-bullet points under each requirement (because the details will be specified by each entity in their program or process, as applicable). This will also ensure that documentation and excessive low-value administrative tasks are removed from the requirements.	The Drafting Team has reviewed the standards and removed prescription where possible. The prescriptiveness that remains is necessary to provide the clarity requested by a majority of commenters. The documentation required by these standards allow Responsible Entities to demonstrate that the policies, processes, and procedures that they have implemented consistently comply with the requirements of
007-R1	R1. This standard should only apply to critical assets. The wording (document all non-critical Cyber Assets…) Is unclear. What is meant by document?	The drafting team has clarified that all requirements in CIP-007 apply to both Critical and non-critical Cyber Assets in the Electronic Security Perimeter. It also has removed the requirement to list non-critical Cyber Assets within the Electronic Security Perimeter because this requirement is in CIP-005 .
007-R2		
007-R3	Why is this requirement separated from CIP-005 R2.1? Drawing a distinction between being on or within the perimeter is arbitrary for this requirement. Would these requirements ever be executed or audited separately, in the real world? Recommend combining the requirements for clarity sake. Also, we restate the concerns here with CIP-005 R2.1 It is too prescriptive and documentation focused. Consider a network consisting of 1000 nodes. With 64,000 possible ports per node, you then have 64,000,000 data points. And this is even before you add services. Creating configuration documentation that is always representative of the network does not seem feasible. Recommend replacing this requirement with a general measure that requires reasonable documentation that access points within the electronic perimeter have been	CIP-005 refers to devices on the Electronic Security Perimeter and CIP-007 refers to devices within the Electronic Security Perimeter. The standard no longer requires the documentation of the configuration and status of all ports and services inside the Electronic Security Perimeter.

	secured.	
007-R4		these standards.
007-R5	Remove R5.1 and R5.2. Each entity should implement this requirement according to their policies. 5.1 and 5.2 are over prescriptive. Consider replacing them with a general measure to the affect Each entity shall document anti-virus management processes and provide reasonable documentation that the management processes are implemented.	The requirement has been reworded. The Responsible Entity is now required to document and implement a process for updating signatures. The process must address testing and installation.
007-R6	R6.1.2 -- This is redundant. Delete.	The requirement has been renumbered to R5 and clarified.
	R6.1.3 -- This is too prescriptive. At any moment in time is confusing. Delete this requirement.	Reference to "any moment in time" has been removed.
	R6.1.4 -- This is overly prescriptive and redundant. Delete What does field devices mean? Should it say cyber assets?	This sub-requirement has been removed.
	Delete R6.3.1 -- 6.3.3. Each entity should follow its password policies. This is over prescriptive.	The requirements address industry comments asking for more spcificity around passwords.
007-R7	This requirement should not apply to all assets within the perimeter. Each company or organization should have the leeway to define which assets should be monitored, and what type of monitoring is required. If monitoring the perimeter, not every asset within the perimeter must be monitored. The combination of host and network, perimeter and internal monitoring is best implemented by each company or organization, based on their own assessment of risk and network topology.	The intent of the requirement is to alert and alarm, and review of logs. Those processes may be manual or automated as deemed appropriate by the Responsible Entity.
	Why is this requirement separated from CIP-005 R3? Drawing a distinction between being on or within the perimeter is arbitrary for this requirement. Would these requirements ever be executed or audited separately, in the real world? Recommend thinking through this and potentially consolidating the requirements.	The drafting team has thought this through in great detail and does not concur with the suggestion, largely based on the explanation provided in response to comments about 007-R3. Other Cyber Assets in use within the same electronic perimeter as Critical Cyber Assets require the same care and vigilance afforded to the latter to help minimize the potential of cross-contamination.
007-R8	Delete 8.1 to 8.3. Each entity should develop the details of their disposal policy and abide by it. They are overly prescriptive. In place of them, consider adding a measure to the affect, Each entity shall provide reasonable documentation verifying the implementation of the disposal procedures.	The requirements define the minimum actions to be taken. The Responsible Entity is expected to use reasonable business judgment in the implementation of these requirements.
007-R9	Why is this requirement separated from CIP-005 R4? Does the fact that this requirement talks about the access points and the other addresses nodes inside the perimeter, merit separating the requirements? Would these requirements ever be executed or audited separately, in the real world? Recommend thinking through this and potentially consolidating the requirements. Requiring annual vulnerability assessments is a costly way to implement the security benefits of this requirement. Full vulnerability scans are highly intrusive to any network, especially real time and control systems. A more cost effective way to achieve the same result would be to provide more flexibility in how often full scans are done (e.g. at least every 5 years), but making sure security test procedures adequately assess vulnerabilities of any incremental changes, as part of the security testing and change management process.	There is a very distinct difference between ports at the access points and ports on a system. Ports and services at access points should be enabled only for those necessary for servicing requirements that systems within the perimeter have to access resources or applications outside the perimeter, or that originate from outside the perimeter into the perimeter. Ports and services on a system within a perimeter include those necessary to also service those applications and resources within the perimeter as well. The requirement has been reworded to "review to verify;" active port scanning is not required. Please see the FAQs.

Also, there should be an exception in cases where operation requirements for high-availability systems will not permit vulnerability scans.

007-R10

007-M1 Refer to general, overall comments submitted on CIP-002 through CIP-009 regarding revision of the measures and compliance specification.

007-M2 Refer to general, overall comments submitted on CIP-002 through CIP-009 regarding revision of the measures and compliance specification.

007-M3 Refer to general, overall comments submitted on CIP-002 through CIP-009 regarding revision of the measures and compliance specification.

007-M4 Refer to general, overall comments submitted on CIP-002 through CIP-009 regarding revision of the measures and compliance specification.

007-M5 Refer to general, overall comments submitted on CIP-002 through CIP-009 regarding revision of the measures and compliance specification.

007-M6 Refer to general, overall comments submitted on CIP-002 through CIP-009 regarding revision of the measures and compliance specification.

007-M7 Refer to general, overall comments submitted on CIP-002 through CIP-009 regarding revision of the measures and compliance specification.

007-M8

007-M9 Refer to general, overall comments submitted on CIP-002 through CIP-009 regarding revision of the measures and compliance specification.

007-M10 Refer to general, overall comments submitted on CIP-002 through CIP-009 regarding revision of the measures and compliance specification.

007-C1,1 Refer to general, overall comments submitted on CIP-002 through CIP-009 regarding revision of the measures and compliance specification.

007-C1,2 Refer to general, overall comments submitted on CIP-002 through CIP-009 regarding revision of the measures and compliance specification.

007-C1,3 Refer to general, overall comments submitted on CIP-002 through CIP-009 regarding revision of the measures and compliance specification.

007-C1,4 Refer to general, overall comments submitted on CIP-002 through CIP-009 regarding revision of the measures and compliance specification.

007-C2,1 Refer to general, overall comments submitted on CIP-002 through CIP-009 regarding revision of the measures and compliance specification.

007-C2,2 Refer to general, overall comments submitted on CIP-002 through CIP-009 regarding revision of the measures and compliance specification.

007-C2,3 Refer to general, overall comments submitted on CIP-002 through CIP-009 regarding revision of the measures and compliance specification.

007-C2,4	Refer to general, overall comments submitted on CIP-002 through CIP-009 regarding revision of the measures and compliance specification.

Name	Jeffrey Mueller	
Entity	PSEG Companies	
Ready to Ballot	No	
General Comments	The PSEG Companies have reviewed and share the concerns expressed in the Comments of PJM and EEI. Accordingly, the PSEG Companies support the comments of PJM and EEI, and request that the concerns expressed in those comments be properly addressed in the next version of the draft standard.	Please see responses to Laurence W. Brown, Edison Electric Institute.
007-R1		
007-R2		
007-R3		
007-R4		
007-R5		
007-R6		
007-R7		
007-R8		
007-R9		
007-R10		
007-M1		
007-M2		
007-M3		
007-M4		
007-M5		
007-M6		
007-M7		
007-M8		
007-M9		

CIP-007 Drafting Team Responses to Comments

007-M10

007-C1,1

007-C1,2

007-C1,3

007-C1,4

007-C2,1

007-C2,2

007-C2,3

007-C2,4

CIP-007 Drafting Team Responses to Comments

Name	Mitchell Needham	
Entity	Tennessee Valley Authority	
Ready to Ballot	No	
General Comments		
007-R1		
007-R2		
007-R3		
007-R4		
007-R5		
007-R6	The phrase 'where technically feasible' should apply to all of R6. The team should realize that many entities use protective relays which would fall in this category and making time oriented changes might prove very expensive. R6.3 has requirements that might be very difficult to do for protective relays unless the above phrase is adopted. In R6.3.3, changing passwords for protective relays is prohibitive for larger entities.	R6 has been renumbered to R5 and clarifications have been added.
007-R7		
007-R8		
007-R9		
007-R10		
007-M1		
007-M2		
007-M3		
007-M4		
007-M5		
007-M6		
007-M7		
007-M8		

CIP-007 Drafting Team Responses to Comments

007-M9

007-M10

007-C1,1

007-C1,2

007-C1,3

007-C1,4

007-C2,1

007-C2,2

007-C2,3

007-C2,4

CIP-007 Drafting Team Responses to Comments

Name	Dave Norton
Entity	Entergy Transmission
Ready to Ballot	Yes
General Comments	
007-R1	
007-R2	
007-R3	
007-R4	
007-R5	
007-R6	
007-R7	
007-R8	
007-R9	
007-R10	
007-M1	
007-M2	
007-M3	
007-M4	
007-M5	
007-M6	
007-M7	
007-M8	
007-M9	
007-M10	

CIP-007 Drafting Team Responses to Comments

007-C1,1

007-C1,2

007-C1,3

007-C1,4

007-C2,1

007-C2,2

007-C2,3

007-C2,4

CIP-007 Drafting Team Responses to Comments

Name	Doug Orlofske	
Entity	Wisconsin Public Power Inc	
Ready to Ballot	No	
General Comments	If no critical assets have been identified then there is no criteria for defining your electronic perimeter. There is also references to CIP003, CIP004 and CIP005 all of which are exempted for cases where no critical assets have been identified. I think that there needs to be an addition that if there are no critical assets then you are exempted from this standard.	Section A.4.2.3 has been added.
007-R1		
007-R2		
007-R3		
007-R4		
007-R5		
007-R6		
007-R7		
007-R8		
007-R9		
007-R10		
007-M1		
007-M2		
007-M3		
007-M4		
007-M5		
007-M6		
007-M7		
007-M8		
007-M9		

CIP-007 Drafting Team Responses to Comments

007-M10

007-C1,1

007-C1,2

007-C1,3

007-C1,4

007-C2,1

007-C2,2

007-C2,3

007-C2,4

CIP-007 Drafting Team Responses to Comments

Name	Kevin Perry	
Entity	Southwest Power Pool	
Ready to Ballot	No	
General Comments	Implementation of all of the requirements in this standard will be hugely expensive in terms of dollar cost, infrastructure cost, and additional staffing required to maintain and review the required documentation.	The documentation required by these standards allows Responsible Entities to demonstrate that the policies, processes, and procedures that they have implemented consistently comply with the requirements of these standards. The drafting team believes the proposed Implementation Schedule affords Responsible Entities the time needed to comply.
007-R1		
007-R2	R2: A "significant change" does not necessarily need to include the installation of a security patch. To require extensive system testing of each and every CCA, as might be required under the provisions of the standard will unnecessarily delay the roll out of security patches to systems at risk, especially the non-CCA systems co-located within the electronic security perimeter. Each change should be evaluated with respect to its impact and tested accordingly.	The requirement is to ensure that the application of patches does not adversely affect security controls required in CIP-007. The extensiveness of the testing is determined by the Responsible Entity and depends on the the Responsible Entity's evaluation of the patch and the problem that the patch is intended to resolve.
007-R3		
007-R4	R4.1: Taking up to 30 days to evaluate a security patch is excessive. The time between identifying a vulnerability and an exploit is typically less than two weeks. Evaluation of upgrades within a 30-day timeframe is also unnecessary. There are many reasons why an upgrade will not be implemented in the short term, including budgeting, system/application incompatibilities, product migration/retirement plans, etc. Entities will often need to take their lead from their vendors and to require an independent evaluation of every possible upgrade within 30 days is unreasonable.	30 days reflects industry consensus. The Responsible Entity may be more restrictive. The reference to upgrade has been changed to security upgrade.
007-R5	R5.1: Many sites use automated processes to constantly update their anti-virus signature files. To require an assessment of each update, which can occur daily in the case of anti-virus signature files, is excessive and unnecessary. Where an evaluation is necessary, a 30-day time frame is also unreasonable. Waiting up to 30 days to evaluate and then apply an anti-virus update unnecessarily exposes systems to considerable risk. The standard should require a much more frequent check (automatic or manual) for updates. R5.2: Documentation should be required only in the cases where the update was not applied. An audit of the update processes and the protected systems on a periodic basis to ensure the update process is working may be necessary. To document each and every update is onerous, especially where the updates are completely automated.	The requirement to assess anti-virus updates within 30 days has been removed. R5.2 has been renumbered to R4.2 and reworded. The Responsible Entity is now required to document and implement a process for updating signatures. The process must address testing and installation.
007-R6	R6.1.3 is onerous. The impact to system performance and the mass storage requirement for logs to track user activities at any moment in time is huge. Especially when this requirement extends to non-CCA systems. Up to two years of detailed log data would have to be retained under this requirement. Many operating systems do not have a provision to log selected user accounts and not others. It is often an all-or-nothing option.	The drafting team has updated the standard to remove the reference to "any moment in time" and defined the retention period as 90 calendar days.

	R6.2.2: While the ability to use individually assigned user accounts may be technically feasible, there may be perfectly valid business reasons to permit the use of a shared account. An example is the operator workstations in the control room. Entities cannot suffer the loss of visibility that occurs for several minutes whenever a user logs out and another logs in. It is appropriate to require individual accounts on such highly privileged accounts such as the Administrator account. To make a blanket requirement to include user accounts that are under continuous observation and in a controlled environment is excessive.	The standard has been updated to allow for procedural controls to track shared accounts.
007-R7		
007-R8	R8.1: This requirement should be extended to all cyber assets. There is always a risk that information contained on a non-CCA system could be used to compromise a CCA.	The requirements have been reworded to address this issue.
	R8.2: A clarification of the requirement is necessary. Some entities might interpret erasure as simple file deletion. Deleting files without repetitive overwrites using varying bit patterns does not prevent the recovery of the "erased" data.	The requirement says "to prevent retrieval of critical cyber security or reliability data". Erasures that do not prevent retrieval do not meet the requirement.
007-R9	A more thorough vulnerability assessment, to include penetration testing, should be performed on a periodic basis (perhaps once every three years). Simply verifying that ports and services are disabled does not significantly contribute to the overall security of the protected networks. Vulnerability assessment needs to verify that all protective controls are adequate and functional, including electronic access point controls such as router ACL's, firewall rules, and intrusion detection/prevention system configurations.	The Responsible Entity may go beyond the minimum requirements of this standard as it deems appropriate.
007-R10		
007-M1		
007-M2		
007-M3		
007-M4		
007-M5		
007-M6		
007-M7		
007-M8		
007-M9		
007-M10		
007-C1,1		

007-C1,2 007-C1,3	R6.3.3: An annual password change is unnecessarily risky. At a minimum, passwords should be changed quarterly, more frequently for highly privileged accounts.	Annual is a minimum and reflects industry consensus. The standard does not preclude a shorter period.
007-C1,4	Approval of exceptions should not be delegated.	Exceptions cannot be taken to NERC standards. It is up to Responsible Entities to define policies, exception handling, and delegation authority.
007-C2,1		
007-C2,2		
007-C2,3		
007-C2,4		

CIP-007 Drafting Team Responses to Comments

Name	Tom Pruitt	
Entity	Duke Power Company	
Ready to Ballot	No	
General Comments	A.4.1 -- Given the critical role of the PSE, why are these standards not applicable to that entity? A.4.2.2 -- Appears to be inconsistent with definition of "Cyber Asset". A.5 -- This should reference the proposed Implementation Plan. Alternatively, the compliance implementation plan should be referenced in the compliance sections for all of CIP002 thru CIP 009.	The standards reflect the Standard Authorization Request (SAR), which excluded PSEs. The drafting team must respect the scope of the SAR and not extend it during standards development. The SAR reflects industry consensus on the scope of the standard to be developed. The SAR also specifically excluded communication links. Although reviewed and voted upon by the industry, the Implementation Plan is not part of the standard and cannot be referenced therein.
007-R1		
007-R2	R2 -- This requirement will cause some systems to be in almost continual re-testing mode. Can the testing be done only once in development for a batch of significant changes that will be applied together in production?	Yes, if the single test accurately reflects the Responsible Entity's production environment.
007-R3		
007-R4		
007-R5		
007-R6	R6.1.2 -- This requirement will be difficult and costly to implement and manage.	The drafting team believes the proposed Implementation Schedule affords Responsible Entities the time needed to comply.
	R6.1.3 -- Is this requirement technically feasible (at any moment in time)? Is this requirement specifically measured against to cause noncompliance?	Reference to "any moment in time" has been removed.
	R6.3 -- Change this section to read: R6.3. In the absence of strong authentication methods (e.g. use of multi-factor access controls, digital certificates, or bio-metrics) the Responsible Entity shall require and utilize passwords. The passswords shall meet the following criteria where technically feasible:	Reference to strong authentication methods has been removed.
007-R7	R7 -- Change "as technically feasible" to "where technically feasible."	See modified verbiage.
007-R8		
007-R9		
007-R10		

CIP-007 Drafting Team Responses to Comments

007-M1

007-M2

007-M3

007-M4

007-M5

007-M6

007-M7

007-M8

007-M9

007-M10

007-C1,1

007-C1,2

007-C1,3

007-C1,4

007-C2,1

007-C2,2

007-C2,3

007-C2,4

CIP-007 Drafting Team Responses to Comments

Name	Duane Radzwion
Entity	Consumers Energy
Ready to Ballot	Yes
General Comments	
007-R1	
007-R2	
007-R3	
007-R4	
007-R5	
007-R6	
007-R7	
007-R8	
007-R9	
007-R10	
007-M1	
007-M2	
007-M3	
007-M4	
007-M5	
007-M6	
007-M7	
007-M8	
007-M9	
007-M10	

CIP-007 Drafting Team Responses to Comments

007-C1,1

007-C1,2

007-C1,3

007-C1,4

007-C2,1

007-C2,2

007-C2,3

007-C2,4

CIP-007 Drafting Team Responses to Comments

Name	Howard Rulf	
Entity	We Energies	
Ready to Ballot	No	
General Comments		
007-R1		
007-R2		
007-R3		
007-R4		
007-R5		
007-R6	For critical cyber assets that are connected to the corporate computing network using routable protocol utilizing domain account administration: R6.3.1: Change password length to 8 characters minimum. R6.3.3: Change passwords every 90 days or less.	The requirement is not technology specific. Because not all control systems support eight characters, it is the consensus of commenters that six characters is acceptable for minimum password length. This does not preclude the Responsible Entity from using eight. The requirement does not prevent the Responsible Entity from changing passwords more frequently.
007-R7		
007-R8		
007-R9		
007-R10		
007-M1		
007-M2		
007-M3		
007-M4		
007-M5		
007-M6		
007-M7		
007-M8		

CIP-007 Drafting Team Responses to Comments

007-M9

007-M10

007-C1,1

007-C1,2

007-C1,3

007-C1,4

007-C2,1

007-C2,2

007-C2,3

007-C2,4

CIP-007 Drafting Team Responses to Comments

Name	Randy Schimka	
Entity	San Diego Gas and Electric Co.	
Ready to Ballot	No	
General Comments		
007-R1	Why should a non-critical asset with the electronic security perimeter be subject to these requirements? We might have a PC installed within the perimeter for some office LAN-rellated purpose that isn't even connected to the secure EMS network, but under this requirement we'd have to put that PC through all of our documented test procedures for Microsoft patches, updates, etc.? We suggest that R1 be changed so that non-critical cyber assets are not included.	CIP-007 has been clarified to state that all requirements in CIP-007 apply to both Critical and non-critical Cyber Assets in the Electronic Security Perimeter. Protecting non-critical Cyber Assets residing within the same Electronic Security Perimeter as Critical Cyber Assets is essential because the non-critical Cyber Assets introduce vulnerabilities exposing the Critical Cyber Assets to threats that must be protected against.
007-R2		
007-R3	Same comment applies from R1 above.	See above.
007-R4	Same comment applies from R1 above.	See above,
007-R5		
007-R6		
007-R7		
007-R8		
007-R9		
007-R10		
007-M1		
007-M2		
007-M3		
007-M4		
007-M5		
007-M6		
007-M7		

CIP-007 Drafting Team Responses to Comments

007-M8

007-M9

007-M10

007-C1,1

007-C1,2

007-C1,3

007-C1,4

007-C2,1

007-C2,2

007-C2,3

007-C2,4

CIP-007 Drafting Team Responses to Comments

Name	Lyman Shaffer	
Entity	PG&E	
Ready to Ballot	Yes	
General Comments		
007-R1	"Noncritical assets..shall be subject to the requirements of this standard." We suggest that you add the phrase "except as noted" since R8 (disposal) applies only to critical cyber assets. Also clarify that these requirements also apply to "cyber assets used in access control"as reflected in CIP5, R.1.5	R8 has been renumbered to R7 and changed to Cyber Assets within the Electronic Security Perimeter. The applicable requirements for Cyber Assets used in the access control and monitoring of the Electronic Security Perimeter as referenced in CIP-005, 1.5 now include those in CIP-003 and CIP-007.
007-R2		
007-R3		
007-R4	R.4.1: we believe that assessmnrt of all security patches is excessively burdensome and suggest that this only apply to "assessment of critical security patches."	Criticality of patches may be addressed in the Responsibility Entity's security patch management program and implemented using reasonable business judgment. `
007-R5	R.5.1 We literally receive updated virus definition files every day. As written, we would have to assess and document them every day. We suggest a more practical requirement would be to require the documentation for anti-virus dat files are wtihin 30 days of release. That would end up hhighlighting those that have had a more significant potential impact rather than minor nuisance virus problems.	The requirement to assess anti-virus updates within 30 days has been removed. R5.2 has been renumbered to R4.2 and reworded. The Responsible Entity is now required to document and implement a process for updating signatures. The process must address testing and installation.
007-R6	R.6.1 We again take issue with the use of the phrase "technically feasible." just because soemthing is feasible doesn't mean we are going to do it particularly if the cost is substantially disproportionate to the risk.	Where technology allows, the entity must comply with the standard. Please refer to the FAQ.
007-R7		
007-R8		
007-R9		
007-R10		
007-M1		
007-M2		
007-M3		
007-M4		
007-M5		

CIP-007 Drafting Team Responses to Comments

007-M6

007-M7

007-M8

007-M9

007-M10

007-C1,1

007-C1,2

007-C1,3

007-C1,4

007-C2,1

007-C2,2

007-C2,3

007-C2,4

CIP-007 Drafting Team Responses to Comments

Name	Neil Shockey	
Entity	Southern California Edison	
Ready to Ballot	No	
General Comments		
007-R1	Change to read: Applicability - Both Critical Cyber Assets and non-Critical Cyber Assets within the Electronic Security Perimeter(s) shall be subject to the requirements of this standard. Note: the last sentence of R1 is duplicative (covered in R1.6 of CIP-005) and can be deleted.	The drafting team has removed the requirement to list non-critical Cyber Assets within the Electronic Security Perimeter because this requirement is in CIP-005 and clarified that all requirements in CIP-007 apply to both Critical and non-critical Cyber Assets in the Electronic Security Perimeter.
007-R2		
007-R3		
007-R4		
007-R5		
007-R6		
007-R7		
007-R8		
007-R9		
007-R10		
007-M1		
007-M2		
007-M3		
007-M4		
007-M5		
007-M6		
007-M7		
007-M8		

CIP-007 Drafting Team Responses to Comments

007-M9

007-M10

007-C1,1

007-C1,2

007-C1,3

007-C1,4

007-C2,1

007-C2,2

007-C2,3

007-C2,4

CIP-007 Drafting Team Responses to Comments

Name	William Smith	
Entity	Allegheny Power	
Ready to Ballot	No	
General Comments		
007-R1		
007-R2		
007-R3	This requirement is too burdensome and should be removed. The documentation of opened ports and services at the electronic access points is suficient.	The standard no longer requires the documentation of the configuration and status of all ports and services inside the Electronic Security Perimeter.
007-R4		
007-R5		
007-R6		
007-R7		
007-R8		
007-R9	R 9.2 -This requirement is too burdensome and should be removed. The documentation of opened ports and services at the electronic access points is suficient.	An annual assessment of Cyber Assets within the Electronic Security Perimeter is essential to protecting the Critical Cyber Assets.
007-R10		
007-M1		
007-M2		
007-M3		
007-M4		
007-M5		
007-M6		
007-M7		
007-M8		
007-M9		

CIP-007 Drafting Team Responses to Comments

007-M10

007-C1,1

007-C1,2

007-C1,3

007-C1,4

007-C2,1

007-C2,2

007-C2,3

007-C2,4

CIP-007 Drafting Team Responses to Comments

Name	Paul Sorenson	
Entity	Open Access Technology International	
Ready to Ballot	Yes	
General Comments	As commented under CIP-005, it is unclear if non-critical assets within the electronic security perimeter are subject to all CIP-002 through CIP-009 standards or just the CIP-005 and CIP-007 standards. This should be made clear. Data retention requirements cited under compliance should cite the 90 day retention of log files.	The language has been amended to specify CIP-007. The drafting team has reviewed and updated the standards for consistency of retention periods.
007-R1		
007-R2		
007-R3		
007-R4		
007-R5		
007-R6		
007-R7		
007-R8		
007-R9		
007-R10		
007-M1		
007-M2		
007-M3		
007-M4		
007-M5		
007-M6		
007-M7		
007-M8		
007-M9		

CIP-007 Drafting Team Responses to Comments

007-M10

007-C1,1

007-C1,2

007-C1,3

007-C1,4

007-C2,1

007-C2,2

007-C2,3

007-C2,4

Name	Robert Strauss	
Entity	NYSEG	
Ready to Ballot	No	
General Comments	Remove the first sentence of the purpose since it is redundant with the rest of the purpose. We prefer the second and third sentence of the purpose. For consistency, this Standard should include an Applicability 4.2.3, "Responsible Entities that, in compliance with CIP-002, identify that they have no Critical Cyber Assets."	Please see responses to Ray A'Brial, Central Hudson Gas & Electric Corp.
007-R1	The wording of R1 requires clarification given that some requirements in this standard refer specifically to Critical Cyber Assets rather than to the more generic "cyber assets". For instance, R8 requires data destruction or removal prior to disposal of a Critical Cyber Asset. On one hand, the wording of R1 could be taken to mean that one should replace the words "Critical Cyber Assets" by the words "Critical and Non-Critical Cyber Assets" when interpreting the standard. Under this interpretation, the Responsible Entity should wipe data on all assets prior to disposal. Alternatively, one could argue that the wording of R8 explicitly excludes non-critical cyber assets, and therefore failure to consider wipe data from non-critical cyber assets does not give rise to non-compliance. Please clarify. Change; Non-critical Cyber Assets as well as the Critical Cyber Assets defined in CIP-002 within the Electronic Security Perimeter(s) defined in CIP-005 shall be subject to the requirements of this standard. to; Cyber Assets associated with the Critical Cyber Assets defined in CIP-002 within the Electronic Security Perimeter(s) defined in CIP-005 shall be subject to the requirements of this standard.	
007-R2	Request clarification on R2. Does this Standard apply to Critical Cyber Assets or Cyber Assets? For clarification, change to "security patches, cumulative service packs, vendor releases, or version upgrades as applied to operating systems, applications, database platforms, or other third-party software or firmware."	
007-R3		
007-R4		
007-R5		
007-R6	R6.1.5 is not clear. This should be rewritten or removed	
007-R7		

CIP-007 Drafting Team Responses to Comments

007-R8	
007-R9	
007-R10	
007-M1	
007-M2	Measures M2.1, M2.2 and M2.3 should be rephrased as measures
007-M3	
007-M4	
007-M5	
007-M6	
007-M7	
007-M8	
007-M9	
007-M10	
007-C1,1	
007-C1,2	
007-C1,3	
007-C1,4	
007-C2,1	
007-C2,2	
007-C2,3	
007-C2,4	

CIP-007 Drafting Team Responses to Comments

Name	Karl Tammar	
Entity	IRC	
Ready to Ballot	No	
General Comments	11. It is unreasonable to require that documents referenced in this standard should be revised within 30 days of a change to the systems or controls. Even minor changes to network configurations or the addition of a single hardware element could require updating the large number of documents specified in this standard. The sheer volume of work involved is very likely to take considerably more than 30 days. Furthermore, since this standard applies to all cyber assets within the electronic security perimeter, the frequency of change could be high for organizations with large numbers of assets within the security perimeter. It is conceivable that the documentation required would be under constant revision (hence making it effectively impossible to establish a measurable date on which the revision is complete). A requirement to update the documents at least annually would be more sensible. 16. Compliance levels in this Standard are not consistent with those established in CIP-005 and CIP-006 for similar levels of logging system unavailability.	The standard has been updated to require changes to procedures be updated within 90 calendar days of a change resulting from a modification. Ninety days reflects industry consensus. The drafting team has reveiwed and modified the standard for consistency with other cyber security standards. Compliance levels have been rewritten.
007-R1	1. The wording of R1 requires clarification given that some requirements in this standard refer specifically to Critical Cyber Assets rather than to the more generic "cyber assets". For instance, R8 requires data destruction or removal prior to disposal of a Critical Cyber Asset. On one hand, the wording of R1 could be taken to mean that one should replace the words "Critical Cyber Assets" by the words "Critical and Non-Critical Cyber Assets" when interpreting the standard. Under this interpretation, the Responsible Entity should wipe data on all assets prior to disposal. Alternatively, one could argue that the wording of R8 explicitly excludes non-critical cyber assets, and therefore failure to consider wipe data from non-critical cyber assets does not give rise to non-compliance. Please clarify.	The drafting team has clarified that all requirements in CIP-007 apply to both Critical and non-critical Cyber Assets in the Electronic Security Perimeter.
007-R2	2. R2 requires that testing be done but it is unclear what that testing is to accomplish.	CIP-007 R2 addresses testing to verify that changes do not adversely affect security controls required in CIP-007.
007-R3		
007-R4		
007-R5	3. R5 requires that virus signatures must be explicitly assessed for applicability, installed under change management and configuration management control, and that all of this must be documented. This is overly prescriptive as it does not contemplate Responsible Entities employing auto-update services commonly offered by service providers.	The requirement to assess anti-virus updates within 30 days has been removed. R5.2 has been renumbered to R4.2 and reworded. The Responsible Entity is now required to document and implement a process for updating signatures. The process must address testing and installation.
007-R6	4. R6.1.1 should be reworded to state, "Wherever technically practical..." 5. There is a verb missing in R6.1.5. 6. R6.1.5 is redundant given the requirements of CIP-003 R5 and CIP-004 R4. R6.1.5 should be	R6 has been renumbered to R5 and its subrequirements clarified. For example, reference to "any given moment" has been removed, the correlation with CIP-004 has been added, and the reference to strong authentication methods removed. R5 is subject to technical feasibility.

	deleted. 7. There appears to be overlap between R6.2.2 and R6.1.1. To avoid confusion, the wording of R6.1 should be modified to include coverage of factory default accounts, and R6.2.2 deleted. 8. The requirement for an audit trail of account use in R6.2.4 overlaps the audit requirement in R6.2.5. These requirements should be combined in R6.2.4, and R6.2.5 deleted to avoid confusion.	
007-R7		
007-R8	The wording of R1 requires clarification given that some requirements in this standard refer specifically to Critical Cyber Assets rather than to the more generic "cyber assets". For instance, R8 requires data destruction or removal prior to disposal of a Critical Cyber Asset. On one hand, the wording of R1 could be taken to mean that one should replace the words "Critical Cyber Assets" by the words "Critical and Non-Critical Cyber Assets" when interpreting the standard. Under this interpretation, the Responsible Entity should wipe data on all assets prior to disposal. Alternatively, one could argue that the wording of R8 explicitly excludes non-critical cyber assets, and therefore failure to consider wipe data from non-critical cyber assets does not give rise to non-compliance. Please clarify.	The requirements in CIP-007 apply to both Critical and non-critical Cyber Assets in the Electronic Security Perimeter. R8 states that the reason for erasure is to prevent unauthorized access to sensitive cyber security or reliabiity data. If non-critical Cyber Assets within the perimeter contain this type of infomration, the data storage media must be destroyed or erased per the requirement.
007-R9	10. R9 should read as Critical Cyber Assets throughout	The drafting team intends the requirements to apply to all Cyber Assets within the Electronic Security Perimeter and has updated the standard to clarify this issue.
007-R10	11. It is unreasonable to require that documents referenced in this standard should be revised within 30 days of a change to the systems or controls. Even minor changes to network configurations or the addition of a single hardware element could require updating the large number of documents specified in this standard. The sheer volume of work involved is very likely to take considerably more than 30 days. Furthermore, since this standard applies to all cyber assets within the electronic security perimeter, the frequency of change could be high for organizations with large numbers of assets within the security perimeter. It is conceivable that the documentation required would be under constant revision (hence making it effectively impossible to establish a measurable date on which the revision is complete). A requirement to update the documents at least annually would be more sensible. 9. In R6.3.2 -- the special character requirement should be removed. This is not enforceable on many systems including AD. (AD allows enforcement of only 3 of 4 items). 4. R6.1.1 should be reworded to state, "Wherever technically practical, ….. 5. There is a verb missing in R6.1.5.	The requirement has been renumbered to R9 and has been modified.
007-M1	6. R6.1.5 is redundant given the requirements of CIP-003 R5 and CIP-004 R4. R6.1.5 should be	
007-M2	12. Measure M2.1, as written, specifies a requirement. Requirements should be specified only in the Requirements section of the document. 13. Measure M2.3 establishes a requirement new to this standard -- to formally accept test results	The measures have been rewritten to refer back to the requirements.

	indicative of successful completion of changes to Critical Cyber Assets. This new requirement should not be established in the Measures section. Consider moving this measure to CIP-003 and associating it with R6.2	
007-M3		
007-M4		
007-M5		
007-M6		
007-M7		
007-M8		
007-M9		
007-M10		
007-C1,1		
007-C1,2		
007-C1,3		
007-C1,4		
007-C2,1	15. Compliance statement 2.1.4 effectively establishes a new requirement for annual review of access privileges and authorization rights. If this is a requirement, it should be established in the Requirements section. Furthermore, this compliance statement should be reviewed for consistency against compliance statements 2.1.1 and 2.2.1 of CIP-004 14. It is unclear in the Compliance section what is meant by the terms "system security controls" or "documented system security controls"since these terms are never defined in the standard. If the intent is to refer to M1 through M10, this should be clearly stated.	The levels of noncompliance have been rewritten to reflect changes to requirements and measures as well as severity of infraction. The requirement and measure have been updated for consistency with time reviews throughout CIP-002 through CIP-009.
007-C2,2	15. Compliance statement 2.1.4 effectively establishes a new requirement for annual review of access privileges and authorization rights. If this is a requirement, it should be established in the Requirements section. Furthermore, this compliance statement should be reviewed for consistency against compliance statements 2.1.1 and 2.2.1 of CIP-004 deleted.	See above.
007-C2,3	7. There appears to be overlap between R6.2.2 and R6.1.1. To avoid confusion, the wording of R6.1 should be modified to include coverage of factory default accounts, and R6.2.2 deleted.	

007-C2,4

8. The requirement for an audit trail of account use in R6.2.4 overlaps the audit requirement in R6.2.5. These requirements should be combined in R6.2.4, and R6.2.5 deleted to avoid confusion.

9. In R6.3.2 -- the special character requirement should be removed. This is not enforceable on many systems including AD. (AD allows enforcement of only 3 of 4 items).

CIP-007 Drafting Team Responses to Comments

Name	Todd Thompson	
Entity	PJM Interconnection	
Ready to Ballot	No	
General Comments	It is unreasonable to require that documents referenced in this standard should be revised within 30 days of a change to the systems or controls. Even minor changes to network configurations or the addition of a single hardware element could require updating the large number of documents specified in this standard. The sheer volume of work involved is very likely to take considerably more than 30 days. Furthermore, since this standard applies to all cyber assets within the electronic security perimeter, the frequency of change could be high for organizations with large numbers of assets within the security perimeter. It is conceivable that the documentation required would be under constant revision (hence making it effectively impossible to establish a measurable date on which the revision is complete). A requirement to update the documents at least annually would be more sensible. Compliance levels in this Standard are not consistent with those established in CIP-005 and CIP-006 for similar levels of logging system unavailability.	Please see responses to Karl Tammar, IRC.
007-R1	The wording of R1 requires clarification given that some requirements in this standard refer specifically to Critical Cyber Assets rather than to the more generic "cyber assets". For instance, R8 requires data destruction or removal prior to disposal of a Critical Cyber Asset. On one hand, the wording of R1 could be taken to mean that one should replace the words "Critical Cyber Assets" by the words "Critical and Non-Critical Cyber Assets" when interpreting the standard. Under this interpretation, the Responsible Entity should wipe data on all assets prior to disposal. Alternatively, one could argue that the wording of R8 explicitly excludes non-critical cyber assets, and therefore failure to consider wipe data from non-critical cyber assets does not give rise to non-compliance. Please clarify.	
007-R2	R2 requires that testing be done but it is unclear what that testing is to accomplish.	
007-R3		
007-R4		
007-R5	R5 requires that virus signatures must be explicitly assessed for applicability, installed under change management and configuration management control, and that all of this must be documented. This is overly prescriptive as it does not contemplate Responsible Entities employing auto-update services commonly offered by service providers.	
007-R6	R6.1.1 should be reworded to state, "Wherever technically practical, …" There is a verb missing in R6.1.5. R6.1.5 is redundant given the requirements of CIP-003 R5 and CIP-004 R4. R6.1.5 should be deleted.	

	There appears to be overlap between R6.2.2 and R6.1.1. To avoid confusion, the wording of R6.1 should be modified to include coverage of factory default accounts, and R6.2.2 deleted. The requirement for an audit trail of account use in R6.2.4 overlaps the audit requirement in R6.2.5. These requirements should be combined in R6.2.4, and R6.2.5 deleted to avoid confusion. In R6.3.2 -- the special character requirement should be removed. This is not enforceable on many
007-R7	
007-R8	
007-R9	R9 should read as Critical Cyber Assets throughout.
007-R10	
007-M1	
007-M2	Measure M2.1, as written, specifies a requirement. Requirements should be specified only in the Requirements section of the document. Measure M2.3 establishes a requirement new to this standard -- to formally accept test results indicative of successful completion of changes to Critical Cyber Assets. This new requirement should not be established in the Measures section. Consider moving this measure to CIP-003 and associating it with R6.2
007-M3	
007-M4	
007-M5	
007-M6	
007-M7	
007-M8	
007-M9	
007-M10	
007-C1,1	
007-C1,2	
007-C1,3	

007-C1,4 systems including AD. (AD allows enforcement of only 3 of 4 items).

007-C2,1 It is unclear in the Compliance section what is meant by the terms "system security controls" or "documented system security controls"since these terms are never defined in the standard. If the intent is to refer to M1 through M10, this should be clearly stated.

Compliance statement 2.1.4 effectively establishes a new requirement for annual review of access privileges and authorization rights. If this is a requirement, it should be established in the Requirements section. Furthermore, this compliance statement should be reviewed for consistency against compliance statements 2.1.1 and 2.2.1 of CIP-004.

007-C2,2

007-C2,3

007-C2,4

Name	Steven Townsend	
Entity	Consumers Energy Co.	
Ready to Ballot	No	
General Comments	Consumers Energy has also submitted comments via the ECAR CIPP.	Please see responses to Larry Conrad, ECAR CIPP.
007-R1		
007-R2		
007-R3		
007-R4		
007-R5		
007-R6		
007-R7		
007-R8		
007-R9		
007-R10		
007-M1		
007-M2		
007-M3		
007-M4		
007-M5		
007-M6		
007-M7		
007-M8		
007-M9		
007-M10		

CIP-007 Drafting Team Responses to Comments

007-C1,1

007-C1,2

007-C1,3

007-C1,4

007-C2,1

007-C2,2

007-C2,3

007-C2,4

CIP-007 Drafting Team Responses to Comments

Name	Martin Trence	
Entity	Xcel Energy - Northen States Power (NSP)	
Ready to Ballot	No	
General Comments		
007-R1		
007-R2		
007-R3		
007-R4		
007-R5		
007-R6	R6.1.5 - Delete the word "periodic" from the requirement, as the relationship is established in CIP-003 and CIP-004. Comments concerning periodic were addressed in CIP-004, and should be referenced only in one standard.	This requirement has been clairified.
	R6.3.2Change the word "and" to "or", as it is common industry practice to use a combination of alpha and numeric characters (Upper and Lower Case), where the inclusion of special characters is not.	The requirements are subject to technical feasibility to address cases such as you point out.
007-R7		
007-R8		
007-R9		
007-R10		
007-M1		
007-M2		
007-M3		
007-M4		
007-M5		
007-M6		
007-M7		

CIP-007 Drafting Team Responses to Comments

007-M8

007-M9

007-M10

007-C1,1

007-C1,2

007-C1,3

007-C1,4

007-C2,1

007-C2,2

007-C2,3

007-C2,4

CIP-007 Drafting Team Responses to Comments

Name	Rick Vermeers
Entity	Avistacorp
Ready to Ballot	Yes
General Comments	
007-R1	
007-R2	
007-R3	
007-R4	
007-R5	
007-R6	
007-R7	
007-R8	
007-R9	
007-R10	
007-M1	
007-M2	
007-M3	
007-M4	
007-M5	
007-M6	
007-M7	
007-M8	
007-M9	
007-M10	

CIP-007 Drafting Team Responses to Comments

007-C1,1

007-C1,2

007-C1,3

007-C1,4

007-C2,1

007-C2,2

007-C2,3

007-C2,4

Name Robert C. Webb

Entity Instrumentation, Systems and Automation Society

Ready to Ballot No

General Comments

1. Who is ISA and Why is ISA commenting on CIP-002 through CIP-009?

These comments were developed by members of the Instrumentation, Systems and Automation Society, (ISA), SP99, "Manufacturing and Control Systems Security" committee's leadership team. The overall committee is composed of over 200 members including many users, government representatives, academics, control systems manufactures, and engineers with expertise in automation and control systems. ISA's SP99 is working to develop control systems security standards that provide sufficient guidance to the control systems and IT domain stakeholders to assure that security risks can be appropriately reduced without adversely affecting the intended functionality of those systems. ISA has published over 150 pages of guidance specific to the application of cyber security to control systems, in the form of two technical reports: ISA's ANSI/ISA-TR99.00.01-2004, "Security Technologies for Manufacturing and Control Systems", and ANSI/ISA-TR99.00.02-2004, "Integrating Electronic Security into the Manufacturing and Control Systems Environment." Both highlight the unique aspects of control systems which must be considered when applying security procedures and technology to control systems. ISA's constituency includes both fossil and nuclear power plant automation practitioners, and ISA has active standards committees in both of these areas (SP77, Fossil Power Plant Standards, and SP67, Nuclear Power Plant Standards).

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 have been working with NERC to establish a liaison process that would allow such considerations to be addressed earlier in the process. The development of that liaison process is nearly complete. However, comments are due at this time, and we believe these issues need to be addressed now, before approval of these standards, for the standards to be effective, without damaging the systems they are intended to protect. Thus members of the SP99 committee leadership team, with domain expertise in power generation and associated control systems have put together summary comments in several areas that should be addressed before issue of these standards.

2. Overview and Summary of Essential Changes

In general, we found these documents to be excellent examples of how an industry group can (and should) provide coherent and well structured guidance on cybersecurity. We commend NERC's drafting team and review process; it has resulted in a quality set of documents that should be widely used.

At the same time, and in fact because of the expected wide application of these documents, we believe that three general areas should be addressed before approval of these documents.

a) Broader scope - to address a larger % of generation resources and key distribution resources,

Regarding comment #2a, the exclusionary language concerning generation assets has been removed with the exception of nuclear generation which is excluded by the SAR. Because distribution assets are not considered part of the Bulk Electric System, these resources remain excluded as well.

Regarding comment #2b, much of the prescriptive language on how certain security measures should be applied has been removed. For example, the requirement for port scans in CIP 005, R4.2 has been replaced by a requirement to review only ports and services required for operations are enabled. In addition, the Drafting Team has removed most references to "how" security measures should be applied throughout the Standards unless it is required for compliance purposes.

Regarding comment #2c, language has been added to reflect the fact that some security solutions that are available today were not available when some legacy systems were designed and put into service. CIP-003, CIP-004, CIP-005, and CIP-006 contain language addressing exceptions to their policies that may be required to deal with legacy systems and facilities where modern security solutions are not technically possible. In these cases, the Responsible Entities must identify and document the exception and describe the mitigating steps they are taking to secure the assets in lieu of the modern solution.

Regarding the comments #3, #4, and #5 related to scope, the Standard reflects the Standard Authorization Request which excluded distribution, nuclear generation, and telecommunication infrastructure. The Drafting Team cannot exceed the scope of the SAR.

A SAR reflects the industry consensus on the scope of any particular standard to be developed. Once SAR has been approved for standards drafting, the scope cannot be changed.

The NERC Reliability Standards process would require new SARs to address these scope issues.

and avoid excessive reliance on one boundary or layer of defense from cyber attacks. While we recognize the need to prioritize and prevent excessive requirements, we believe the current scope is overly restrictive, and excludes a significant portion of generation, and thereby significant vulnerabilities, in some areas. This is addressed in our specific comments on CIP-002-1, (and also CIP-003-1 through 009-1), which follow.
b) Additional cautions and guidance for control systems - in the form of specific requirements and references to key industry documents, to assure that the measures applied do not result in systems failures and reduced reliability instead of reduced risk. These cautions and guidance are necessary to address the special considerations needed when applying many normal security practices to control systems and control system networks -- particularly the bulk of legacy systems in operation today. Many do not have any ability to provide most of the required security features, and can be adversely affected by the application of other requirements. One good example is the requirement to do port scans (CIP 005-1, R4.2). Many legacy control networks are halted by port scans. The standard should include this caution, and suggest the use of alternatives to identify open ports on operational systems which have not been specifically designed and demonstrated to support this kind of testing without production failures. In general, more specific guidance on how to apply these requirements to the many legacy systems in use today should be provided.
c) Mandatory additional protection for inadequate legacy systems -- The phrase "where technically feasible" is used in a number of locations throughout the document. In many of these cases, alternatives are required. However, in others, no alternatives are required. Clearly stated requirements to add protection or barriers to cyber attack ("mitigation measures"), where they cannot be configured or incorporated into existing systems, should be added. It is not acceptable, in our view, to identify unacceptable risks, and then leave them because the existing equipment cannot be appropriately hardened. Appropriate countermeasures, to reduce risks to acceptable levels, should be required in all cases.

Addressing these concerns does not mean significant revision to this set of standards, or significant delay, in our opinion. It can be done effectively with minor changes and references in the generic text and in several specific locations. We suggest some of the specifics below. We believe these considerations are important to prevent the standards from being counterproductive or missing significant vulnerabilities.

3. Scope - Distribution assets that could have cyber impacts on transmission assets are excluded. All distribution assets that could have cyber impacts on Bulk Electric system assets should be included, to meet the objectives of the Standards. This comment also applies to the identical sections of the remaining standards (CIP-003 -- CIP-009).

4. Scope - Exclusion 3.2.1 should be removed; it excludes some of the larger generators that would otherwise be included under R1.1.4, and the NRC's requirements should be coordinated with, not independent of these requirements. This comment also applies to the identical sections of the remaining standards, (Section 4.2.1 of CIP-003 -- CIP-009).

5. Scope - Exclusion 3.2.2 should be removed; even when those communications systems are provided by others, the defined entities are still ultimately responsible for their proper operation and security. This comment also applies to the identical sections of the remaining standards, (Section 4.2.2 of CIP-003 -- CIP-009).

CIP-007 Drafting Team Responses to Comments

007-R1		
007-R2	Additional cautions and guidance for control systems -- R2. Significant changes must also include control or monitoring system configuration changes that could impact cyber access.	If the Cyber Assets used to control and monitor are within the Electronic Security Perimeter, they are subject to the requirements of 007. The Responsible Entity may go beyond the minimum requirements of this standard if it deems it appropriate to do so.
007-R3	Additional cautions and guidance for control systems -- See comments on CIP-005 R2, (repeated here for ease of reference): "Ports and services used in control system applications are not always known. Control system suppliers may not be able to provide this information as they do not know what ports and services will be utilized by the utility. Consequently, this requirement may not be feasible for many legacy SCADA systems as well as power plant and substation control systems. This requirement should have explicit cautions to test any change on fully representative non-production systems before application, and/or to provide alternative mitigation measures external to the control network per se. A "where possible" caveat is not adequate; it does not adequately highlight the dangers to operational systems, in what would seem to be a very simple activity."	The point of this requirement is not to document each and every port; rather, the objective is awareness as to what port and services are awake and listening for connection requests. Those ports that are not used must be disabled. If the Responsible Entity cannot ensure only those ports and services required for normal and emergency operations are enabled due to legacy issues, then the Responsible Entity must write and approve an exception as required in CIP-003.
007-R4	Minor comment - The 30 calendar day limit needs to be defined - is it when the vendor is notified or the Responsible Entity is notified?	The intent of "of availability" was to define the assessment of the patches relative to the vendor's notification of availability. However, this term is subject to the Responsible Entity's reasonable business judgment.
007-R5	Additional cautions and guidance for control systems -- R5.2 There needs to be a requirement that testing be performed on non production control systems with CPUs loaded at representative levels, to assure that Anti-Virus definition updates do not cause a loss of system control during the update process. Prior experience has identified that control systems, depending on the vintage and loading of the microprocessor, can lose control during Anti-Virus definition updates. Integrity monitoring tools may not be applicable to substation or power plant control systems without appropriate testing.	The type of testing you suggest should be considered when the Responsible Entity develops its process for updating anti-virus and malware prevention tools. Testing and installation of signatures must be part of the process.
007-R6		
007-R7	Additional cautions and guidance for control systems -- R7.3 This requirement should state that the end-user should determine if logging capability exists. If so, logs must be maintained. If logging capability does not exist, alternate means must be devised.	"where technically feasible " has been added.
007-R8		
007-R9	Additional cautions and guidance for control systems -- R9.2. This should read- A review and verification that Cyber Assets have no unsecured cyber connections. "Ports and services" imply protocols, knowledge, scanning, or penetration test that may not be appropriate or provide the necessary information, and can also lead to control system shutdown.	The standard does not require scanning or a penetration test. See the FAQ.
007-R10		
007-M1	Additional cautions and guidance for control systems -- Measures need to be adjusted where appropriate in response to the above considerations under requirements.	Please see responses above.
007-M2		

CIP-007 Drafting Team Responses to Comments

007-M3		
007-M4		
007-M5		
007-M6		
007-M7		
007-M8		
007-M9		
007-M10		
007-C1,1	Additional cautions and guidance for control systems -- Compliance needs to be adjusted where appropriate in response to the above considerations under requirements.	Please see responses above.
007-C1,2		
007-C1,3		
007-C1,4		
007-C2,1		
007-C2,2		
007-C2,3		
007-C2,4		

CIP-007 Drafting Team Responses to Comments

Name	Laurent Webber	
Entity	Western Area Power Administration	
Ready to Ballot	No	
General Comments	These requirements are too proscriptive and not wrapped in a risk-based management program. As such they lead to cascading requirements that are too costly for the associated risk. The entire section should be replaced by a requirement to follow a risk management lifecycle process for mitigating risk to an acceptable level.	The cyber security standards embody the concept of risk management. The standards development process itself relies on industry consensus to identify minimum levels of acceptable risk. The intent of the standards is to provide a minimum level of consistency across the industry. As long as the requirements of these standards are met, the Responsible Entity is free to use its own risk assessment process to manage risk.
007-R1	Non-critical cyber assets should not be included in a blanket statement. Responsible entities must be allowed to evaluate the threats, vulnerabilities, and risks associated with non-critical cyber assets and apply appropriate mitigation.	CIP-007 has been clarified to state that all requirements in CIP-007 apply to both Critical and non-critical Cyber Assets in the Electronic Security Perimeter. Protecting non-critical cyber assets residing within the same Electronic Security Perimeter as Critical Cyber Assets is essential because the non-critical cyber assets introduce vulnerabilities exposing the Critical Cyber Assets to threats that must be protected against. See response to General Comments, above.
007-R2	The testing requirements under CIP-003, R6 are adequate, so R2, R2.1, R2.2, and R2.3 should be deleted.	The testing requirement has been removed from 003 and consolidated in CIP-007. CIP-007 R2 addresses testing to verify that changes do not adversely affect security controls required in CIP-007.
007-R3	R3: What do you mean by the term "status" as different from "configuration"? If these are not entirely separate concepts, remove the word "status". R3: R9.2 calls for the same restriction to only necessary ports and services, so R3 can be removed. Also, CIP-005, R2 requires that all unnecessary ports and services be disabled, so again R3 here is redundant and can be removed.	The standard no longer requires the documentation of the configuration and status of all ports and services inside the Electronic Security Perimeter. CIP-005 refers to devices on the Electronic Security Perimeter and CIP-007 refers to devices within the Electronic Security Perimeter.
007-R4	R4.1: States that upgrades must be assessed with 30 days. This should only apply to security related upgrades. Change wording to "security upgrades."	The requirement has been modified as suggested.
007-R5		
007-R6	The requirements for account management are adequately addressed in CIP-003, R5 and specific details should be left to the Responsible Entities' individual security plans and policies, so all of R6, including its sub-sections, can be deleted.	CIP-007 addresses the requirements for implementing the access rights defined in CIP-003. The requirement has been updated to reference CIP-003.

	R6.3.3: The wholesale modification of passwords to substation IEDs is a formidable task with detrimental effect on reliability if there is any small error. A reasonable plan considering security and reliability is to modify substation IED passwords on a 3 year schedule except where a breach of security has occurred or a specific threat has been made that requires passwords to be changed.	The annual time frame is supported by a consensus of commenters.
007-R7	R7.5: When using automated tools, as is encouraged in R7, it is unnecessary to review all logs. This requirement should be limited to the review of alarms and events related to cyber security incidents.	This is the intent of the requirement; see modified verbiage.
007-R8		
007-R9	The requirement for cyber vulnerability assessments inside every Electronic Security Perimeter is too much. It should only apply to the control centers and perimeter scans be deemed adequate for substations and other remote Electronic Security Perimeters.	An annual assessment of Cyber Assets within the Electronic Security Perimeter is essential to protecting the Critical Cyber Assets. Note that the standard does not require scanning or a penetration test. Please see the FAQ.
007-R10	Annual review of documents is adequate. Remove the 30-day update requirement.	The requirement has been clarified to state that documentation must be updated within 90 days if changes to system or controls are made. 90 days reflects industry consensus.
007-M1	A list of non-critical Cyber Assets is not necessary and will be too costly to maintain. Remove this measure.	
007-M2	Test procedures covered in CM requirements under CIP-003. Remove this measure.	See response at the Requirement. Measures have been reworded.
007-M3	Remove the word "status."	See response at the Requirement. Measures have been reworded.
007-M4		
007-M5		
007-M6	This is covered in CIP-003. Remove this measure.	See response at the Requirement. Measures have been reworded.
007-M7		
007-M8		
007-M9		
007-M10	Remove "30 calendar days" and only refer to annual review and update.	See response at the Requirement. Measures have been reworded.
007-C1,1		
007-C1,2		
007-C1,3		
007-C1,4	A 3 year schedule is more realistic with work load and employee turnover. The requirement should be, "Each entity shall have a policy, plan, and procedure to change passwords periodically, with provisions for emergency password changes when risk factors warrant.	
007-C2,1	Compliance 2.1.3: Remove "30 calendar days" and only refer to annual review and update.	The levels of noncompliance have been rewritten to reflect changes to requirements and measures.

007-C2,2	Compliance 2.2.3: Remove "60 calendar days" and only refer to annual review and update. Compliance 2.2.4: Remove "30 calendar days" and only refer to annual review and update.	The levels of noncompliance have been rewritten to reflect changes to requirements and measures.
007-C2,3	Compliance 2.3.3: Remove "90 calendar days" and only refer to annual review and update. Compliance 2.3.4: Remove "30 calendar days" and only refer to annual review and update.	The levels of noncompliance have been rewritten to reflect changes to requirements and measures.
007-C2,4	Compliance 2.4.3: Remove "120 calendar days" and only refer to annual review and update. Compliance 2.4.4: Remove "30 calendar days" and only refer to annual review and update.	The levels of noncompliance have been rewritten to reflect changes to requirements and measures.

CIP-007 Drafting Team Responses to Comments

Name	Michal Zeithammel
Entity	Brascan Power
Ready to Ballot	Yes
General Comments	
007-R1	
007-R2	
007-R3	
007-R4	
007-R5	
007-R6	
007-R7	
007-R8	
007-R9	
007-R10	
007-M1	
007-M2	
007-M3	
007-M4	
007-M5	
007-M6	
007-M7	
007-M8	
007-M9	
007-M10	

CIP-007 Drafting Team Responses to Comments

007-C1,1

007-C1,2

007-C1,3

007-C1,4

007-C2,1

007-C2,2

007-C2,3

007-C2,4

Name	Guy Zito	
Entity	NPCC	
Ready to Ballot	No	
General Comments	Remove the first sentence of the purpose since it is redundant with the rest of the purpose. We prefer the second and third sentence of the purpose. For consistency, this Standard should include an Applicability 4.2.3, "Responsible Entities that, in compliance with CIP-002, identify that they have no Critical Cyber Assets."	Please see responses to Ray A'Brial, Central Hudson Gas & Electric Corp.
007-R1	The wording of R1 requires clarification given that some requirements in this standard refer specifically to Critical Cyber Assets rather than to the more generic "cyber assets". For instance, R8 requires data destruction or removal prior to disposal of a Critical Cyber Asset. On one hand, the wording of R1 could be taken to mean that one should replace the words "Critical Cyber Assets" by the words "Critical and Non-Critical Cyber Assets" when interpreting the standard. Under this interpretation, the Responsible Entity should wipe data on all assets prior to disposal. Alternatively, one could argue that the wording of R8 explicitly excludes non-critical cyber assets, and therefore failure to consider wipe data from non-critical cyber assets does not give rise to non-compliance. Please clarify. Change; Non-critical Cyber Assets as well as the Critical Cyber Assets defined in CIP-002 within the Electronic Security Perimeter(s) defined in CIP-005 shall be subject to the requirements of this standard. to; Cyber Assets associated with the Critical Cyber Assets defined in CIP-002 within the Electronic Security Perimeter(s) defined in CIP-005 shall be subject to the requirements of this standard.	
007-R2	Request clarification on R2. Does this Standard apply to Critical Cyber Assets or Cyber Assets? For clarification, change to "security patches, cumulative service packs, vendor releases, or version upgrades as applied to operating systems, applications, database platforms, or other third-party software or firmware."	
007-R3		
007-R4		
007-R5		
007-R6	R6.1.5 is not clear. This should be rewritten or removed	
007-R7		

007-R8	
007-R9	
007-R10	
007-M1	
007-M2	Measures M2.1, M2.2 and M2.3 should be rephrased as measures
007-M3	
007-M4	
007-M5	
007-M6	
007-M7	
007-M8	
007-M9	
007-M10	
007-C1,1	
007-C1,2	
007-C1,3	
007-C1,4	
007-C2,1	
007-C2,2	
007-C2,3	
007-C2,4	

CIP-008 Drafting Team Responses to Comments

Name	Raymond A'Brial	
Entity	Central Hudson Gas & Electric Corp	
Ready to Ballot:	No	
General Comment	This Standard references the IAW SOP in R1.1 and R1.3. Prior to Version 0, NERC Operating Policies and Planning Standards sometimes "hid" requirements in other documents. Version 0 moved all requirements and measures into the new Standards. We do not want to recreate the earlier mess. Also, a CIPC group is re-writing the IAW SOP. That re-write is outside the Standards process. It is inappropriate to change a Standard without using the Standards process. We recommend removing those IAW SOP references.	Reference to IAW SOP has been removed.
008-R1	Change R1.1 to "The Responsible Entity shall define procedures to characterize and classify events as Cyber Security Incidents." Change R1.3 to "The Responsibility Entity must ensure that the Cyber Security Incident is reported to the ES-ISAC either directly or through an intermediary."	Both suggested changes have need made.
008-R2	Remove R2.1 and R2.2 since not all relevant incidents will give rise to all of the types of documentation listed. For instance, physical security incidents will generally not give rise to system or application log file entries and cyber incidents will not give rise to video and/or physical access records. Also remove "at a minimum" since the phrase is superfluous.	The requirement has been changed to refer to relevant documentation per Requirement R1.1.
008-M1		
008-M2		
008-C1,1		
008-C1,2		
008-C1,3		
008-C1,4		
008-C2,1		
008-C2,2	Change 2.2.3 to "A reportable Cyber Security Incident has occurred but was not reported to the ES-ISAC; or"	Done.
008-C2,3	Change 2.3.2 to "Two or more reportable Cyber Security Incidents have occurred but were not reported to ES-ISAC"	Done.
008-C2,4		

CIP-008 Drafting Team Responses to Comments

Name	Ori Artman
Entity	Teltone
Ready to Ballot:	Yes
General Comment	
008-R1	
008-R2	
008-M1	
008-M2	
008-C1,1	
008-C1,2	
008-C1,3	
008-C1,4	
008-C2,1	
008-C2,2	
008-C2,3	
008-C2,4	

CIP-008 Drafting Team Responses to Comments

Name	Steve Badgett
Entity	Riverside Public Utilitities
Ready to Ballot:	Yes
General Comment	
008-R1	
008-R2	
008-M1	
008-M2	
008-C1,1	
008-C1,2	
008-C1,3	
008-C1,4	
008-C2,1	
008-C2,2	
008-C2,3	
008-C2,4	

CIP-008 Drafting Team Responses to Comments

Name	Terry Baker
Entity	Platte River Power Authority
Ready to Ballot:	Yes
General Comment	
008-R1	
008-R2	
008-M1	
008-M2	
008-C1,1	
008-C1,2	
008-C1,3	
008-C1,4	
008-C2,1	
008-C2,2	
008-C2,3	
008-C2,4	

CIP-008 Drafting Team Responses to Comments

Name	Terry Bilke
Entity	Midwest ISO
Ready to Ballot:	No
General Comment	
008-R1	
008-R2	
008-M1	
008-M2	
008-C1,1	
008-C1,2	
008-C1,3	
008-C1,4	
008-C2,1	
008-C2,2	
008-C2,3	
008-C2,4	

CIP-008 Drafting Team Responses to Comments

Name	Pat Bourassa
Entity	Wisconsin Public Service Corporation
Ready to Ballot:	Yes
General Comment	
008-R1	
008-R2	
008-M1	
008-M2	
008-C1,1	
008-C1,2	
008-C1,3	
008-C1,4	
008-C2,1	
008-C2,2	
008-C2,3	
008-C2,4	

CIP-008 Drafting Team Responses to Comments

Name	Laurence W. Brown	
Entity	Edison Electric Institute	
Ready to Ballot:	No	
General Comment		
008-R1		
008-R2		
008-M1		
008-M2		
008-C1,1		
008-C1,2		
008-C1,3		
008-C1,4		
008-C2,1	Additional number 2.1.1 unnecessary.	Done.
008-C2,2		
008-C2,3		
008-C2,4	Additional number 2.4.1 unnecessary.	

CIP-008 Drafting Team Responses to Comments

Name	Peter Burke	
Entity	American Transmission Company	
Ready to Ballot:	No	
General Comment	American Transmission Company concurs with the comments submitted separately by the Edison Electric Institute and by the Midwest Reliability Organization.	Please see responses to Laurence W. Brown, Edison Electric Institute.
008-R1		
008-R2		
008-M1		
008-M2		
008-C1,1		
008-C1,2		
008-C1,3		
008-C1,4		
008-C2,1	American Transmission Company concurs with the comments submitted separately by the Edison Electric Institute.	
008-C2,2		
008-C2,3		
008-C2,4	American Transmission Company concurs with the comments submitted separately by the Edison Electric Institute.	

CIP-008 Drafting Team Responses to Comments

Name	Marc Butts	
Entity	Southern Company	
Ready to Ballot:	Yes	
General Comment		
008-R1	R1 - How does the required reporting to ES ISAC in this standard relate to the DOE EIA-417 reporting that is also required of electric utilities with an actual or suspected cyber attack? The FAQ at a minimum should acknowledge this duplicate reporting, if required.	The drafting team will address this issues in an FAQ.
008-R2		
008-M1		
008-M2		
008-C1,1		
008-C1,2		
008-C1,3		
008-C1,4		
008-C2,1		
008-C2,2		
008-C2,3		
008-C2,4		

CIP-008 Drafting Team Responses to Comments

Name	Gary Campbell	
Entity	MAIN	
Ready to Ballot:	No	
General Comment	address items below. This standrd as written provides no conssitency of reporting because each entities plan could be different. It sounds like we are requiring a plan to follow a procedure. I think the requirement should be to follow the identified procedure for inccident reporting or deveolop a NERC reporting procedure and follow it. I worry that no consistency would come out of this standard which is essential to reporting. This standard creates a process on top of an already defined procedure.	The majority of comments received regarding this standard do not support the making the IAW SOP mandatory. Therefore, the DT does not support the creation of any mandatory incident reporting procedures. Responsible Entities may elect to follow the criteria and thresholds defined in the Incident, Analysis, and Warning (IAW) program, for example, or create their own.
008-R1		
008-R2		
008-M1		
008-M2		
008-C1,1		
008-C1,2		
008-C1,3		
008-C1,4		
008-C2,1		
008-C2,2		
008-C2,3		
008-C2,4		

CIP-008 Drafting Team Responses to Comments

Name	Linda Campbell	
Entity	FRCC	
Ready to Ballot:	No	
General Comment		
008-R1		
008-R2	R2.1 System and application logs are not mentioned prior to this standard. Do you mean user account activity logs and system event logs mentioned in CIP-007. If not, should those logs related to cyber security incidents be added to CIP-007 R7.3? R2.5 The scope of R2 is reportable incidents. So what does it mean to keep "all cyber security incidents" records? R2.1 -- 2.5 describe the documents to be kept and R2.5 includes subsequent reports? So what else are we keeping with this requirement?? Do you mean the standardized format for reporting all three stages of incident data? Please be more specific in the wording.	The requirement has been changed to refer to relevant documentation per Requirement R1.1
008-M1		
008-M2		
008-C1,1	In the applicability section 4.1.10 and 4.1.11, RRO's and NERC are included. Who has the monitoring responsibility for a RRO or NERC? Add Self-Certification and Audit information to this section. Proposed language would be: 1.1. Complaince Monitoring Responsibility Regional Reliability Organization. 1.1.1. The Compliance Monitor will request a self-certification annually. 1.1.2. The Compliance Monitor will perform an audit at least once every three (3)calendar years.	NERC will audit RROs and an independent auditor will audit NERC. Self-certification language has been added.
008-C1,2	D2.2.4 Clarify that by changing to "Records related to reportable cyber security incidents"	Clarified.
008-C1,3	To complement a audit every three years, the data retention period should be 3 years.	The data retention has been modified to read "The Responsible Entity shall keep all required documentation relating to reportable Cyber Security Incidents for three calendar years." All other documentation, in response to industry comment, is required to be kept for the previous full calendar year.
008-C1,4		
008-C2,1		

CIP-008 Drafting Team Responses to Comments

008-C2,2

008-C2,3

008-C2,4

CIP-008 Drafting Team Responses to Comments

Name	Roger Champagne	
Entity		
Ready to Ballot:	No	
General Comment	This Standard references the IAW SOP in R1.1 and R1.3. Prior to Version 0, NERC Operating Policies and Planning Standards sometimes had requirements in other documents. Version 0 moved all requirements and measures into the new Standards. Also, a CIPC group is re-writing the IAW SOP. That re-write is not being done as part of the NERC Reliability Standards "ANSI approved" process. It is inappropriate to change a Standard without using the Reliability Standards process. We recommend removing those IAW SOP references.	Please see responses to Ray A'Brial, Central Hudson Gas & Electric Corp.
008-R1	Change R1.1 to "The Responsible Entity shall define procedures to characterize and classify events as Cyber Security Incidents." Change R1.3 to "The Responsibility Entity must ensure that the Cyber Security Incident is reported to the ES-ISAC either directly or through an intermediary."	
008-R2	Remove R2.1 and R2.2 since not all relevant incidents will give rise to all of the types of documentation listed. For instance, physical security incidents will generally not give rise to system or application log file entries and cyber incidents will not give rise to video and/or physical access records. Also remove "at a minimum" since the phrase is superfluous.	
008-M1		
008-M2		
008-C1,1		
008-C1,2		
008-C1,3		
008-C1,4		
008-C2,1		
008-C2,2	Change 2.2.3 to "A reportable Cyber Security Incident has occurred but was not reported to the ES-ISAC; or"	
008-C2,3	Change 2.3.2 to "Two or more reportable Cyber Security Incidents have occurred but were not reported to ES-ISAC"	
008-C2,4		

CIP-008 Drafting Team Responses to Comments

Name	Larry Conrad
Entity	ECAR Critical Infrastructure Protection Panel
Ready to Ballot:	Yes
General Comment	
008-R1	
008-R2	
008-M1	
008-M2	
008-C1,1	
008-C1,2	
008-C1,3	
008-C1,4	
008-C2,1	
008-C2,2	
008-C2,3	
008-C2,4	

CIP-008 Drafting Team Responses to Comments

Name	Larry Conrad	
Entity	Cinergy	
Ready to Ballot:	No	
General Comment	Need additional information or definition of what constitutes a "reportable" incident.	The Responsible Entity must define its own criteria for “reportable’ cyber security incident. Please refer to FAQ for examples of how "reportable" incidents may be characterized.
008-R1		
008-R2		
008-M1		
008-M2		
008-C1,1		
008-C1,2		
008-C1,3		
008-C1,4		
008-C2,1		
008-C2,2		
008-C2,3		
008-C2,4		

CIP-008 Drafting Team Responses to Comments

Name	Theodore Creedon, P.E.
Entity	Creedon Engineering
Ready to Ballot:	Yes
General Comment	
008-R1	
008-R2	
008-M1	
008-M2	
008-C1,1	
008-C1,2	
008-C1,3	
008-C1,4	
008-C2,1	
008-C2,2	
008-C2,3	
008-C2,4	

CIP-008 Drafting Team Responses to Comments

Name	Joel De Granda
Entity	Florida Power and Light
Ready to Ballot:	Yes
General Comment	
008-R1	
008-R2	
008-M1	
008-M2	
008-C1,1	
008-C1,2	
008-C1,3	
008-C1,4	
008-C2,1	
008-C2,2	
008-C2,3	
008-C2,4	

CIP-008 Drafting Team Responses to Comments

Name	Richard Engelbrecht	
Entity	RGE	
Ready to Ballot:	No	
General Comment	This Standard references the IAW SOP in R1.1 and R1.3. Prior to Version 0, NERC Operating Policies and Planning Standards sometimes had requirements in other documents. Version 0 moved all requirements and measures into the new Standards. Also, a CIPC group is re-writing the IAW SOP. That re-write is not being done as part of the NERC Reliability Standards "ANSI approved" process. It is inappropriate to change a Standard without using the Reliability Standards process. We recommend removing those IAW SOP references.	Please see responses to Ray A'Brial, Central Hudson Gas & Electric Corp
008-R1	Change R1.1 to "The Responsible Entity shall define procedures to characterize and classify events as Cyber Security Incidents." Change R1.3 to "The Responsibility Entity must ensure that the Cyber Security Incident is reported to the ES-ISAC either directly or through an intermediary."	
008-R2	Remove R2.1 and R2.2 since not all relevant incidents will give rise to all of the types of documentation listed. For instance, physical security incidents will generally not give rise to system or application log file entries and cyber incidents will not give rise to video and/or physical access records. Also remove "at a minimum" since the phrase is superfluous.	
008-M1		
008-M2		
008-C1,1		
008-C1,2		
008-C1,3		
008-C1,4		
008-C2,1		
008-C2,2	Change 2.2.3 to "A reportable Cyber Security Incident has occurred but was not reported to the ES-ISAC; or"	
008-C2,3	Change 2.3.2 to "Two or more reportable Cyber Security Incidents have occurred but were not reported to ES-ISAC"	
008-C2,4		

CIP-008 Drafting Team Responses to Comments

Name	Ken Fell	
Entity	New York ISO	
Ready to Ballot:	No	
General Comment	This Standard references the IAW SOP in R1.1 and R1.3. Prior to Version 0, NERC Operating Policies and Planning Standards sometimes had requirements in other documents. Version 0 moved all requirements and measures into the new Standards. Also, a CIPC group is re-writing the IAW SOP. That re-write is not being done as part of the NERC Reliability Standards "ANSI approved" process. It is inappropriate to change a Standard without using the Reliability Standards process. We recommend removing those IAW SOP references.	Please see responses to Ray A'Brial, Central Hudson Gas & Electric Corp.
008-R1	Change R1.1 to "The Responsible Entity shall define procedures to characterize and classify events as Cyber Security Incidents." Change R1.3 to "The Responsibility Entity must ensure that the Cyber Security Incident is reported to the ES-ISAC either directly or through an intermediary."	
008-R2	Remove R2.1 and R2.2 since not all relevant incidents will give rise to all of the types of documentation listed. For instance, physical security incidents will generally not give rise to system or application log file entries and cyber incidents will not give rise to video and/or physical access records. Also remove "at a minimum" since the phrase is superfluous.	
008-M1		
008-M2		
008-C1,1		
008-C1,2		
008-C1,3		
008-C1,4		
008-C2,1		
008-C2,2	Change 2.2.3 to "A reportable Cyber Security Incident has occurred but was not reported to the ES-ISAC; or"	
008-C2,3	Change 2.3.2 to "Two or more reportable Cyber Security Incidents have occurred but were not reported to ES-ISAC"	
008-C2,4		

CIP-008 Drafting Team Responses to Comments

Name	Francis Flynn	
Entity	National Grid USA	
Ready to Ballot:	No	
General Comment	This Standard references the IAW SOP in R1.1 and R1.3. Prior to Version 0, NERC Operating Policies and Planning Standards sometimes had requirements in other documents. Version 0 moved all requirements and measures into the new Standards. Also, a CIPC group is re-writing the IAW SOP. That re-write is not being done as part of the NERC Reliability Standards "ANSI approved" process. It is inappropriate to change a Standard without using the Reliability Standards process. National Grid recommends removing those IAW SOP references.	Please see responses to Ray A'Brial, Central Hudson Gas & Electric Corp.
008-R1	Change R1.1 to "The Responsible Entity shall define procedures to characterize and classify events as Cyber Security Incidents." Change R1.3 to "The Responsibility Entity must ensure that the Cyber Security Incident is reported to the ES-ISAC either directly or through an intermediary."	
008-R2	Remove R2.1 and R2.2 since not all relevant incidents will give rise to all of the types of documentation listed. For instance, physical security incidents will generally not give rise to system or application log file entries and cyber incidents will not give rise to video and/or physical access records. Also remove "at a minimum" since the phrase is superfluous.	
008-M1		
008-M2		
008-C1,1		
008-C1,2		
008-C1,3		
008-C1,4		
008-C2,1		
008-C2,2	Change 2.2.3 to "A reportable Cyber Security Incident has occurred but was not reported to the ES-ISAC; or"	
008-C2,3	Change 2.3.2 to "Two or more reportable Cyber Security Incidents have occurred but were not reported to ES-ISAC"	
008-C2,4		

CIP-008 Drafting Team Responses to Comments

Name	Greg Fraser
Entity	Manitoba Hydro
Ready to Ballot:	Yes
General Comment	
008-R1	
008-R2	
008-M1	
008-M2	
008-C1,1	
008-C1,2	
008-C1,3	
008-C1,4	
008-C2,1	
008-C2,2	
008-C2,3	
008-C2,4	

CIP-008 Drafting Team Responses to Comments

Name	Jerry Freese	
Entity	American Electric Power	
Ready to Ballot:	No	
General Comment	Based on the expanded scope set forth in CIP-002 R1 for the Critical Assets and the subsequently expanded scope of the Critical Cyber Assets and the Electronic Security Perimeter, it would be impractical and infeasible to meet the obligations set forth in this requirement.	CIP-002 has been changed.
008-R1		
008-R2		
008-M1		
008-M2		
008-C1,1		
008-C1,2		
008-C1,3		
008-C1,4		
008-C2,1		
008-C2,2		
008-C2,3		
008-C2,4		

CIP-008 Drafting Team Responses to Comments

Name	Edwin C. Goff III	
Entity	Progress Energy	
Ready to Ballot:	No	
General Comment		
008-R1		
008-R2	R2.1 & R2.2 - The requirement to keep documentation for 3 calendar years is excessive, given lifecycle of Operating Systems, software applications, patches etc., referring back to details of 3 year old exploit does not seem to have value over keeping for 1 full year. Would like to see data retention for these items be at 1 year.	This information has important forensic value. For example, it may be necessary to support civil or criminal investigations, which can last longer than one year.
008-M1		
008-M2		
008-C1,1		
008-C1,2		
008-C1,3		
008-C1,4		
008-C2,1		
008-C2,2		
008-C2,3		
008-C2,4		

Name	Kenneth Goldsmith	
Entity	Alliant Energy	
Ready to Ballot:	No	
General Comment		
008-R1	R1.1 requires Responsible Entities to define procedures to classify events as Cyber Security Incidents in accordance with cyber event criteria defined in NERC's Indications, Analysis & Warning Program (IAW) Standard Operating Procedure. This creates a circular reference conflict with the defintion of Cyber Security Incidents, as provided in the definitions section. A standard definition is provided, but the requirement indicates an entity should craft its own definition - both of these things can't be true. To resolve this conflict, the definition of a Cyber Security Incident should be modified to coordinate with R1.1 - the definition should clarify that an incident is defined by each entity in accordance with guidance from NERC's IAW.	Refences to the IAW Program have been removed.
008-R2		
008-M1		
008-M2		
008-C1,1		
008-C1,2		
008-C1,3		
008-C1,4		
008-C2,1		
008-C2,2		
008-C2,3		
008-C2,4		

CIP-008 Drafting Team Responses to Comments

Name	Kathleen Goodman	
Entity	ISO New England Inc	
Ready to Ballot:	No	
General Comment	The IAW SOP is a criteria and procedure document that is undergoing re-development. It is also a document that is not vetted and voted on by the industry. Therefore it is not appropriate to make it a "defacto standard" by referecne. Any references to it should be removed.	Please see responses to Ray A'Brial, Central Hudson Gas & Electric
008-R1	Change R1.1 to "The Responsible Entity shall define procedures to characterize and classify events as Cyber Security Incidents." Change R1.3 to "The Responsibility Entity must ensure that the Cyber Security Incident is reported to the ES-ISAC either directly or through an intermediary." R1.3 Question: Are there appropriate and in-appropriate "intermediaries"?	The standard has been revised as suggested. The word "appropriate" has been removed.l
008-R2	R2 Remove "at a minimum" since not all items are relevant to all incidents. Remove R2.1 and R2.2 since not all relevant incidents will give rise to all of the types of documentation listed. For instance, physical security incidents will generally not give rise to system or application log file entries and cyber incidents will not give rise to video and/or physical access records.	
008-M1		
008-M2		
008-C1,1		
008-C1,2		
008-C1,3	It is not clear when you mean documents, records, or data. These are three distinct items and should not be referenced interchangeably. Please clarify.	The standards have been revised to ensure that these terms are used correctly and consistently. The section title "Data Retention" is part of the Standard NERC template and can not be changed. An FAQ has been added to address this topic.]
008-C1,4		
008-C2,1		
008-C2,2	2.2.3 Remove "...in accordance with the IAW SOP...".	
008-C2,3	2.3.2 Remove "...in accordance with the IAW SOP...".	
008-C2,4		

CIP-008 Drafting Team Responses to Comments

Name	Tim Hattaway
Entity	Alabama Electric Cooperative
Ready to Ballot:	Yes
General Comment	
008-R1	
008-R2	
008-M1	
008-M2	
008-C1,1	
008-C1,2	
008-C1,3	
008-C1,4	
008-C2,1	
008-C2,2	
008-C2,3	
008-C2,4	

CIP-008 Drafting Team Responses to Comments

Name	Jerry Heeren
Entity	MEAG Power
Ready to Ballot:	Yes
General Comment	
008-R1	
008-R2	
008-M1	
008-M2	
008-C1,1	
008-C1,2	
008-C1,3	
008-C1,4	
008-C2,1	
008-C2,2	
008-C2,3	
008-C2,4	

CIP-008 Drafting Team Responses to Comments

Name	Peter Henderson	
Entity	Independent Electricity System Operator (IESO)	
Ready to Ballot:	No	
General Comment		
008-R1		
008-R2	1. The final sentence of Requirement R2 should be reworded as, "this documentation must include, where relevant, the following:" This change is needed since not all relevant incidents will give rise to all of the types of documentation listed. For instance, physical security incidents will generally not give rise to system or application log file entries and cyber incidents will not give rise to video and/or physical access records. 2. R2 Retention period should be 2 years. The utility of a 3 year retention period is unclear.	1. The sub-requirements for R2 have been removed and the word relevant added. 2. This information has important forensic value. For example, it may be necessary to support civil or criminal investigations, which can last a year or longer. Three years was deemed reasonable.
008-M1		
008-M2		
008-C1,1		
008-C1,2		
008-C1,3		
008-C1,4		
008-C2,1		
008-C2,2		
008-C2,3		
008-C2,4		

CIP-008 Drafting Team Responses to Comments

Name	E. Nick Henery	
Entity	SMUD	
Ready to Ballot:	Yes	
General Comment	The Drafting Team will need to go through the Standard and assign responsibility to each function from the functional model like the Version 0 STD. For this Standard to enforceable the generic use of Responsible Entity is the same as the generic use of Control Area. Even if the Standard lists the different functions it leaves open the possibility of misinterpretation as to which function is truly responsible.	The Responsible Entities are clearly enumerated in the standard Section A, item 4.
008-R1		
008-R2		
008-M1		
008-M2		
008-C1,1		
008-C1,2		
008-C1,3		
008-C1,4		
008-C2,1		
008-C2,2		
008-C2,3		
008-C2,4		

CIP-008 Drafting Team Responses to Comments

Name	Jack Hobbick
Entity	Consumers Energy
Ready to Ballot:	Yes
General Comment	
008-R1	
008-R2	
008-M1	
008-M2	
008-C1,1	
008-C1,2	
008-C1,3	
008-C1,4	
008-C2,1	
008-C2,2	
008-C2,3	
008-C2,4	

CIP-008 Drafting Team Responses to Comments

Name	Richard Kafka	
Entity	Pepco Holdings, Inc.	
Ready to Ballot:	Yes	
General Comment		
008-R1		
008-R2		
008-M1		
008-M2		
008-C1,1		
008-C1,2		
008-C1,3		
008-C1,4		
008-C2,1	Is 2.1.1 necessary?	Levels of non-compliance align with Requirements and Measures.
008-C2,2		
008-C2,3		
008-C2,4	Is 2.4.1 necessary?	Levels of non-compliance align with Requirements and Measures.

CIP-008 Drafting Team Responses to Comments

Name	Tony Kroskey	
Entity	Brazos Electric Power Cooperative	
Ready to Ballot:	No	
General Comment	Subsection 4.2, remove the word "entities".	Changed.
008-R1		
008-R2	Suggest changing the text "Cyber Security Incidents reportable per R1.1" to "reportable Cyber Security Incidents".	Done,.
008-M1		
008-M2		
008-C1,1		
008-C1,2		
008-C1,3		
008-C1,4		
008-C2,1		
008-C2,2		
008-C2,3		
008-C2,4		

CIP-008 Drafting Team Responses to Comments

Name	Carol Krysevig	
Entity	Allegheny Energy Supply Co. LLC	
Ready to Ballot:	No	
General Comment	D2.2.1. -- Add '(if necessary)' after 'but has not been updated'.	2.2.1 has been changed to"reviewed within the last calendar year."
008-R1		
008-R2		
008-M1		
008-M2		
008-C1,1		
008-C1,2		
008-C1,3		
008-C1,4		
008-C2,1		
008-C2,2		
008-C2,3		
008-C2,4		

CIP-008 Drafting Team Responses to Comments

Name	John Lim	
Entity	Con Edison	
Ready to Ballot:	No	
General Comment	This Standard references the IAW SOP in R1.1 and R1.3. Prior to Version 0, NERC Operating Policies and Planning Standards sometimes had requirements in other documents. Version 0 moved all requirements and measures into the new Standards. Also, a CIPC group is re-writing the IAW SOP. That re-write is not being done as part of the NERC Reliability Standards "ANSI approved" process. It is inappropriate to change a Standard without using the Reliability Standards process. We recommend removing those IAW SOP references.	Please see responses to Ray A'Brial, Central Hudson Gas & Electric.
008-R1	Change R1.1 to "The Responsible Entity shall define procedures to characterize and classify events as Cyber Security Incidents." Change R1.3 to "The Responsibility Entity must ensure that the Cyber Security Incident is reported to the ES-ISAC either directly or through an intermediary."	
008-R2	Remove R2.1 and R2.2 since not all relevant incidents will give rise to all of the types of documentation listed. For instance, physical security incidents will generally not give rise to system or application log file entries and cyber incidents will not give rise to video and/or physical access records. Also remove "at a minimum" since the phrase is superfluous.	
008-M1		
008-M2		
008-C1,1		
008-C1,2		
008-C1,3		
008-C1,4		
008-C2,1		
008-C2,2	Change 2.2.3 to "A reportable Cyber Security Incident has occurred but was not reported to the ES-ISAC; or"	
008-C2,3	Change 2.3.2 to "Two or more reportable Cyber Security Incidents have occurred but were not reported to ES-ISAC"	
008-C2,4		

CIP-008 Drafting Team Responses to Comments

Name	Deborah Linke	
Entity	Bureau of Reclamation	
Ready to Ballot:	No	
General Comment	Generally, we believe that annual updates and reviews of documentation are adequate absent a major system change. Based on this we recommended deleting references to other time frames.	The standard requires an annual review of the incident response plan and updates as necessary. It is important that the plan be updated within 90 days of any changes, so that personnel are adequately prepared to respond to incidents.
008-R1	R1.5: The level of required testing is not well-defined.	Additional defintion has been added. It now states that a test of the incident response plan can range from a paper drill, to a full operational exercise, to an actual incident.
008-R2		
008-M1		
008-M2		
008-C1,1		
008-C1,2		
008-C1,3		
008-C1,4		
008-C2,1		
008-C2,2		
008-C2,3		
008-C2,4		

CIP-008 Drafting Team Responses to Comments

Name	Greg Mason
Entity	Dynegy Generation
Ready to Ballot:	Yes
General Comment	
008-R1	
008-R2	
008-M1	
008-M2	
008-C1,1	
008-C1,2	
008-C1,3	
008-C1,4	
008-C2,1	
008-C2,2	
008-C2,3	
008-C2,4	

CIP-008 Drafting Team Responses to Comments

Name	Paul McClay	
Entity	Tampa Electric	
Ready to Ballot:	No	
General Comment		
008-R1		
008-R2	Clarify by changing to "documentation related to reportable cyber security incidents......"	Revised.
	Move the retention to compliance section D1.3 instead of here.	Duplicate references to data reterntion have been removed.
	R2.1 System and application logs are not mentioned prior to this standard. Do you mean user account activity logs and system event logs mentioned in CIP-007. If not, should those logs related to cyber security incidents be added to CIP-007 R7.3?	R2.1 - R2.5 have been removed.
	R2.5 The scope of R2 is "reportable incidents". This requirement says documentation includes: "records of all cyber security incidents and subsequent reports submitted to the ESISAC". R2.1 -- 2.5 describe specific documents to be kept, so what else are we keeping with this requirement? Do you mean the standardized report sent to ESISAC? Please be more specific in the wording.	
008-M1		
008-M2		
008-C1,1		
008-C1,2		
008-C1,3		
008-C1,4		
008-C2,1		
008-C2,2	D2.2.4 Change to "Records related to reportable cyber security incidents…."	Done.
008-C2,3		
008-C2,4		

CIP-008 Drafting Team Responses to Comments

Name	David McCoy
Entity	Great Plains Energy/Kansas City Power & Light
Ready to Ballot:	Yes
General Comment	
008-R1	
008-R2	
008-M1	
008-M2	
008-C1,1	
008-C1,2	
008-C1,3	
008-C1,4	
008-C2,1	
008-C2,2	
008-C2,3	
008-C2,4	

CIP-008 Drafting Team Responses to Comments

Name	Don Miller
Entity	First Energy Corp
Ready to Ballot:	Yes
General Comment	
008-R1	
008-R2	
008-M1	
008-M2	
008-C1,1	
008-C1,2	
008-C1,3	
008-C1,4	
008-C2,1	
008-C2,2	
008-C2,3	
008-C2,4	

CIP-008 Drafting Team Responses to Comments

Name	Patrick Miller
Entity	PacifiCorp
Ready to Ballot:	Yes
General Comment	
008-R1	
008-R2	
008-M1	
008-M2	
008-C1,1	
008-C1,2	
008-C1,3	
008-C1,4	
008-C2,1	
008-C2,2	
008-C2,3	
008-C2,4	

CIP-008 Drafting Team Responses to Comments

Name	Jeff Mitchell
Entity	ECAR
Ready to Ballot:	Yes
General Comment	N/A
008-R1	
008-R2	
008-M1	
008-M2	
008-C1,1	
008-C1,2	
008-C1,3	
008-C1,4	
008-C2,1	
008-C2,2	
008-C2,3	
008-C2,4	

CIP-008 Drafting Team Responses to Comments

Name	Scott Mix
Entity	KEMA, Inc
Ready to Ballot:	Yes
General Comment	
008-R1	
008-R2	
008-M1	
008-M2	
008-C1,1	
008-C1,2	
008-C1,3	
008-C1,4	
008-C2,1	
008-C2,2	
008-C2,3	
008-C2,4	

Name	Darrick Moe	
Entity	WAPA	
Ready to Ballot:	No	
General Comment	We do not feel that these standards should be balloted individually; rather, they need to be balloted as a group.	The drafting team supports this position.
008-R1		
008-R2		
008-M1		
008-M2		
008-C1,1		
008-C1,2		
008-C1,3		
008-C1,4		
008-C2,1		
008-C2,2		
008-C2,3		
008-C2,4		

CIP-008 Drafting Team Responses to Comments

Name	Selby Mohr
Entity	Sacramento Municipal Utility District
Ready to Ballot:	Yes
General Comment	
008-R1	
008-R2	
008-M1	
008-M2	
008-C1,1	
008-C1,2	
008-C1,3	
008-C1,4	
008-C2,1	
008-C2,2	
008-C2,3	
008-C2,4	

CIP-008 Drafting Team Responses to Comments

Name	Kurt Muehlbauer	
Entity	Exelon	
Ready to Ballot:	No	
General Comment	The documentation and processes around the responsible entity s tasks are too prescriptive. The industry needs to be extremely careful to avoid the creation of purely documentation-based non-compliances. With increasing legal requirements for compliance, and the associated penalties for noncompliance, noncompliance should be reserved for real security issues. It is simply too easy to make a mistake in documentation in light of the constantly evolving cyber environment. Each entity should develop its own processes in support of the requirements, and these processes should be required to contain provisions for periodic review and approval applicable to each requirement. The processes should also be required to produce reasonable documentation to demonstrate compliance. However, it is not necessary to specify the details of the documentation or review periods. The above approach can be met by removing references to documentation from the requirements section. Then, in the measures section require each entity to reasonably document programs and processes that support the security requirements and to produce reasonable documentation required to demonstrate compliance to the security requirements. Please refer to our overall comments on defining reasonable. If the above approach is taken, it will be possible to delete many of the sub-bullet points under each requirement (because the details will be specified by each entity in their program or process, as applicable). This will also ensure that documentation and excessive low-value administrative tasks are removed from the requirements.	The Drafting team has reviewed the standards and removed prescription where possible. The prescription that remains is necessary to provide the clarity requested by a majority of commenters. The documentation required by these standards allow Responsible Entities to demonstrate that the policies, processes, and procedures that they have implemented consistently comply with the requirements of these standards.
008-R1		
008-R2	2.1 -- 2.5 Delete these sub requirements. They are overly prescriptive. Each entity should develop their incident response plan and maintain needed documentation to demonstrate compliance.	The sub-requirements have been deleted.
008-M1	Refer to general, overall comments submitted on CIP-002 through CIP-009 regarding revision of the measures and compliance specification.	
008-M2	Refer to general, overall comments submitted on CIP-002 through CIP-009 regarding revision of the measures and compliance specification.	
008-C1,1	Refer to general, overall comments submitted on CIP-002 through CIP-009 regarding revision of the measures and compliance specification.	
008-C1,2	Refer to general, overall comments submitted on CIP-002 through CIP-009 regarding revision of the measures and compliance specification.	
008-C1,3	Refer to general, overall comments submitted on CIP-002 through CIP-009 regarding revision of the measures and compliance specification.	

CIP-008 Drafting Team Responses to Comments

008-C1,4 Refer to general, overall comments submitted on CIP-002 through CIP-009 regarding revision of the measures and compliance specification.

008-C2,1 Refer to general, overall comments submitted on CIP-002 through CIP-009 regarding revision of the measures and compliance specification.

008-C2,2 Refer to general, overall comments submitted on CIP-002 through CIP-009 regarding revision of the measures and compliance specification.

008-C2,3 Refer to general, overall comments submitted on CIP-002 through CIP-009 regarding revision of the measures and compliance specification.

008-C2,4 Refer to general, overall comments submitted on CIP-002 through CIP-009 regarding revision of the measures and compliance specification.

Name	Jeffrey Mueller	
Entity	PSEG Companies	
Ready to Ballot:	No	
General Comment	The PSEG Companies have reviewed and share the concerns expressed in the Comments of PJM and EEI. Accordingly, the PSEG Companies support the comments of PJM and EEI, and request that the concerns expressed in those comments be properly addressed in the next version of the draft standard.	Please see responses to Laurence W. Brown, EEI.
008-R1		
008-R2		
008-M1		
008-M2		
008-C1,1		
008-C1,2		
008-C1,3		
008-C1,4		
008-C2,1		
008-C2,2		
008-C2,3		
008-C2,4		

CIP-008 Drafting Team Responses to Comments

Name	Mitchell Needham
Entity	Tennessee Valley Authority
Ready to Ballot:	Yes
General Comment	
008-R1	
008-R2	
008-M1	
008-M2	
008-C1,1	
008-C1,2	
008-C1,3	
008-C1,4	
008-C2,1	
008-C2,2	
008-C2,3	
008-C2,4	

CIP-008 Drafting Team Responses to Comments

Name	Dave Norton	
Entity	Entergy Transmission	
Ready to Ballot:	No	
General Comment		
008-R1	R1.3: Suggestion: Hyperlinks to "IAW SOP" and "ES ISAC" might be helpful...	References to IAW SOP have been removed.
008-R2	R2 and M2: M2 reads "All documentation per R2." But all required documentation listed in R2.1 -- R2.5 may not be relevant to each and every incident. Suggestion: Convert the R2.1 -- R2.5 requirements list to a list of bullets, and change "must include, at a minimum" to "may include some or all of." Otherwise, as it is, compliance with M2 is binary, and if one of the listed requirements has no bearing on the case, the Responsible Entity could be non-compliant by default but had done nothing incorrectly. Or, substantially modify the Measures and Levels of Non-Compliance sections.	Sub-requirements 2.1 -- 2.5 have been removed.
008-M1		
008-M2	R2 and M2: M2 reads "All documentation per R2." But all required documentation listed in R2.1 -- R2.5 may not be relevant to each and every incident. Suggestion: Convert the R2.1 -- R2.5 requirements list to a list of bullets, and change "must include, at a minimum" to "may include some or all of." Otherwise, as it is, compliance with M2 is binary, and if one of the listed requirements has no bearing on the case, the Responsible Entity could be non-compliant by default but had done nothing incorrectly. Or, substantially modify the Measures and Levels of Non-Compliance sections.	Sub-requirements 2.1 -- 2.5 have been removed.
008-C1,1		
008-C1,2		
008-C1,3		
008-C1,4		
008-C2,1		
008-C2,2		
008-C2,3		
008-C2,4		

CIP-008 Drafting Team Responses to Comments

Name	Doug Orlofske
Entity	Wisconsin Public Power Inc
Ready to Ballot:	Yes
General Comment	
008-R1	
008-R2	
008-M1	
008-M2	
008-C1,1	
008-C1,2	
008-C1,3	
008-C1,4	
008-C2,1	
008-C2,2	
008-C2,3	
008-C2,4	

CIP-008 Drafting Team Responses to Comments

Name	Kevin Perry	
Entity	Southwest Power Pool	
Ready to Ballot:	Yes	
General Comment	Ready for ballot, subject to minor clarifications as noted in the following comments.	
008-R1		
008-R2		
008-M1		
008-M2		
008-C1,1		
008-C1,2		
008-C1,3		
008-C1,4	Approval of exceptions should not be delegated.	Exceptions cannot be taken to NERC standards. It is up to Responsible Entities to define policies, exception handling, and delegation authority.
008-C2,1	C2.1.1: This is not necessarily measurable. Only in case of a personnel change stemming from the resignation or other departure of an employee would a document modification within 90 days of the "change" be auditable.	Changes can be precipitated by personnel change. They also result from drills, exercises, lessons learned, actual incident response and changes to critical cyber assets. These can be tracked and are measurable.
008-C2,2		
008-C2,3		
008-C2,4		

CIP-008 Drafting Team Responses to Comments

Name	Tom Pruitt	
Entity	Duke Power Company	
Ready to Ballot:	No	
General Comment	Clarify that this standard applies only to Cyber A.3 -- Security Incidents related to the Critical Cyber Assets. A.4.1 -- Given the critical role of the PSE, why are these standards not applicable to that entity? A.4.2.2 -- Appears to be inconsistent with definition of "Cyber Asset". A.5 -- This should reference the proposed Implementation Plan. Alternatively, the compliance implementation plan should be referenced in the compliance sections for all of CIP 002 thru CIP 009.	"associated with Critical Cyber Assets" added. The standards reflect the Standard Authorization Request (SAR), which excluded PSEs. The drafting team must respect the scope of the SAR and not extend it during standards development. The SAR reflects industry consensus on the scope of the standard to be developed. The SAR also specifically excluded communication links. Although reviewed and voted upon by the industry, the Implementation is not part of the standard and cannot be referenced therein.
008-R1	R1 -- Clarify that this response plan must be approved by a level of management. R1.1 -- Clarify that this standard applies only to Cyber Security Incidents related to the Critical Cyber Assets. By reference, this requirement effectively gives the IAW SOP the full force and weight of a standard, without due process. As such, any future changes to the IAW SOP effectively become standards. At a minimum, this should reference the current version of the IAW SOP. Any potential changes to the IAW SOP or to the IAW SOP referenced here should be treated as a standard revision and be subject to the standards development process. R1.2 -- By reference, this requirement effectively gives the IAW SOP the full force and weight of a standard, without due process. As such, any future changes to the IAW SOP effectively become standards. At a minimum, this should reference the current version of the IAW SOP. Any potential changes to the IAW SOP or to the IAW SOP referenced here should be treated as a standard revision and be subject to the standards development process.	This was not the intent of the drafting team, but a Responsible Entity is not prevented from requiring such approval in its own policies. References to the IAW have been removed.
008-R2	R2.5 -- Clarify who has the responsibility for data retention when reports are submitted thru an intermediary.	The Responsible Entity is ultimately responsible for compliance to these standards. Data retention applies to the Responsible Entity.
008-M1		
008-M2		
008-C1,1		
008-C1,2		

008-C1,3		
008-C1,4	1.4.1 -- There is no requirement for the Cyber Response plan be approved by senior management. Therefore, the senior management referenced here has not been identified. Suggest adding senior management approval of plan to R1.	A Responsible Entity is not prevented from requiring senior management approval. As long as compliance is achieved, each Entity has the flexibility to manage its organization as it sees fit.
008-C2,1		
008-C2,2		
008-C2,3		
008-C2,4		

CIP-008 Drafting Team Responses to Comments

Name	Duane Radzwion
Entity	Consumers Energy
Ready to Ballot:	Yes
General Comment	
008-R1	
008-R2	
008-M1	
008-M2	
008-C1,1	
008-C1,2	
008-C1,3	
008-C1,4	
008-C2,1	
008-C2,2	
008-C2,3	
008-C2,4	

CIP-008 Drafting Team Responses to Comments

Name	Howard Rulf
Entity	We Energies
Ready to Ballot:	Yes
General Comment	
008-R1	
008-R2	
008-M1	
008-M2	
008-C1,1	
008-C1,2	
008-C1,3	
008-C1,4	
008-C2,1	
008-C2,2	
008-C2,3	
008-C2,4	

CIP-008 Drafting Team Responses to Comments

Name	Randy Schimka
Entity	San Diego Gas and Electric Co.
Ready to Ballot:	Yes
General Comment	
008-R1	
008-R2	
008-M1	
008-M2	
008-C1,1	
008-C1,2	
008-C1,3	
008-C1,4	
008-C2,1	
008-C2,2	
008-C2,3	
008-C2,4	

CIP-008 Drafting Team Responses to Comments

Name	Lyman Shaffer
Entity	PG&E
Ready to Ballot:	Yes
General Comment	
008-R1	
008-R2	
008-M1	
008-M2	
008-C1,1	
008-C1,2	
008-C1,3	
008-C1,4	
008-C2,1	
008-C2,2	
008-C2,3	
008-C2,4	

CIP-008 Drafting Team Responses to Comments

Name	Neil Shockey
Entity	Southern California Edison
Ready to Ballot:	Yes
General Comment	
008-R1	
008-R2	
008-M1	
008-M2	
008-C1,1	
008-C1,2	
008-C1,3	
008-C1,4	
008-C2,1	
008-C2,2	
008-C2,3	
008-C2,4	

CIP-008 Drafting Team Responses to Comments

Name	William Smith
Entity	Allegheny Power
Ready to Ballot:	Yes
General Comment	
008-R1	
008-R2	
008-M1	
008-M2	
008-C1,1	
008-C1,2	
008-C1,3	
008-C1,4	
008-C2,1	
008-C2,2	
008-C2,3	
008-C2,4	

CIP-008 Drafting Team Responses to Comments

Name	Paul Sorenson	
Entity	Open Access Technology International	
Ready to Ballot:	Yes	
General Comment	Clarification: If an entity has contracted with an agent to operate/manage critical cyber assets, is the responsible entity required to directly file incident reports, or does the managing/operational entity have to directly file incident reports?	R1.3 states that the Responsible Entity must ensure that all reportable Cyber Security Incidents are reported to the ES ISAC either directly or through an intermediary. A FAQ also addresses this topic.
008-R1		
008-R2		
008-M1		
008-M2		
008-C1,1		
008-C1,2		
008-C1,3		
008-C1,4		
008-C2,1		
008-C2,2		
008-C2,3		
008-C2,4		

CIP-008 Drafting Team Responses to Comments

Name	Robert Strauss	
Entity	NYSEG	
Ready to Ballot:	No	
General Comment	This Standard references the IAW SOP in R1.1 and R1.3. Prior to Version 0, NERC Operating Policies and Planning Standards sometimes had requirements in other documents. Version 0 moved all requirements and measures into the new Standards. Also, a CIPC group is re-writing the IAW SOP. That re-write is not being done as part of the NERC Reliability Standards "ANSI approved" process. It is inappropriate to change a Standard without using the Reliability Standards process. We recommend removing those IAW SOP references.	Please see responses to Ray A'Brial, Central Hudson Gas & Electric.
008-R1	Change R1.1 to "The Responsible Entity shall define procedures to characterize and classify events as Cyber Security Incidents." Change R1.3 to "The Responsibility Entity must ensure that the Cyber Security Incident is reported to the ES-ISAC either directly or through an intermediary."	
008-R2	Remove R2.1 and R2.2 since not all relevant incidents will give rise to all of the types of documentation listed. For instance, physical security incidents will generally not give rise to system or application log file entries and cyber incidents will not give rise to video and/or physical access records. Also remove "at a minimum" since the phrase is superfluous.	
008-M1		
008-M2		
008-C1,1		
008-C1,2		
008-C1,3		
008-C1,4		
008-C2,1		
008-C2,2	Change 2.2.3 to "A reportable Cyber Security Incident has occurred but was not reported to the ES-ISAC; or"	
008-C2,3	Change 2.3.2 to "Two or more reportable Cyber Security Incidents have occurred but were not reported to ES-ISAC"	
008-C2,4		

CIP-008 Drafting Team Responses to Comments

Name	Karl Tammar	
Entity	IRC	
Ready to Ballot:	No	
General Comment		
008-R1		
008-R2	1. The final sentence of Requirement R2 should be reworded as, "this documentation must include, where relevant, the following:.....". This change is needed since not all relevant incidents will give rise to all of the types of documentation listed. For instance, physical security incidents will generally not give rise to system or application log file entries and cyber incidents will not give rise to video and/or physical access records. 2. R2 Retention period should be 2 years. The utility of a 3 year retention period is unclear.	1. The sub-requirements for R2 have been removed. 2. The consensus opinion appears to support a three-year retention period for documentation regarding a reportable event, which corresponds with the three-year audit cycle. All other documentation required by this standard must be retained for one calendar year.
008-M1		
008-M2		
008-C1,1		
008-C1,2		
008-C1,3		
008-C1,4		
008-C2,1		
008-C2,2		
008-C2,3		
008-C2,4		

CIP-008 Drafting Team Responses to Comments

Name	Todd Thompson	
Entity	PJM Interconnection	
Ready to Ballot:	No	
General Comment		
008-R1		
008-R2	The final sentence of Requirement R2 should be reworded as, "this documentation must include, where relevant, the following:.....". This change is needed since not all relevant incidents will give rise to all of the types of documentation listed. For instance, physical security incidents will generally not give rise to system or application log file entries and cyber incidents will not give rise to video and/or physical access records. R2 Retention period should be 2 years. The utility of a 3 year retention period is unclear.	The sub-requirements for R2 have been removed. 2. The consensus opinion appears to support a three-year retention period for documentation regarding a reportable event, which corresponds with the three-year audit cycle. All other documentation required by this standard must be retained for one calendar year.
008-M1		
008-M2		
008-C1,1		
008-C1,2		
008-C1,3		
008-C1,4		
008-C2,1		
008-C2,2		
008-C2,3		
008-C2,4		

CIP-008 Drafting Team Responses to Comments

Name	Steven Townsend
Entity	Consumers Energy Co.
Ready to Ballot:	Yes
General Comment	
008-R1	
008-R2	
008-M1	
008-M2	
008-C1,1	
008-C1,2	
008-C1,3	
008-C1,4	
008-C2,1	
008-C2,2	
008-C2,3	
008-C2,4	

CIP-008 Drafting Team Responses to Comments

Name	Martin Trence	
Entity	Xcel Energy - Northen States Power (NSP)	
Ready to Ballot:	No	
General Comment		
008-R1	R1.3 - This requirement ignores the requirement by the DOE to submit a 417R for cases of suspected Cyber Security intrusions. This is a statutory requirement, and any reporting requirements developed must be coordinated with all statutory requirements as such. Review all statutory reporting requirements and revise this portion of the standard accordingly.	DOE-required reporting is not addressed in this standard. The drafting team will prepare a FAQ discussing the relationship between DOE and the ES ISAC.
008-R2		
008-M1		
008-M2		
008-C1,1		
008-C1,2		
008-C1,3		
008-C1,4		
008-C2,1		
008-C2,2		
008-C2,3		
008-C2,4		

Name	Rick Vermeers
Entity	Avistacorp
Ready to Ballot:	Yes
General Comment	
008-R1	
008-R2	
008-M1	
008-M2	
008-C1,1	
008-C1,2	
008-C1,3	
008-C1,4	
008-C2,1	
008-C2,2	
008-C2,3	
008-C2,4	

Name	Robert C. Webb	
Entity	Instrumentation, Systems and Automation Society	
Ready to Ballot:	No	
General Comment	1. Who is ISA and Why is ISA commenting on CIP-002 through CIP-009? These comments were developed by members of the Instrumentation, Systems and Automation Society, (ISA), SP99, "Manufacturing and Control Systems Security" committee's leadership team. The overall committee is composed of over 200 members including many users, government representatives, academics, control systems manufactures, and engineers with expertise in automation and control systems. ISA's SP99 is working to develop control systems security standards that provide sufficient guidance to the control systems and IT domain stakeholders to assure that security risks can be appropriately reduced without adversely affecting the intended functionality of those systems. ISA has published over 150 pages of guidance specific to the application of cyber security to control systems, in the form of two technical reports: ISA's ANSI/ISA-TR99.00.01-2004, "Security Technologies for Manufacturing and Control Systems", and ANSI/ISA-TR99.00.02-2004, "Integrating Electronic Security into the Manufacturing and Control Systems Environment." Both highlight the unique aspects of control systems which must be considered when applying security procedures and technology to control systems. ISA's constituency includes both fossil and nuclear power plant automation practitioners, and ISA has active standards committees in both of these areas (SP77, Fossil Power Plant Standards, and SP67, Nuclear Power Plant Standards). 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 have been working with NERC to establish a liaison process that would allow such considerations to be addressed earlier in the process. The development of that liaison process is nearly complete. However, comments are due at this time, and we believe these issues need to be addressed now, before approval of these standards, for the standards to be effective, without damaging the systems they are intended to protect. Thus members of the SP99 committee leadership team, with domain expertise in power generation and associated control systems have put together summary comments in several areas that should be addressed before issue of these standards. 2. Overview and Summary of Essential Changes In general, we found these documents to be excellent examples of how an industry group can (and should) provide coherent and well structured guidance on cybersecurity. We commend NERC's drafting team and review process; it has resulted in a quality set of documents that should be widely used. At the same time, and in fact because of the expected wide application of these documents, we believe that three general areas should be addressed before approval of these documents. a) Broader scope - to address a larger % of generation resources and key distribution resources,	Regarding comment #2a, the exclusionary language concerning generation assets has been removed with the exception of nuclear generation which is excluded by the SAR. Because distribution assets are not considered part of the Bulk Electric System, these resources remain excluded as well. Regarding comment #2b, much of the prescriptive language on how certain security measures should be applied has been removed. For example, the requirement for port scans in CIP 005, R4.2 has been replaced by a requirement to review only ports and services required for operations are enabled. In addition, the Drafting Team has removed most references to "how" security measures should be applied throughout the Standards unless it is required for compliance purposes. Regarding comment #2c, language has been added to reflect the fact that some security solutions that are available today were not available when some legacy systems were designed and put into service. CIP-003, CIP- 004, CIP-005, and CIP-006 contain language addressing exceptions to their policies that may be required to deal with legacy systems and facilities where modern security solutions are not technically possible. In these cases, the Responsible Entities must identify and document the exception and describe the mitigating steps they are taking to secure the assets in lieu of the modern solution. Regarding the comments #3, #4, and #5 related to scope, the Standard reflects the Standard Authorization Request which excluded distribution, nuclear generation, and telecommunication infrastructure. The Drafting Team cannot exceed the scope of the SAR. A SAR reflects the industry consensus on the scope of any particular standard to be developed. Once SAR has been approved for standards drafting, the scope cannot be changed. The NERC Reliability Standards process would require new SARs to address these scope issues.

s

and avoid excessive reliance on one boundary or layer of defense from cyber attacks. While we recognize the need to prioritize and prevent excessive requirements, we believe the current scope is overly restrictive, and excludes a significant portion of generation, and thereby significant vulnerabilities, in some areas. This is addressed in our specific comments on CIP-002-1, (and also CIP-003-1 through 009-1), which follow.

b) Additional cautions and guidance for control systems - in the form of specific requirements and references to key industry documents, to assure that the measures applied do not result in systems failures and reduced reliability instead of reduced risk. These cautions and guidance are necessary to address the special considerations needed when applying many normal security practices to control systems and control system networks -- particularly the bulk of legacy systems in operation today. Many do not have any ability to provide most of the required security features, and can be adversely affected by the application of other requirements. One good example is the requirement to do port scans (CIP 005-1, R4.2). Many legacy control networks are halted by port scans. The standard should include this caution, and suggest the use of alternatives to identify open ports on operational systems which have not been specifically designed and demonstrated to support this kind of testing without production failures. In general, more specific guidance on how to apply these requirements to the many legacy systems in use today should be provided.

c) Mandatory additional protection for inadequate legacy systems -- The phrase "where technically feasible" is used in a number of locations throughout the document. In many of these cases, alternatives are required. However, in others, no alternatives are required. Clearly stated requirements to add protection or barriers to cyber attack ("mitigation measures"), where they cannot be configured or incorporated into existing systems, should be added. It is not acceptable, in our view, to identify unacceptable risks, and then leave them because the existing equipment cannot be appropriately hardened. Appropriate countermeasures, to reduce risks to acceptable levels, should be required in all cases.

Addressing these concerns does not mean significant revision to this set of standards, or significant delay, in our opinion. It can be done effectively with minor changes and references in the generic text and in several specific locations. We suggest some of the specifics below. We believe these considerations are important to prevent the standards from being counterproductive or missing significant vulnerabilities.

3. Scope - Distribution assets that could have cyber impacts on transmission assets are excluded. All distribution assets that could have cyber impacts on Bulk Electric system assets should be included, to meet the objectives of the Standards. This comment also applies to the identical sections of the remaining standards (CIP-003 -- CIP-009).

4. Scope - Exclusion 3.2.1 should be removed; it excludes some of the larger generators that would otherwise be included under R1.1.4, and the NRC's requirements should be coordinated with, not independent of these requirements. This comment also applies to the identical sections of the remaining standards, (Section 4.2.1 of CIP-003 -- CIP-009).

5. Scope - Exclusion 3.2.2 should be removed; even when those communications systems are provided by others, the defined entities are still ultimately responsible for their proper operation and security. This comment also applies to the identical sections of the remaining standards, (Section 4.2.2 of CIP-003 -- CIP-009).

CIP-008 Drafting Team Responses to Comments

008-R1

008-R2

008-M1

008-M2

008-C1,1

008-C1,2

008-C1,3

008-C1,4

008-C2,1

008-C2,2

008-C2,3

008-C2,4

CIP-008 Drafting Team Responses to Comments

Name	Laurent Webber	
Entity	Western Area Power Administration	
Ready to Ballot:	No	
General Comment		
008-R1	R1.4: Remove the words, "and shall update the plan within ninety calendar days of any changes." Annual review and update is adequate. R1.5: The depth of the required testing is not well defined. Add a sentence similar to this one from CIP-009, "An exercise can range from a paper drill to a full operational and physical changeover." Sample wording could be, "The test can range from a walk-through of the Cyber Security Incident response plan to a full exercise of the plan. Actual Cyber Security Incident responses in compliance with the plan, followed by an analysis of the response and lessons learned will meet the testing requirement."	The standard requires an annual review of the incident response plan and updates as necessary. It is important that the plan be updated within 90 days of any changes, so that personnel are adequately prepared to respond to incidents. The following language was added: “A test can range from a paper drill, to a full operational exercise, to the response to an actual incident.
008-R2		
008-M1		
008-M2		
008-C1,1		
008-C1,2		
008-C1,3		
008-C1,4		
008-C2,1	Compliance 2.1.1: Change the phrase "within ninety calendar days of changes" to "annually." Annual updates are adequate.	Please see response, above.
008-C2,2		
008-C2,3		
008-C2,4		

Name	Michal Zeithammel
Entity	Brascan Power
Ready to Ballot:	Yes
General Comment	
008-R1	
008-R2	
008-M1	
008-M2	
008-C1,1	
008-C1,2	
008-C1,3	
008-C1,4	
008-C2,1	
008-C2,2	
008-C2,3	
008-C2,4	

CIP-008 Drafting Team Responses to Comments

Name	Guy Zito	
Entity	NPCC	
Ready to Ballot:	No	
General Comment	This Standard references the IAW SOP in R1.1 and R1.3. Prior to Version 0, NERC Operating Policies and Planning Standards sometimes had requirements in other documents. Version 0 moved all requirements and measures into the new Standards. Also, a CIPC group is re-writing the IAW SOP. That re-write is not being done as part of the NERC Reliability Standards "ANSI approved" process. It is inappropriate to change a Standard without using the Reliability Standards process. We recommend removing those IAW SOP references.	Please see responses to Ray A'Brial, Central Hudson Gas & Electric.
008-R1	Change R1.1 to "The Responsible Entity shall define procedures to characterize and classify events as Cyber Security Incidents." Change R1.3 to "The Responsibility Entity must ensure that the Cyber Security Incident is reported to the ES-ISAC either directly or through an intermediary."	
008-R2	Remove R2.1 and R2.2 since not all relevant incidents will give rise to all of the types of documentation listed. For instance, physical security incidents will generally not give rise to system or application log file entries and cyber incidents will not give rise to video and/or physical access records. Also remove "at a minimum" since the phrase is superfluous.	
008-M1		
008-M2		
008-C1,1		
008-C1,2		
008-C1,3		
008-C1,4		
008-C2,1		
008-C2,2	Change 2.2.3 to "A reportable Cyber Security Incident has occurred but was not reported to the ES-ISAC; or"	
008-C2,3	Change 2.3.2 to "Two or more reportable Cyber Security Incidents have occurred but were not reported to ES-ISAC"	
008-C2,4		

CIP-009 Drafting Team Responses to Comments

Name	Raymond A'Brial
Entity	Central Hudson Gas & Electric Corp
Ready to Ballot:	Yes
General Comments	
009-R1	
009-R2	
009-R3	
009-R4	
009-R5	
009-M1	
009-M2	
009-M3	
009-M4	
009-M5	
009-C1,1	
009-C1,2	
009-C1,3	
009-C1,4	
009-C2,1	
009-C2,2	
009-C2,3	
009-C2,4	

CIP-009 Drafting Team Responses to Comments

Name	Ori Artman
Entity	Teltone
Ready to Ballot:	Yes
General Comments	
009-R1	
009-R2	
009-R3	
009-R4	
009-R5	
009-M1	
009-M2	
009-M3	
009-M4	
009-M5	
009-C1,1	
009-C1,2	
009-C1,3	
009-C1,4	
009-C2,1	
009-C2,2	
009-C2,3	
009-C2,4	

CIP-009 Drafting Team Responses to Comments

Name	Steve Badgett
Entity	Riverside Public Utilitities
Ready to Ballot:	Yes
General Comments	
009-R1	
009-R2	
009-R3	
009-R4	
009-R5	
009-M1	
009-M2	
009-M3	
009-M4	
009-M5	
009-C1,1	
009-C1,2	
009-C1,3	
009-C1,4	
009-C2,1	
009-C2,2	
009-C2,3	
009-C2,4	

CIP-009 Drafting Team Responses to Comments

Name	Terry Baker
Entity	Platte River Power Authority
Ready to Ballot:	Yes
General Comments	
009-R1	
009-R2	
009-R3	
009-R4	
009-R5	
009-M1	
009-M2	
009-M3	
009-M4	
009-M5	
009-C1,1	
009-C1,2	
009-C1,3	
009-C1,4	
009-C2,1	
009-C2,2	
009-C2,3	
009-C2,4	

CIP-009 Drafting Team Responses to Comments

Name	Terry Bilke
Entity	Midwest ISO
Ready to Ballot:	No
General Comments	
009-R1	
009-R2	
009-R3	
009-R4	
009-R5	
009-M1	
009-M2	
009-M3	
009-M4	
009-M5	
009-C1,1	
009-C1,2	
009-C1,3	
009-C1,4	
009-C2,1	
009-C2,2	
009-C2,3	
009-C2,4	

CIP-009 Drafting Team Responses to Comments

Name	Pat Bourassa	
Entity	Wisconsin Public Service Corporation	
Ready to Ballot:	Yes	
General Comments		
009-R1		
009-R2	Full exercises are likely to cause disruption in operations centers and introduce real time problems. Table top exercises may be more appropriate annually, with a full exercise every 3-5 years.	The requirement states that "An exercise of the recovery plan can range from a paper drill, to a full operational exercise, to recovery from an actual incident."
009-R3		
009-R4		
009-R5		
009-M1		
009-M2		
009-M3		
009-M4		
009-M5		
009-C1,1		
009-C1,2		
009-C1,3		
009-C1,4		
009-C2,1		
009-C2,2		
009-C2,3		
009-C2,4		

CIP-009 Drafting Team Responses to Comments

Name	Laurence W. Brown	
Entity	Edison Electric Institute	
Ready to Ballot:	No	
General Comments		
009-R1	The Recovery Plan should also address notification of needed repairs, actual repair work, and similar activities to ensure that Critical Cyber Assets can be recovered or re-established following a Cyber Security Incident.	The requirements do not prohibit Responsible Entities from including the suggested level of detail in its Recovery Plan.
009-R2		
009-R3		
009-R4	"Secure storage" is unclear. Does the phrase imply security consistent with other requirements of the Standards? If so, that is excessive. It would be more reasonable to make clarify (perhaps in the FAQ) that this Requirement can be met by following practices such as those outlined in the NERC-CIPC Data Storage Guideline. SEE ALSO M4 and C2.2.2. SEE ALSO the Definition of Cyber Assets.	Reference to secure has been removed.
009-R5	"Prolonged period of time" is unclear, especially in conjunction with annual testing. Is data stored for more than one year but less than two covered? Does this apply to any data stored for longer than one year, as implied by M5? SEE ALSO C2.3.1.Reference to	Reference to a prolonged period of time has been clarified to read "at least annually."
009-M1		
009-M2		
009-M3		
009-M4		
009-M5		
009-C1,1		
009-C1,2		
009-C1,3		
009-C1,4		
009-C2,1		
009-C2,2		

CIP-009 Drafting Team Responses to Comments

009-C2,3

009-C2,4

CIP-009 Drafting Team Responses to Comments

Name	Peter Burke	
Entity	American Transmission Company	
Ready to Ballot:	No	
General Comments	American Transmission Company concurs with the comments submitted separately by the Edison Electric Institute and by the Midwest Reliability Organization.	Pleas see responses to Laurence W. Brown, Edison Electric Institute.
009-R1	American Transmission Company concurs with the comments submitted separately by the Edison Electric Institute.	
009-R2		
009-R3		
009-R4	American Transmission Company concurs with the comments submitted separately by the Edison Electric Institute.	
009-R5	American Transmission Company concurs with the comments submitted separately by the Edison Electric Institute and by the Midwest Reliability Organization.	
009-M1		
009-M2		
009-M3		
009-M4		
009-M5		
009-C1,1		
009-C1,2		
009-C1,3		
009-C1,4		
009-C2,1		
009-C2,2		
009-C2,3		
009-C2,4		

CIP-009 Drafting Team Responses to Comments

Name	Marc Butts	
Entity	Southern Company	
Ready to Ballot:	Yes	
General Comments		
009-R1		
009-R2		
009-R3		
009-R4		
009-R5		
009-M1		
009-M2		
009-M3		
009-M4		
009-M5		
009-C1,1		
009-C1,2		
009-C1,3		
009-C1,4		
009-C2,1		
009-C2,2		
009-C2,3	2.3.1 Level 3 - There is no definition for "a prolonged period of time". Also, this does not seem to be a Level 3 offense. Suggest dropping it or moving it to Level 2 - it seems to be a subset of the procedures required in 2.2.2 right above it.	Reference to a prolonged period of time has been removed.
009-C2,4		

CIP-009 Drafting Team Responses to Comments

Name	Gary Campbell	
Entity	MAIN	
Ready to Ballot:	No	
General Comments	address items below	
009-R1	Delete "response" and use "action". The word response is just to subtle for recovery plans and to canned.	The words "action in response to" have been added.
009-R2		
009-R3		
009-R4		
009-R5		
009-M1	Delete "response" and use "action". The word response is just to subtle for recovery plans and to canned.	M1 has been reworded. It now reads "Recovery plans(s) as specified in Requirement R1."
009-M2		
009-M3		
009-M4		
009-M5		
009-C1,1		
009-C1,2		
009-C1,3		
009-C1,4		
009-C2,1	2.1.1 Needs to be reworded. If the plans have been exercised, you would think then the types of events to activate the plan have been mentioned in the plan.	2.1.1 has been reworded.
009-C2,2	2.2.1 Why are we not testing for the 90 day calendar requiement mentioned in R3. Also, There is no requirement that I saw for a review to be done.	R1 requires Responsible Entites to create and annually review recovery plan(s) for Critical Cyber Assets. 2.1.2 has been modified to address the 90-day notification of changes to the plan.
009-C2,3	2.3.2 Could not find a requirement that records of reviews must be maintained for three years. Should be changed.	Changed to previous full calendar year.
009-C2,4		

CIP-009 Drafting Team Responses to Comments

Name	Linda Campbell	
Entity	FRCC	
Ready to Ballot:	No	
General Comments		
009-R1		
009-R2		
009-R3		
009-R4		
009-R5		
009-M1		
009-M2		
009-M3		
009-M4		
009-M5		
009-C1,1	In the applicability section 4.1.10 and 4.1.11, RRO's and NERC are included. Who has the monitoring responsibility for a RRO or NERC?	NERC will monitor the RROs and a third party without vested interest in the outcome will monitor NERC.
	Add Self-Certification and Audit information to this section. Proposed language would be: 1.1. Complaince Monitoring Responsibility Regional Reliability Organization. 1.1.1. The Compliance Monitor will request a self-certification annually. 1.1.2. The Compliance Monitor will perform an audit at least once every three (3)calendar years.	Self-certification has been added under "Additional Compliance Information."
009-C1,2		
009-C1,3	To complement a audit every three years, the data retention period should be 3 years.	The data retention period matches the requirement. The compliance monitor is required to keep records of an audit for 3 years.
009-C1,4		
009-C2,1		
009-C2,2		

009-C2,3

009-C2,4

CIP-009 Drafting Team Responses to Comments

Name	Roger Champagne
Entity	
Ready to Ballot:	Yes
General Comments	
009-R1	
009-R2	
009-R3	
009-R4	
009-R5	
009-M1	
009-M2	
009-M3	
009-M4	
009-M5	
009-C1,1	
009-C1,2	
009-C1,3	
009-C1,4	
009-C2,1	
009-C2,2	
009-C2,3	
009-C2,4	

CIP-009 Drafting Team Responses to Comments

Name	Larry Conrad
Entity	ECAR Critical Infrastructure Protection Panel
Ready to Ballot:	Yes
General Comments	
009-R1	
009-R2	
009-R3	
009-R4	
009-R5	
009-M1	
009-M2	
009-M3	
009-M4	
009-M5	
009-C1,1	
009-C1,2	
009-C1,3	
009-C1,4	
009-C2,1	
009-C2,2	
009-C2,3	
009-C2,4	

CIP-009 Drafting Team Responses to Comments

Name	Larry Conrad	
Entity	Cinergy	
Ready to Ballot:	No	
General Comments		
009-R1		
009-R2		
009-R3		
009-R4		
009-R5	R5. "Information stored on computer media for a prolonged period of time shall be tested at least annually to ensure that the information is recoverable." Please provide more specifics about what this information is, i.e., is it a complete system backup?	The requirement has been changed to read " Information essential to recovery that is stored on backup media...."
009-M1		
009-M2		
009-M3		
009-M4		
009-M5		
009-C1,1		
009-C1,2		
009-C1,3		
009-C1,4		
009-C2,1		
009-C2,2		
009-C2,3		
009-C2,4		

CIP-009 Drafting Team Responses to Comments

Name	Theodore Creedon, P.E.	
Entity	Creedon Engineering	
Ready to Ballot:	No	
General Comments	Periodic network testing and port scanning need to be thououghly addressed in this section. It is probable that lack of coordination between the IT department and engineering will result in inadvertent opened or blocked ports.	Please see drafting team response to this issue in CIP-007.
009-R1	Add: Recovery plans shall consider the impact of telecommunications failure during a Natinal Emergency. Manual procedures to restore power shall be considered. Loss of a single computer containing authorization keys shall be considered.	Per industry consensus during the SAR process, telecommunication infrastructure between the Electronic Security Perimeter is out of scope for these standards. Responsible Entities may include additional items in their response plans should they deem appropriate.
009-R2		
009-R3		
009-R4		
009-R5		
009-M1		
009-M2		
009-M3		
009-M4		
009-M5		
009-C1,1		
009-C1,2		
009-C1,3		
009-C1,4		
009-C2,1		
009-C2,2		
009-C2,3		
009-C2,4		

CIP-009 Drafting Team Responses to Comments

Name	Joel De Granda
Entity	Florida Power and Light
Ready to Ballot:	Yes
General Comments	
009-R1	
009-R2	
009-R3	
009-R4	
009-R5	
009-M1	
009-M2	
009-M3	
009-M4	
009-M5	
009-C1,1	
009-C1,2	
009-C1,3	
009-C1,4	
009-C2,1	
009-C2,2	
009-C2,3	
009-C2,4	

CIP-009 Drafting Team Responses to Comments

Name	Richard Engelbrecht
Entity	RGE
Ready to Ballot:	Yes
General Comments	
009-R1	
009-R2	
009-R3	
009-R4	
009-R5	
009-M1	
009-M2	
009-M3	
009-M4	
009-M5	
009-C1,1	
009-C1,2	
009-C1,3	
009-C1,4	
009-C2,1	
009-C2,2	
009-C2,3	
009-C2,4	

CIP-009 Drafting Team Responses to Comments

Name	Ken Fell
Entity	New York ISO
Ready to Ballot:	Yes
General Comments	
009-R1	
009-R2	
009-R3	
009-R4	
009-R5	
009-M1	
009-M2	
009-M3	
009-M4	
009-M5	
009-C1,1	
009-C1,2	
009-C1,3	
009-C1,4	
009-C2,1	
009-C2,2	
009-C2,3	
009-C2,4	

CIP-009 Drafting Team Responses to Comments

Name	Francis Flynn
Entity	National Grid USA
Ready to Ballot:	Yes
General Comments	
009-R1	
009-R2	
009-R3	
009-R4	
009-R5	
009-M1	
009-M2	
009-M3	
009-M4	
009-M5	
009-C1,1	
009-C1,2	
009-C1,3	
009-C1,4	
009-C2,1	
009-C2,2	
009-C2,3	
009-C2,4	

CIP-009 Drafting Team Responses to Comments

Name	Greg Fraser
Entity	Manitoba Hydro
Ready to Ballot:	Yes
General Comments	
009-R1	
009-R2	
009-R3	
009-R4	
009-R5	
009-M1	
009-M2	
009-M3	
009-M4	
009-M5	
009-C1,1	
009-C1,2	
009-C1,3	
009-C1,4	
009-C2,1	
009-C2,2	
009-C2,3	
009-C2,4	

CIP-009 Drafting Team Responses to Comments

Name	Jerry Freese	
Entity	American Electric Power	
Ready to Ballot:	No	
General Comments	Based on the expanded scope set forth in CIP-002 R1 for the Critical Assets and the subsequently expanded scope of the Critical Cyber Assets and the Electronic Security Perimeter, it would be impractical and infeasible to meet the obligations set forth in this requirement.	CIP-002 has been changed.
009-R1		
009-R2		
009-R3		
009-R4		
009-R5		
009-M1		
009-M2		
009-M3		
009-M4		
009-M5		
009-C1,1		
009-C1,2		
009-C1,3		
009-C1,4		
009-C2,1		
009-C2,2		
009-C2,3		
009-C2,4		

CIP-009 Drafting Team Responses to Comments

Name	Edwin C. Goff III
Entity	Progress Energy
Ready to Ballot:	Yes
General Comments	
009-R1	
009-R2	
009-R3	
009-R4	
009-R5	
009-M1	
009-M2	
009-M3	
009-M4	
009-M5	
009-C1,1	
009-C1,2	
009-C1,3	
009-C1,4	
009-C2,1	
009-C2,2	
009-C2,3	
009-C2,4	

CIP-009 Drafting Team Responses to Comments

Name	Kenneth Goldsmith
Entity	Alliant Energy
Ready to Ballot:	Yes
General Comments	
009-R1	
009-R2	
009-R3	
009-R4	
009-R5	
009-M1	
009-M2	
009-M3	
009-M4	
009-M5	
009-C1,1	
009-C1,2	
009-C1,3	
009-C1,4	
009-C2,1	
009-C2,2	
009-C2,3	
009-C2,4	

CIP-009 Drafting Team Responses to Comments

Name	Kathleen Goodman	
Entity	ISO New England Inc	
Ready to Ballot:	No	
General Comments		
009-R1	R1.1 Should be removed. It is not clear what is being asked for here. Why you make a decision to activate recovery plans is a case-by-case decision that can not always be anticipated. What you do is important and is addressed in R1.2 through R1.5.	The requirement asks for Responsible Entities to plan for recovery of Critical Cyber Assets after a reasonably foreseeable unplanned event. This does not require a Responsible Entity to anticipate every possible event.
009-R2		
009-R3		
009-R4		
009-R5		
009-M1		
009-M2		
009-M3		
009-M4		
009-M5		
009-C1,1		
009-C1,2		
009-C1,3	It is not clear when you mean documents, records, or data. These are three distinct items and should not be referenced interchangeably. Please clarify.	The Drafting Team has revised the standards for consistency and uses the terms as follows: DATA: information in a raw form. RECORDS: objective evidence that an activity has occurred. Records typically provide a snapshot in time of past actions and events, and can be used to demonstrate compliance. Records can only be modified or revised in compliance with proper and auditable trails. LOGS: Generally, collections of records of events that are generated automatically or by following a manual process. They identify who or what caused the event to be written and are time-stamped to indicate when the event occurred. DOCUMENTS: demonstrate what an organization does and plans to do and instruct employees how they should perform their tasks. Documents include but are not limited to policies, processes and procedures, specifications, drawings, maps, etc. A document can be in paper or electronic format. See the FAQ.

009-C1,4		
009-C2,1	2.1. should be removed.	This section is necessary to establish progressive levels of non-compliance.
009-C2,2		
009-C2,3		
009-C2,4		

Name	Tim Hattaway
Entity	Alabama Electric Cooperative
Ready to Ballot:	Yes
General Comments	
009-R1	
009-R2	
009-R3	
009-R4	
009-R5	
009-M1	
009-M2	
009-M3	
009-M4	
009-M5	
009-C1,1	
009-C1,2	
009-C1,3	
009-C1,4	
009-C2,1	
009-C2,2	
009-C2,3	
009-C2,4	

CIP-009 Drafting Team Responses to Comments

Name	Jerry Heeren
Entity	MEAG Power
Ready to Ballot:	Yes
General Comments	
009-R1	
009-R2	
009-R3	
009-R4	
009-R5	
009-M1	
009-M2	
009-M3	
009-M4	
009-M5	
009-C1,1	
009-C1,2	
009-C1,3	
009-C1,4	
009-C2,1	
009-C2,2	
009-C2,3	
009-C2,4	

CIP-009 Drafting Team Responses to Comments

Name	Peter Henderson
Entity	Independent Electricity System Operator (IESO)
Ready to Ballot:	Yes
General Comments	
009-R1	
009-R2	
009-R3	
009-R4	
009-R5	
009-M1	
009-M2	
009-M3	
009-M4	
009-M5	
009-C1,1	
009-C1,2	
009-C1,3	
009-C1,4	
009-C2,1	
009-C2,2	
009-C2,3	
009-C2,4	

CIP-009 Drafting Team Responses to Comments

Name	E. Nick Henery	
Entity	SMUD	
Ready to Ballot:	Yes	
General Comments	The Drafting Team will need to go through the Standard and assign responsibility to each function from the functional model like the Version 0 STD. For this Standard to enforceable the generic use of Responsible Entity is the same as the generic use of Control Area. Even if the Standard lists the different functions it leaves open the possibility of misinterpretation as to which function is truly responsible.	The Responsible Entities are clearly enumerated in the standard Section A, item 4.
009-R1		
009-R2		
009-R3		
009-R4		
009-R5		
009-M1		
009-M2		
009-M3		
009-M4		
009-M5		
009-C1,1		
009-C1,2		
009-C1,3		
009-C1,4		
009-C2,1		
009-C2,2		
009-C2,3		
009-C2,4		

CIP-009 Drafting Team Responses to Comments

Name	Jack Hobbick
Entity	Consumers Energy
Ready to Ballot:	Yes
General Comments	
009-R1	
009-R2	
009-R3	
009-R4	
009-R5	
009-M1	
009-M2	
009-M3	
009-M4	
009-M5	
009-C1,1	
009-C1,2	
009-C1,3	
009-C1,4	
009-C2,1	
009-C2,2	
009-C2,3	
009-C2,4	

CIP-009 Drafting Team Responses to Comments

Name	Richard Kafka	
Entity	Pepco Holdings, Inc.	
Ready to Ballot:	No	
General Comments		
009-R1	The Recovery Plan should also address notification of needed repairs, actual repair work, and similar activities to ensure that Critical Cyber Assets can be recovered or re-established following a Cyber Security Incident.	Please see responses to Laurence W. Brown, Edison Electric Institute.
009-R2		
009-R3		
009-R4	"Secure storage" is unclear. See comments on definitions.	
009-R5	"Prolonged period of time" is unclear, especially in conjunction with annual testing. Is data stored for more than one year but less than two covered? Does this apply to any data stored for longer than one year, as implied by M5?	
009-M1		
009-M2		
009-M3		
009-M4		
009-M5		
009-C1,1		
009-C1,2		
009-C1,3		
009-C1,4		
009-C2,1		
009-C2,2		
009-C2,3		
009-C2,4		

CIP-009 Drafting Team Responses to Comments

Name	Tony Kroskey	
Entity	Brazos Electric Power Cooperative	
Ready to Ballot:	No	
General Comments		
009-R1		
009-R2		
009-R3		
009-R4	Suggest changing word "chips' to "electronic components".	Changed as suggested.
009-R5		
009-M1		
009-M2		
009-M3		
009-M4		
009-M5		
009-C1,1		
009-C1,2		
009-C1,3		
009-C1,4		
009-C2,1		
009-C2,2		
009-C2,3		
009-C2,4		

CIP-009 Drafting Team Responses to Comments

Name	Carol Krysevig	
Entity	Allegheny Energy Supply Co. LLC	
Ready to Ballot:	No	
General Comments	D2.2.1. Add '(if necessary)' after 'but have not been reviewed and updated'.	Reference to "updated" in 2.2.1 has been removed.
009-R1		
009-R2	Is the intent of the exercise requirement to require that all recovery plan(s) be exercised each year or just a representative sample of the plan(s)? A representative sample of the plan(s) would fulfill the intent of the exercise requirement without being overly onerous.	The intent is to test the major elements of the Recovery Plan. Please refer to the FAQs for guidance.
009-R3		
009-R4		
009-R5		
009-M1		
009-M2		
009-M3		
009-M4		
009-M5		
009-C1,1		
009-C1,2		
009-C1,3		
009-C1,4		
009-C2,1		
009-C2,2		
009-C2,3		
009-C2,4		

CIP-009 Drafting Team Responses to Comments

Name	John Lim	
Entity	Con Edison	
Ready to Ballot:	No	
General Comments	While CIP-009 appears ready for balloting, Con Edison believes that balloting should be performed for all the standards as a group. Consequently, we have marked CIP-009 as not ready for balloting.	The drafting team supports balloting this standard as part of a suite of cyber security standards, CIP-002 through CIP-009.
009-R1		
009-R2		
009-R3		
009-R4		
009-R5		
009-M1		
009-M2		
009-M3		
009-M4		
009-M5		
009-C1,1		
009-C1,2		
009-C1,3		
009-C1,4		
009-C2,1		
009-C2,2		
009-C2,3		
009-C2,4		

CIP-009 Drafting Team Responses to Comments

Name	Deborah Linke	
Entity	Bureau of Reclamation	
Ready to Ballot:	No	
General Comments	Generally, we believe that annual updates and reviews of documentation are adequate absent a major system change. Based on this we recommended deleting references to other time frames.	The standard requires an annual review of the recovery plan and updates as necessary. It is important that appropriate personnel be advised of changes to the plan. Industry consensus, gauged by comments received, supports notification within 90 days as reasonable.
009-R1		
009-R2		
009-R3		
009-R4		
009-R5	R5: This requirement should only apply to critical restoration information for critical cyber assets. Sample wording could be, "Information crucial to the restoration of Critical Cyber Assets and stored on computer media for a prolonged period of time..."	The requirement has been changed to read "Information essential to recovery that is stored on backup media shall be tested at least annually to ensure that the information is available. Testing can be completed off site."
009-M1		
009-M2		
009-M3		
009-M4		
009-M5		
009-C1,1		
009-C1,2		
009-C1,3		
009-C1,4		
009-C2,1		
009-C2,2		
009-C2,3		
009-C2,4		

CIP-009 Drafting Team Responses to Comments

Name	Greg Mason
Entity	Dynegy Generation
Ready to Ballot:	Yes
General Comments	
009-R1	
009-R2	
009-R3	
009-R4	
009-R5	
009-M1	
009-M2	
009-M3	
009-M4	
009-M5	
009-C1,1	
009-C1,2	
009-C1,3	
009-C1,4	
009-C2,1	
009-C2,2	
009-C2,3	
009-C2,4	

CIP-009 Drafting Team Responses to Comments

Name	Paul McClay
Entity	Tampa Electric
Ready to Ballot:	Yes
General Comments	
009-R1	
009-R2	
009-R3	
009-R4	
009-R5	
009-M1	
009-M2	
009-M3	
009-M4	
009-M5	
009-C1,1	
009-C1,2	
009-C1,3	
009-C1,4	
009-C2,1	
009-C2,2	
009-C2,3	
009-C2,4	

CIP-009 Drafting Team Responses to Comments

Name	David McCoy	
Entity	Great Plains Energy/Kansas City Power & Light	
Ready to Ballot:	No	
General Comments		
009-R1		
009-R2		
009-R3		
009-R4		
009-R5		
009-M1		
009-M2		
009-M3		
009-M4		
009-M5		
009-C1,1		
009-C1,2		
009-C1,3		
009-C1,4		
009-C2,1		
009-C2,2	"Secure storage of information" should be defined somewhere.	Reference to "secure" has been removed.
009-C2,3	"Prolonged period of time" should be defined.	The verbiage was changed to "at least annually."
009-C2,4		

CIP-009 Drafting Team Responses to Comments

Name	Don Miller
Entity	First Energy Corp
Ready to Ballot:	Yes
General Comments	
009-R1	
009-R2	
009-R3	
009-R4	
009-R5	
009-M1	
009-M2	
009-M3	
009-M4	
009-M5	
009-C1,1	
009-C1,2	
009-C1,3	
009-C1,4	
009-C2,1	
009-C2,2	
009-C2,3	
009-C2,4	

CIP-009 Drafting Team Responses to Comments

Name	Patrick Miller	
Entity	PacifiCorp	
Ready to Ballot:	No	
General Comments		
009-R1		
009-R2		
009-R3		
009-R4		
009-R5		
009-M1	For M1, the language is leaning toward scenario-based response, which is not considered best-practice except where a particular scnario has a high likelihood of occurring.	The requirement asks for Responsible Entities to plan for recovery of Critical Cyber Assets after a reasonably foreseeable unplanned event. This does not require a Responsible Entity to anticipate every possible event.
009-M2		
009-M3		
009-M4		
009-M5		
009-C1,1		
009-C1,2		
009-C1,3		
009-C1,4		
009-C2,1		
009-C2,2		
009-C2,3		
009-C2,4		

CIP-009 Drafting Team Responses to Comments

Name	Jeff Mitchell
Entity	ECAR
Ready to Ballot:	Yes
General Comments	N/A
009-R1	
009-R2	
009-R3	
009-R4	
009-R5	
009-M1	
009-M2	
009-M3	
009-M4	
009-M5	
009-C1,1	
009-C1,2	
009-C1,3	
009-C1,4	
009-C2,1	
009-C2,2	
009-C2,3	
009-C2,4	

CIP-009 Drafting Team Responses to Comments

Name	Scott Mix
Entity	KEMA, Inc
Ready to Ballot:	Yes
General Comments	
009-R1	
009-R2	
009-R3	
009-R4	
009-R5	
009-M1	
009-M2	
009-M3	
009-M4	
009-M5	
009-C1,1	
009-C1,2	
009-C1,3	
009-C1,4	
009-C2,1	
009-C2,2	
009-C2,3	
009-C2,4	

CIP-009 Drafting Team Responses to Comments

Name	Darrick Moe	
Entity	WAPA	
Ready to Ballot:	No	
General Comments		
009-R1		
009-R2		
009-R3		
009-R4		
009-R5	Regarding R5 Testing Backup Media: The annual testing of information recoverability should apply only to information (programs & data) necessary to restore normal operations of the critical cyber assets. Purely historical information associated with the assets should be specifically exempted from the yearly recoverability test.	The requirement has been changed to read "Information essential to recovery that is stored on backup media shall be tested at least annually to ensure that the information is available.
009-M1		
009-M2		
009-M3		
009-M4		
009-M5		
009-C1,1		
009-C1,2		
009-C1,3		
009-C1,4		
009-C2,1		
009-C2,2		
009-C2,3		
009-C2,4		

CIP-009 Drafting Team Responses to Comments

Name	Selby Mohr
Entity	Sacramento Municipal Utility District
Ready to Ballot:	Yes
General Comments	
009-R1	
009-R2	
009-R3	
009-R4	
009-R5	
009-M1	
009-M2	
009-M3	
009-M4	
009-M5	
009-C1,1	
009-C1,2	
009-C1,3	
009-C1,4	
009-C2,1	
009-C2,2	
009-C2,3	
009-C2,4	

CIP-009 Drafting Team Responses to Comments

Name	Kurt Muehlbauer	
Entity	Exelon	
Ready to Ballot:	No	
General Comments	The documentation and processes around the responsible entity s tasks are too prescriptive. The industry needs to be extremely careful to avoid the creation of purely documentation-based non-compliances. With increasing legal requirements for compliance, and the associated penalties for noncompliance, noncompliance should be reserved for real security issues. It is simply too easy to make a mistake in documentation in light of the constantly evolving cyber environment. Each entity should develop its own processes in support of the requirements, and these processes should be required to contain provisions for periodic review and approval applicable to each requirement. The processes should also be required to produce reasonable documentation to demonstrate compliance. However, it is not necessary to specify the details of the documentation or review periods. The above approach can be met by removing references to documentation from the requirements section. Then, in the measures section require each entity to reasonably document programs and processes that support the security requirements and to produce reasonable documentation required to demonstrate compliance to the security requirements. Please refer to our overall comments on defining reasonable. If the above approach is taken, it will be possible to delete many of the sub-bullet points under each requirement (because the details will be specified by each entity in their program or process, as applicable). This will also ensure that documentation and excessive low-value administrative tasks are removed from the requirements.	The Drafting team has reviewed the standards and removed prescription where possible. The prescriptiveness that remains is necessary to provide the clarity requested by a majority of commenters. The documentation required by these standards allow Responsible Entities to demonstrate that the policies, processes, and procedures that they have implemented consistently comply with the requirements of these standards.
009-R1		
009-R2		
009-R3		
009-R4		
009-R5		
009-M1	Refer to general, overall comments submitted on CIP-002 through CIP-009 regarding revision of the measures and compliance specification.	
009-M2	Refer to general, overall comments submitted on CIP-002 through CIP-009 regarding revision of the measures and compliance specification.	

CIP-009 Drafting Team Responses to Comments

009-M3 Refer to general, overall comments submitted on CIP-002 through CIP-009 regarding revision of the measures and compliance specification.

009-M4 Refer to general, overall comments submitted on CIP-002 through CIP-009 regarding revision of the measures and compliance specification.

009-M5 Refer to general, overall comments submitted on CIP-002 through CIP-009 regarding revision of the measures and compliance specification.

009-C1,1 Refer to general, overall comments submitted on CIP-002 through CIP-009 regarding revision of the measures and compliance specification.

009-C1,2 Refer to general, overall comments submitted on CIP-002 through CIP-009 regarding revision of the measures and compliance specification.

009-C1,3 Refer to general, overall comments submitted on CIP-002 through CIP-009 regarding revision of the measures and compliance specification.

009-C1,4 Refer to general, overall comments submitted on CIP-002 through CIP-009 regarding revision of the measures and compliance specification.

009-C2,1 Refer to general, overall comments submitted on CIP-002 through CIP-009 regarding revision of the measures and compliance specification.

009-C2,2 Refer to general, overall comments submitted on CIP-002 through CIP-009 regarding revision of the measures and compliance specification.

009-C2,3 Refer to general, overall comments submitted on CIP-002 through CIP-009 regarding revision of the measures and compliance specification.

009-C2,4 Refer to general, overall comments submitted on CIP-002 through CIP-009 regarding revision of the measures and compliance specification.

CIP-009 Drafting Team Responses to Comments

Name	Jeffrey Mueller	
Entity	PSEG Companies	
Ready to Ballot:	No	
General Comments	The PSEG Companies have reviewed and share the concerns expressed in the Comments of PJM and EEI. Accordingly, the PSEG Companies support the comments of PJM and EEI, and request that the concerns expressed in those comments be properly addressed in the next version of the draft standard.	Please see response to Laurence W. Brown, Edison Electric Institute.
009-R1		
009-R2		
009-R3		
009-R4		
009-R5		
009-M1		
009-M2		
009-M3		
009-M4		
009-M5		
009-C1,1		
009-C1,2		
009-C1,3		
009-C1,4		
009-C2,1		
009-C2,2		
009-C2,3		
009-C2,4		

CIP-009 Drafting Team Responses to Comments

Name	Mitchell Needham
Entity	Tennessee Valley Authority
Ready to Ballot:	Yes
General Comments	
009-R1	
009-R2	
009-R3	
009-R4	
009-R5	
009-M1	
009-M2	
009-M3	
009-M4	
009-M5	
009-C1,1	
009-C1,2	
009-C1,3	
009-C1,4	
009-C2,1	
009-C2,2	
009-C2,3	
009-C2,4	

CIP-009 Drafting Team Responses to Comments

Name	Dave Norton
Entity	Entergy Transmission
Ready to Ballot:	Yes
General Comments	
009-R1	
009-R2	
009-R3	
009-R4	
009-R5	
009-M1	
009-M2	
009-M3	
009-M4	
009-M5	
009-C1,1	
009-C1,2	
009-C1,3	
009-C1,4	
009-C2,1	
009-C2,2	
009-C2,3	
009-C2,4	

CIP-009 Drafting Team Responses to Comments

Name	Doug Orlofske
Entity	Wisconsin Public Power Inc
Ready to Ballot:	Yes
General Comments	
009-R1	
009-R2	
009-R3	
009-R4	
009-R5	
009-M1	
009-M2	
009-M3	
009-M4	
009-M5	
009-C1,1	
009-C1,2	
009-C1,3	
009-C1,4	
009-C2,1	
009-C2,2	
009-C2,3	
009-C2,4	

CIP-009 Drafting Team Responses to Comments

Name	Kevin Perry	
Entity	Southwest Power Pool	
Ready to Ballot:	No	
General Comments	Recovery Plans for cyber systems is a business continuity issue and not a cyber security issue. Requirements for continuity of business/disaster recovery are adequately covered by other NERC standards.	To ensure reliability, the Critical Cyber Assets must not only be secured but a plan must be in place to return them to functional operability following an incident or event. Effective Recovery plan(s) are an essential function of Critical Cyber Asset security.
009-R1	This is not a cyber security issue. It is a continuity of business/disaster recovery issue. This requirement should not be in a cyber security standard.	See above.
009-R2	This is not a cyber security issue. It is a continuity of business/disaster recovery issue. This requirement should not be in a cyber security standard.	See above.
009-R3	This is not a cyber security issue. It is a continuity of business/disaster recovery issue. This requirement should not be in a cyber security standard.	See above.
009-R4	This is not a cyber security issue. It is a continuity of business/disaster recovery issue. This requirement should not be in a cyber security standard.	See above.
009-R5	This is not a cyber security issue. It is a continuity of business/disaster recovery issue. This requirement should not be in a cyber security standard.	See above.
009-M1		
009-M2		
009-M3		
009-M4		
009-M5		
009-C1,1		
009-C1,2		
009-C1,3		
009-C1,4	Approval of exceptions to the standard should not be delegated.	Exceptions cannot be taken to NERC standards. It is up to Responsible Entities to define policies, exception handling, and delegation authority.
009-C2,1		
009-C2,2		
009-C2,3		
009-C2,4		

CIP-009 Drafting Team Responses to Comments

Name	Tom Pruitt	
Entity	Duke Power Company	
Ready to Ballot:	No	
General Comments	A.4.1 -- Given the critical role of the PSE, why are these standards not applicable to that entity? A.4.2.2 -- Appears to be inconsistent with definition of "Cyber Asset". A.5 -- This should reference the proposed Implementation Plan. Alternatively, the compliance implementation plan should be referenced in the compliance sections for all of CIP002 thru CIP 009.	The standards reflect the Standard Authorization Request (SAR), which excluded PSEs. The drafting team must respect the scope of the SAR and not extend it during standards development. The SAR reflects industry consensus on the scope of the standard to be developed. The SAR also specifically excluded communication links. Although reviewed and commented upon by the industry, the Implementation Plan is not part of the standard and cannot be referenced therein.
009-R1		
009-R2		
009-R3		
009-R4		
009-R5	R5 -- Clarify "prolonged period of time"; alternatively, clarify the intent of the testing requirement.	Reference to prolonged period of time has been removed. The requirement now states that "Information essential to recovery that is stored on backup media shall be tested at least annually to ensure that the information is available."
009-M1		
009-M2		
009-M3		
009-M4		
009-M5		
009-C1,1		
009-C1,2		
009-C1,3		
009-C1,4		
009-C2,1		
009-C2,2		
009-C2,3		
009-C2,4		

CIP-009 Drafting Team Responses to Comments

Name	Duane Radzwion
Entity	Consumers Energy
Ready to Ballot:	Yes
General Comments	
009-R1	
009-R2	
009-R3	
009-R4	
009-R5	
009-M1	
009-M2	
009-M3	
009-M4	
009-M5	
009-C1,1	
009-C1,2	
009-C1,3	
009-C1,4	
009-C2,1	
009-C2,2	
009-C2,3	
009-C2,4	

CIP-009 Drafting Team Responses to Comments

Name	Howard Rulf
Entity	We Energies
Ready to Ballot:	Yes
General Comments	
009-R1	
009-R2	
009-R3	
009-R4	
009-R5	
009-M1	
009-M2	
009-M3	
009-M4	
009-M5	
009-C1,1	
009-C1,2	
009-C1,3	
009-C1,4	
009-C2,1	
009-C2,2	
009-C2,3	
009-C2,4	

CIP-009 Drafting Team Responses to Comments

Name	Randy Schimka
Entity	San Diego Gas and Electric Co.
Ready to Ballot:	Yes
General Comments	
009-R1	
009-R2	
009-R3	
009-R4	
009-R5	
009-M1	
009-M2	
009-M3	
009-M4	
009-M5	
009-C1,1	
009-C1,2	
009-C1,3	
009-C1,4	
009-C2,1	
009-C2,2	
009-C2,3	
009-C2,4	

CIP-009 Drafting Team Responses to Comments

Name	Lyman Shaffer	
Entity	PG&E	
Ready to Ballot:	Yes	
General Comments		
009-R1		
009-R2		
009-R3		
009-R4		
009-R5	Testing Back Up media" if this means all backups for critical cyber assets, then it is overly burdonsome.	The requirement has been clarified to read "Information essential to recovery that is stored on backup media shall be tested at least annually to ensure that the information is available."
009-M1		
009-M2		
009-M3		
009-M4		
009-M5		
009-C1,1		
009-C1,2		
009-C1,3		
009-C1,4		
009-C2,1		
009-C2,2		
009-C2,3		
009-C2,4		

CIP-009 Drafting Team Responses to Comments

Name	Neil Shockey
Entity	Southern California Edison
Ready to Ballot:	Yes
General Comments	
009-R1	
009-R2	
009-R3	
009-R4	
009-R5	
009-M1	
009-M2	
009-M3	
009-M4	
009-M5	
009-C1,1	
009-C1,2	
009-C1,3	
009-C1,4	
009-C2,1	
009-C2,2	
009-C2,3	
009-C2,4	

CIP-009 Drafting Team Responses to Comments

Name	William Smith
Entity	Allegheny Power
Ready to Ballot:	Yes
General Comments	
009-R1	
009-R2	
009-R3	
009-R4	
009-R5	
009-M1	
009-M2	
009-M3	
009-M4	
009-M5	
009-C1,1	
009-C1,2	
009-C1,3	
009-C1,4	
009-C2,1	
009-C2,2	
009-C2,3	
009-C2,4	

CIP-009 Drafting Team Responses to Comments

Name	Paul Sorenson	
Entity	Open Access Technology International	
Ready to Ballot:	Yes	
General Comments	What is the rationale or intent behind requiring retention of Recovery Plan documents for three years whereas most of the other standards require only 1 year retention?	Data rentention has been changed to the previous full calendar year.
009-R1		
009-R2		
009-R3		
009-R4		
009-R5		
009-M1		
009-M2		
009-M3		
009-M4		
009-M5		
009-C1,1		
009-C1,2		
009-C1,3		
009-C1,4		
009-C2,1		
009-C2,2		
009-C2,3		
009-C2,4		

CIP-009 Drafting Team Responses to Comments

Name	Robert Strauss
Entity	NYSEG
Ready to Ballot:	Yes
General Comments	
009-R1	
009-R2	
009-R3	
009-R4	
009-R5	
009-M1	
009-M2	
009-M3	
009-M4	
009-M5	
009-C1,1	
009-C1,2	
009-C1,3	
009-C1,4	
009-C2,1	
009-C2,2	
009-C2,3	
009-C2,4	

CIP-009 Drafting Team Responses to Comments

Name	Karl Tammar
Entity	IRC
Ready to Ballot:	Yes
General Comments	
009-R1	
009-R2	
009-R3	
009-R4	
009-R5	
009-M1	
009-M2	
009-M3	
009-M4	
009-M5	
009-C1,1	
009-C1,2	
009-C1,3	
009-C1,4	
009-C2,1	
009-C2,2	
009-C2,3	
009-C2,4	

CIP-009 Drafting Team Responses to Comments

Name	Todd Thompson
Entity	PJM Interconnection
Ready to Ballot:	Yes
General Comments	
009-R1	
009-R2	
009-R3	
009-R4	
009-R5	
009-M1	
009-M2	
009-M3	
009-M4	
009-M5	
009-C1,1	
009-C1,2	
009-C1,3	
009-C1,4	
009-C2,1	
009-C2,2	
009-C2,3	
009-C2,4	

CIP-009 Drafting Team Responses to Comments

Name	Steven Townsend
Entity	Consumers Energy Co.
Ready to Ballot:	Yes
General Comments	
009-R1	
009-R2	
009-R3	
009-R4	
009-R5	
009-M1	
009-M2	
009-M3	
009-M4	
009-M5	
009-C1,1	
009-C1,2	
009-C1,3	
009-C1,4	
009-C2,1	
009-C2,2	
009-C2,3	
009-C2,4	

CIP-009 Drafting Team Responses to Comments

Name	Martin Trence
Entity	Xcel Energy - Northen States Power (NSP)
Ready to Ballot:	Yes
General Comments	
009-R1	
009-R2	
009-R3	
009-R4	
009-R5	
009-M1	
009-M2	
009-M3	
009-M4	
009-M5	
009-C1,1	
009-C1,2	
009-C1,3	
009-C1,4	
009-C2,1	
009-C2,2	
009-C2,3	
009-C2,4	

CIP-009 Drafting Team Responses to Comments

Name	Rick Vermeers
Entity	Avistacorp
Ready to Ballot:	Yes
General Comments	
009-R1	
009-R2	
009-R3	
009-R4	
009-R5	
009-M1	
009-M2	
009-M3	
009-M4	
009-M5	
009-C1,1	
009-C1,2	
009-C1,3	
009-C1,4	
009-C2,1	
009-C2,2	
009-C2,3	
009-C2,4	

Name Robert C. Webb

Entity Instrumentation, Systems and Automation Society

Ready to Ballot: No

General Comments

1. Who is ISA and Why is ISA commenting on CIP-002 through CIP-009?

These comments were developed by members of the Instrumentation, Systems and Automation Society, (ISA), SP99, "Manufacturing and Control Systems Security" committee’s leadership team. The overall committee is composed of over 200 members including many users, government representatives, academics, control systems manufactures, and engineers with expertise in automation and control systems. ISA’s SP99 is working to develop control systems security standards that provide sufficient guidance to the control systems and IT domain stakeholders to assure that security risks can be appropriately reduced without adversely affecting the intended functionality of those systems. ISA has published over 150 pages of guidance specific to the application of cyber security to control systems, in the form of two technical reports: ISA’s ANSI/ISA-TR99.00.01-2004, "Security Technologies for Manufacturing and Control Systems", and ANSI/ISA-TR99.00.02-2004, "Integrating Electronic Security into the Manufacturing and Control Systems Environment." Both highlight the unique aspects of control systems which must be considered when applying security procedures and technology to control systems. ISA’s constituency includes both fossil and nuclear power plant automation practitioners, and ISA has active standards committees in both of these areas (SP77, Fossil Power Plant Standards, and SP67, Nuclear Power Plant Standards).

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 have been working with NERC to establish a liaison process that would allow such considerations to be addressed earlier in the process. The development of that liaison process is nearly complete. However, comments are due at this time, and we believe these issues need to be addressed now, before approval of these standards, for the standards to be effective, without damaging the systems they are intended to protect. Thus members of the SP99 committee leadership team, with domain expertise in power generation and associated control systems have put together summary comments in several areas that should be addressed before issue of these standards.

2. Overview and Summary of Essential Changes

In general, we found these documents to be excellent examples of how an industry group can (and should) provide coherent and well structured guidance on cybersecurity. We commend NERC’s drafting team and review process; it has resulted in a quality set of documents that should be widely used.

At the same time, and in fact because of the expected wide application of these

Regarding comment #2a, the exclusionary language concerning generation assets has been removed with the exception of nuclear generation which is excluded by the SAR. Because distribution assets are not considered part of the Bulk Electric System, these resources remain excluded as well.

Regarding comment #2b, much of the prescriptive language on how certain security measures should be applied has been removed. For example, the requirement for port scans in CIP 005, R4.2 has been replaced by a requirement to review only ports and services required for operations are enabled. In addition, the Drafting Team has removed most references to “how” security measures should be applied throughout the Standards unless it is required for compliance purposes.

Regarding comment #2c, language has been added to reflect the fact that some security solutions that are available today were not available when some legacy systems were designed and put into service. CIP-003, CIP- 004, CIP-005, and CIP-006 contain language addressing exceptions to their policies that may be required to deal with legacy systems and facilities where modern security solutions are not technically possible. In these cases, the Responsible Entities must identify and document the exception and describe the mitigating steps they are taking to secure the assets in lieu of the modern solution.

Regarding the comments #3, #4, and #5 related to scope, the Standard reflects the Standard Authorization Request which excluded distribution, nuclear generation, and telecommunication infrastructure. The Drafting Team cannot exceed the scope of the SAR.

A SAR reflects the industry consensus on the scope of any particular standard to be developed. Once SAR has been approved for standards drafting, the scope cannot be changed.

The NERC Reliability Standards process would require new SARs to address these scope issues.

documents, we believe that three general areas should be addressed before approval of these documents.

a) Broader scope - to address a larger % of generation resources and key distribution resources, and avoid excessive reliance on one boundary or layer of defense from cyber attacks. While we recognize the need to prioritize and prevent excessive requirements, we believe the current scope is overly restrictive, and excludes a significant portion of generation, and thereby significant vulnerabilities, in some areas. This is addressed in our specific comments on CIP-002-1, (and also CIP-003-1 through 009-1), which follow.
b) Additional cautions and guidance for control systems - in the form of specific requirements and references to key industry documents, to assure that the measures applied do not result in systems failures and reduced reliability instead of reduced risk. These cautions and guidance are necessary to address the special considerations needed when applying many normal security practices to control systems and control system networks -- particularly the bulk of legacy systems in operation today. Many do not have any ability to provide most of the required security features, and can be adversely affected by the application of other requirements. One good example is the requirement to do port scans (CIP 005-1, R4.2). Many legacy control networks are halted by port scans. The standard should include this caution, and suggest the use of alternatives to identify open ports on operational systems which have not been specifically designed and demonstrated to support this kind of testing without production failures. In general, more specific guidance on how to apply these requirements to the many legacy systems in use today should be provided.
c) Mandatory additional protection for inadequate legacy systems -- The phrase "where technically feasible" is used in a number of locations throughout the document. In many of these cases, alternatives are required. However, in others, no alternatives are required. Clearly stated requirements to add protection or barriers to cyber attack ("mitigation measures"), where they cannot be configured or incorporated into existing systems, should be added. It is not acceptable, in our view, to identify unacceptable risks, and then leave them because the existing equipment cannot be appropriately hardened. Appropriate countermeasures, to reduce risks to acceptable levels, should be required in all cases.

Addressing these concerns does not mean significant revision to this set of standards, or significant delay, in our opinion. It can be done effectively with minor changes and references in the generic text and in several specific locations. We suggest some of the specifics below. We believe these considerations are important to prevent the standards from being counterproductive or missing significant vulnerabilities.

3. Scope - Distribution assets that could have cyber impacts on transmission assets are excluded. All distribution assets that could have cyber impacts on Bulk Electric system assets should be included, to meet the objectives of the Standards. This comment also applies to the identical sections of the remaining standards (CIP-003 -- CIP-009).

4. Scope - Exclusion 3.2.1 should be removed; it excludes some of the larger generators that would otherwise be included under R1.1.4, and the NRC's requirements should be coordinated with, not independent of these requirements. This comment also applies to the identical sections of the remaining standards, (Section 4.2.1 of CIP-003 -- CIP-009).

5. Scope - Exclusion 3.2.2 should be removed; even when those communications systems are provided by others, the defined entities are still ultimately responsible for their proper operation and security. This comment also applies to the identical sections of the remaining standards, (Section 4.2.2 of CIP-003 -- CIP-009).

009-R1

009-R2

009-R3

009-R4

009-R5

009-M1

009-M2

009-M3

009-M4

009-M5

009-C1,1

009-C1,2

009-C1,3

009-C1,4

009-C2,1

009-C2,2

009-C2,3

009-C2,4

CIP-009 Drafting Team Responses to Comments

Name	Laurent Webber	
Entity	Western Area Power Administration	
Ready to Ballot:	No	
General Comments		
009-R1		
009-R2		
009-R3	Change the phrase "within ninety calendar days of the change" to "annually." Annual updates are adequate.	This requirement refers to the allowable period of time to notify personnel of changes to the recovery plan. The recovery plan is required to be reviewed and tested annually.
009-R4		
009-R5	This requirement should only apply to critical restoration information for critical cyber assets. Sample wording could be, "Information crucial to the restoration of Critical Cyber Assets and stored on computer media for a prolonged period of time..."	Requirement has been changed to read "Information essential to recovery that is stored on backup media shall be tested at least annually to ensure that the information is available."
009-M1		
009-M2		
009-M3		
009-M4		
009-M5		
009-C1,1		
009-C1,2		
009-C1,3	Data Retention 1.3.1: In keeping with the other CIPs, the retention requirement for the Responsible Entity should be only one year.	Data retention period has been changed.
009-C1,4		
009-C2,1		
009-C2,2		
009-C2,3	Compliance 2.3.2: Records of reviews and updates should only be retained for one year. Change "three" to "one".	2.3.2 has been removed.
009-C2,4		

CIP-009 Drafting Team Responses to Comments

Name	Michal Zeithammel
Entity	Brascan Power
Ready to Ballot:	Yes
General Comments	
009-R1	
009-R2	
009-R3	
009-R4	
009-R5	
009-M1	
009-M2	
009-M3	
009-M4	
009-M5	
009-C1,1	
009-C1,2	
009-C1,3	
009-C1,4	
009-C2,1	
009-C2,2	
009-C2,3	
009-C2,4	

CIP-009 Drafting Team Responses to Comments

Name	Guy Zito
Entity	NPCC
Ready to Ballot:	Yes
General Comments	
009-R1	
009-R2	
009-R3	
009-R4	
009-R5	
009-M1	
009-M2	
009-M3	
009-M4	
009-M5	
009-C1,1	
009-C1,2	
009-C1,3	
009-C1,4	
009-C2,1	
009-C2,2	
009-C2,3	
009-C2,4	

Drafting Team Responses to Comments on the Implementation Plan for CIP-002-1 through CIP-009-1

Raymond A'Brial

Central Hudson Gas & Electric Corp

Agree: No

Comments:	For Tables 1, 2 and 3, many requirements depend on historical retention for one year. The AC dates for those requirements should allow for the beginning of historical retention. Consequently, those AC dates should be pushed out. Budgets would be approved in 2006. Software would be written in 2007. Historical retention begins in 2008. First reporting against historical retention in 2009.	A new category has been added to the Implementation Plan -- "Compliant." Compliant means the entity meets the full intent of the requirements and is beginning to maintain the required “data,” “documents,” “documentation,” “logs,” and “records," necessary to become Auditably Compliant.
	For Table 2, there is concern with compliance for substations. Therefore it is recommended the substantial compliance for substations be phased in over two years. The first year would expect 50% of substations to be substantially compliant. The second year would expect 100% of substations to be substantially compliant.	The revised Implementation Plan calls for Responsible Entities to Begin Work and start implementing the requirements by the end of the second quarter, 2007 and be Auditably Compliant by the end of the second quarter, 2010.
	For Table 3, if someone registers January 1, 2006 then the last column will be January 1, 2009. The last column in Table 2 is December 31, 2009. If the registration is in 2006, then these dates should be pushed out or Table 2 applies.	The dates have been adjusted.

Ori Artman

Teltone

Agree: Yes

Comments: Of the three compliance definitions BW and AC are clear.
SC - the scope or quantity is not clear. How about specifying that the amount of work completed be in ratio to the time left in 10% increments? Example:
10 month between BW and AC. The date now is 4 months prior to AC, the utility should have 60% +/-10% of equipment installed, personnel trained etc...

Substantially Compliant calls for Responsible Entities to be “well along” in their implementation, as gauged using their own reasonable business judgment.

Steve Badgett

Riverside Public Utilitities

Agree: Yes

Comments:

Terry Baker

Platte River Power Authority

Agree: Yes

Comments:

Terry Bilke

Midwest ISO

Agree: No

Comments:

Pat Bourassa

Wisconsin Public Service Corporation

Agree: No

Comments: Depending on the requirements for DCS equipment, auditable compliance may not be attainable.

Please see FAQs on technical feasibility and reasonable business judgment.

Laurence W. Brown

Edison Electric Institute

Agree:	No	
Comments:	Table 3 still reflects "Registration," which could result in implementation even earlier than unter Tables 1 or 2. The word should be expanded or defined to clarify that it means registration following some period after the date the Standards become effective.	Revised to "Upon Registration," which is expected to be after the effective date of these standards.

Peter Burke

American Transmission Company

Agree: No

Comments: American Transmission Company concurs with the comments submitted separately by the Edison Electric Institute.

Marc Butts

Southern Company

Agree: No

Comments: The implementation time may not be sufficient. This will ultimately depend on the risk assessment in CIP-002. In 'Group 3', if Generator Owner/Operator registration occurs in 2005 as is likely to happen, then Registration +36 months requires this group (which should have the longest implementation time) to be compliant ahead of Group 2 (4Q2008 vs 2Q2009).

The Implementation Plan has been revised.

Gary Campbell

MAIN

Agree: Yes

Comments:

Linda Campbell

FRCC

Agree: No

Comments: We thank the drafting committee for recognizing the complexity and cost associated with coming into compliance with the requirements of this standard. We strongly support an implementation plan that provides a phased approach to compliance. Any more aggressive plan would make it extremely difficult to meeting the objectives of these standards.

In a NERC conference call, it was stated that the entity to which the tables apply is the functional entity. So that if a company is registered under multiple functional entities, our assumption is that not all functional areas of the company must implement the standards at the same time. Ergo Table 1 applies to critical cyber assets used by the Energy Control Center (balancing authority and transmission operator who were required to self-certify under std 1200). The Generating Plants function (Generation Owners), once they register, would use Table 3 and the Transmission Provider (sic) function within same company would use Table 2. If that is correct, can you clarify that in the Implementation Plan wording?

Transmission Provider is not a term used in the currently posted Functional Model. Should this say Transmission Service Provider?

Please clarify what it means to be in Substantial compliance (SC). In an EEI conference call, it was stated that you should have all procedures in place to be in SC. If you have only “begun to implement something” as the definition suggests or are even in-progress of implementing in second quarter of 2006, you cannot have data from the previous the full calendar year in 2nd quarter of 2007 to be Auditably Compliant (AC) by then. With the exception of those few requirements where you are SC for two years before being AC, SC would seem to mean that you are compliant with the exception of having a full calendar year of documentation.

Table 1
As the implementation plan currently reads, in order to be Auditably Compliant (AC) in 2nd quarter of 2007, you must have documentation/records for all of 2006. For System Control Centers this implementation plan requires that you have many procedures and documents in place by the end of 2005. There are numerous new requirements in this standard as compared to the Urgent Action Standard. If this standard is not approved until November 2005, it would be difficult to get all new procedures in place by year end in order to be AC by 2nd quarter of 2007. We request that the drafting committee reassess the timeframe from compliance to all new requirements included in CIP-002 through CIP-009.

CIP007-1 Systems Security Management; requirement for the control center goes from BW in 2nd qtr 2006 to AC in 2nd Qtr 2007; shouldn’t that be SC in 2nd quarter, 2007?
Table 2

The Implementation Plan has been clarified.

The term has been corrected.

Substantially Compliant calls for Responsible Entities to be “well along,” in their implementation, as gauged using their own reasonable business judgment. A new category, " Compliant" has been added, which means the Responsible Entity meets the full intent of the requirements and is beginning to maintain the required “data,” “documents,” “documentation,” “logs,” and “records" necessary to become Auditably Compliant.

The Implementation Plan has been revised to reflect the expected effective date of the standards.

Table 1: The Implementation Plan has been changed.

Table 2: The Implementation Plan has been changed and those inconsistencies removed.

The first column in Table 3 has been changed to "Upon Registration." The description of Begin Work has been clarified.

What does “Dec 31, 2009 & beyond” mean?
Table 2 includes Transmission Providers. According to the NERC website, this entity hasn’t been identified as registered yet. From the NERC site:
Although the NERC standards identify numerous entities, NERC has only identified six categories of entities at this time:

§ Balancing authorities
§ Planning authorities
§ Regional reliability organizations
§ Reliability coordinators
§ Transmission operators
§ Transmission planners

Therefore, it would seem more appropriate to include Transmission Service Providers in Table 3.

Several requirements (CIP-008 R1 & R2, CIP-009 R1 and R3, R4, R5) must be in Auditable Compliance by 2nd qtr 2007. This requires Substantial Compliance by 2nd qtr 2006 in order to meet retention requirements. But the requirements show Begin Work for that date. Since Transmission Service Providers are not yet registered, this seems quite unreasonable.

CIP002-1 requirements don’t need to be fully completed until 2nd quarter 2008 in order to be in auditable compliance by Dec 31, 2009 & beyond, but several other requirements must be in auditable compliant before this. It seems inconsistent to require auditable compliance for procedures and actions on your assets before the lists of critical assets and critical cyber assets are in auditable compliant.

Table 3
It would appear that you must have a compliance plan (BW) at the time you register as any of the functional entities listed for Table Three. Is this reasonable?

Roger Champagne

Hydro-Québec TransÉnergie

Agree: No

Comments: For Tables 1, 2 and 3, many requirements depend on historical retention for one year. The AC dates for those requirements should allow for the beginning of historical retention. Consequently, those AC dates should be pushed out. Budgets would be approved in 2006. Software would be written in 2007. Historical retention begins in 2008. First reporting against historical retention in 2009.

For Table 2, there is concern with compliance for substations. Therefore it is recommended the substantial compliance for substations be phased in over two years. The first year would expect 50% of substations to be substantially compliant. The second year would expect 100% of substations to be substantially compliant.

For Table 3, if someone registers January 1, 2006 then the last column will be January 1, 2009. The last column in Table 2 is December 31, 2009. If the registration is in 2006, then these dates should be pushed out or Table 2 applies.

Please see responses to Ray A'Brial, Central Hudson Gas & Electric Corp.

Larry Conrad

ECAR Critical Infrastructure Protection Panel

Agree: Yes

Comments:

Larry Conrad

Cinergy

Agree:	No	
Comments:	Table #1 states that “Other Facilities” must be audibly compliant with all Security Management Controls (CIP 003) by 2nd quarter of 2008. However, Table #1 also states that the deadline for “Other Facilities” to be audibly compliant with Systems Security Management (CIP 007) requirements is 2nd quarter of 2009. We recommend that the implementation plan be reviewed and similar items, such as security management, should be implemented on a similar timetable.	The Implementation Plan has been changed.
	From Table 3, for Generator Operators/Owners, the implementation schedule begins upon an entity's registration to a Functional Model function. What does this mean? When do we register to the functional model? What is involved with registering to the functional model? Need more specifics on Table #3.	The description of "Begin Work" has been clarified. More information about the Functional Model and registration is available from NERC’s Compliance Enforcement office.
	Need more specifics on how the functional model relates to the various tables. For example, if an entity is both a Balancing Authority and a Generation Owner, will there be multiple certification dates that they must adhere to?	Clarified.

Theodore Creedon, P.E.

Creedon Engineering

Agree: Yes

Comments: It is expected that some systems will be made less reliable in the short term because of the technical difficulty required. SKills are not readily available. However, this will be a learning experience.

Industry consensus is that skilled people are available to plan and implement the requirements of these standards without compromising reliability.

Joel De Granda

Florida Power and Light

Agree: Yes

Comments:

Richard Engelbrecht

RGE

Agree: No

Comments: For Tables 1, 2 and 3, many requirements depend on historical retention for one year. The AC dates for those requirements should allow for the beginning of historical retention. Consequently, those AC dates should be pushed out. Budgets would be approved in 2006. Software would be written in 2007. Historical retention begins in 2008. First reporting against historical retention in 2009. Also these dates are based upon approval of the standard by the fall of 2005. If there are substantive changes or approval is delayed these dates may require further adjustment.

For Table 2, there is concern with compliance for substations. Therefore it is recommended the substantial compliance for substations be phased in over two years. The first year would expect 50% of substations to be substantially compliant. The second year would expect 100% of substations to be substantially compliant.

For Table 3, if someone registers January 1, 2006 then the last column will be January 1, 2009. The last column in Table 2 is December 31, 2009. If the registration is in 2006, then these dates should be pushed out or Table 2 applies.

Please see responses to Ray A'Brial, Central Hudson Gas & Electric Corp.

Ken Fell

New York ISO

Agree: No

Comments: For Tables 1, 2 and 3, many requirements depend on historical retention for one year. The AC dates for those requirements should allow for the beginning of historical retention. Consequently, those AC dates should be pushed out. Budgets would be approved in 2006. Software would be written in 2007. Historical retention begins in 2008. First reporting against historical retention in 2009.

For Table 2, there is concern with compliance for substations. Therefore it is recommended the substantial compliance for substations be phased in over two years. The first year would expect 50% of substations to be substantially compliant. The second year would expect 100% of substations to be substantially compliant.

For Table 3, if someone registers January 1, 2006 then the last column will be January 1, 2009. The last column in Table 2 is December 31, 2009. If the registration is in 2006, then these dates should be pushed out or Table 2 applies.

Please see responses to Ray A'Brial, Central Hudson Gas & Electric Corp.

Francis Flynn

National Grid USA

Agree: No

Comments: For Tables 1, 2 and 3, many requirements depend on historical retention for one year. The AC dates for those requirements should allow for the beginning of historical retention. Consequently, those AC dates should be pushed out. Budgets would be approved in 2006. Software would be written in 2007. Historical retention begins in 2008. First reporting against historical retention in 2009.

For Table 2, there is concern with compliance for substations. Therefore it is recommended the substantial compliance for substations be phased in over two years. The first year would expect 50% of substations to be substantially compliant should they be classified as critcal with critical cyber assets. The second year would expect 100% of substations to be substantially compliant should they be classified as critcal with critical cyber assets..

For Table 3, if someone registers January 1, 2006 then the last column will be January 1, 2009. The last column in Table 2 is December 31, 2009. If the registration is in 2006, then these dates should be pushed out or Table 2 applies.

Please see responses to Ray A'Brial, Central Hudson Gas & Electric Corp.

Greg Fraser

Manitoba Hydro

Agree:	No	
Comments:	Suggest a paragraph in the Implementation Plan suggesting how a Responsible Entity should comply with the cyber security standards for a new Critical Asset or new Critical Cyber Asset. For example, must the Responsible Entity comply prior to the asset goes into production, could a mitigation plan be tabled or could Table 3 be applied.	Responsible Entities' new assets are expected to be compliant per the schedule. See FAQs on reasonable business judgment.

Jerry Freese

American Electric Power

Agree: No

Comments: Based on the expanded scope set forth in CIP-002 R1 for the Critical Assets and the subsequently expanded scope of the Critical Cyber Assets and the Electronic Security Perimeter, it would be impractical and infeasible to meet the obligations set forth in this requirement within the time alloted in Implementation Plan.

CIP-002 R1 has been revised.

Edwin C. Goff III

Progress Energy

Agree: No

Comments: Page 3 of 7, R8 -- It appears that System Control Centers must move from "BW" compliance in 2nd Qtr 2006 to a "AC" compliance by 2nd Qtr 2007. Should the 2nd Qtr 2007 entry by "SC" instead of "AC" ?

There are several areas where the plan calls for going from BW to AC. We thought that the flow should go from BW to SC to AC to achieve a graduated approach to achieving full AC..

The Implementation Plan has been changed.

Kenneth Goldsmith

Alliant Energy

Agree: Yes

Comments:

Kathleen Goodman

ISO New England Inc

Agree: No

Comments: For Tables 1, 2 and 3, many requirements depend on historical retention for one year. The AC dates for those requirements should allow for the beginning of historical retention. Consequently, those AC dates should be pushed out. Budgets would be approved in 2006. Software would be written in 2007. Historical retention begins in 2008. First reporting against historical retention in 2009.

For Table 2, there is concern with compliance for substations. Therefore it is recommended the substantial compliance for substations be phased in over two years. The first year would expect 50% of substations to be substantially compliant. The second year would expect 100% of substations to be substantially compliant.

For Table 3, if someone registers January 1, 2006 then the last column will be January 1, 2009. The last column in Table 2 is December 31, 2009. If the registration is in 2006, then these dates should be pushed out or Table 2 applies.

Please see responses to Ray A'Brial, Central Hudson Gas & Electric Corp.

Tim Hattaway

Alabama Electric Cooperative

Agree: No

Comments:

Jerry Heeren

MEAG Power

Agree: Yes

Comments:

Peter Henderson

Independent Electricity System Operator
(IESO)

Agree: No

Comments: Since the standard will not become official before October 1, 2005, it is unrealistic to expect an acceptable level of auditable compliance in 2007 for the following reasons:

1. NERC CIP-002 through CIP-009 establish requirements which are new and/or requirements of broader scope or much greater detail than those of NERC 1200 (See attached table). A significant amount of work will be needed to come into compliance with these new/extended requirements, even for Responsible Entities that are currently compliant with NERC 1200.

2. Most, if not all, Responsible Entities will require significant expenditure to perform the work needed to come into compliance.

3. It is unreasonable to expect that Entities will have budgetted on the basis of standards which are still in flux, the approval of which is not a given. Some Entities may feel that approving funds to satisfy a standard which is not yet approved is unacceptably speculative, bordering on the imprudent.

4. The implementation plan should recognize typical corporate fiscal planning processes. Most Entities are already well into their business planning/budgeting cycle for establishing budgets for 2006. Many, if not most, entities will have finalized their their budgets for 2006 well before this set of Standards is ratified by the NERC Board of Trustees.

5. Even if budgets are approved for 2006 for provisions to come into compliance with the as yet un-approved standards, the scope of CIP-002 through CIP-009 is so much greater than the scope of NERC 1200 that completing the work needed to come into full compliance could take more than a year to complete.

6.We suggest that the earliest date at which Responsible Entities should be required to have processes and technology in place to come into Auditable Compliance should be Q2 2008. This is based on an assumption that the Standards will be approved in October, 2005 and the comment appearing below (#8) is adopted. Should the approval date slip beyond October 2005, the date for Auditable Compliance should be deferred correspondingly.

7. The draft Implementation Plan specifies the year in which entities must be "Auditably Compliant". In the WEBEX conference call of June 1, clarification was sought as to whether this means that entities must have the processes and provisions required to meet the Standards first in place no later than that date, or whether entities must also have at that time the historical records required to withstand a full audit. It was clarified that where the Implementation Plan specifies "Auditable

The Implementation Plan has been revised and these concerns have been addressed.

Compliance" in year "X", the Responsible Entity is expected to be able to produce the historical records required by the Standards at that time. In effect, because some Standards require up to one year's worth of historical records be kept, this means that the Responsible Entity needs to have the processes and provisions needed to meet the Standards' requirements in place up to one year earlier than the date of the first audit.

For instance, an entity which has to be "Auditably Compliant" to CIP-006 R7 in the second quarter of 2007 would have to have provisions in place to begin fulfilling that requirement in the second quarter of 2006. An entity which must be auditably compliant with CIP-008 R2 in 2007 must, in fact, have begun collecting the required records in 2004. Both of these requirements are unreasonable.

In keeping with the comment above, the first date Responsible Entities should be required to have processes and technology in place to meet the standards should be no sooner than Q2-2008. The earliest date for auditable compliance should be Q2-2009.

8. Alternatively, the wording of the standards or of the implementation plan should contemplate that entities may legitimately not have historical records to submit until some time after they are required to come into Auditable Compliance. It is suggested that the pre-amble to the compliance sections of each standard could include text which makes it clear that Responsible Entities which retain necessary documentation from the date that the Standards first come into force will be deemed to be in compliance with requirements to maintain historical records. If this approach is adopted, the earliest date for auditable compliance should be Q2 2008 consistent with the comment above.

The following requirements are either new or substantially greater in scope than those appearing in NERC 1200:

Standard	Requirement Number
CIP-002	R1
CIP-003	R4
	R5
	R6
CIP-005	R1.1
	R1.2
	R1.3
	R1.4
	R1.5
	R2.3
	R2.4
	R2.5

R3.1
R3.3

CIP-006 R1
R1.4
R7

CIP-007 R1
R6.1
R6.2
R6.3
R7
R8

E. Nick Henery

SMUD

Agree: No

Comments: The Drafting Team will need to go through the Standard and assign responsibility to each function from the functional model like the Version 0 STD. For this Standard to be enforceable the generic use of Responsible Entity is the same as the generic use of Control Area. Even if the Standard lists the different functions it leaves open the possibility of misinterpretation as to which function is truly responsible.

The Responsible Entities are clearly enumerated in the standard Section A, item 4.

Jack Hobbick

Consumers Energy

Agree: Yes

Comments:

Richard Kafka

Pepco Holdings, Inc.

Agree: No

Comments:	As Table 3 is open ended (i.e. tied to Registration requirements) is was possible for Table 3 entities to have to be compliant earlier than Table 1 & 2 entities. I do not believe this is the intent. Please clarify (e.g. Registration follows some period after the date the Standard become effective).	The Implementation Plan has been revised.

Tony Kroskey

Brazos Electric Power Cooperative

Agree: Yes

Comments: Compliance schedule dates should be clarified to state whether an entity is expected to be in compliance by the end of the quarter or the beginning of the quarter.

The Implementation Plan has been clarified to show the end of the quarter.

Carol Krysevig

Allegheny Energy Supply Co. LLC

Agree:	No	
Comments:	Table 3 still reflects "Registration," which could result in implementation even earlier than under Tables 1 or 2. Clarify the intent of registration following some period after the date the Standards become effective.	The table has been clarified to "Upon registration," which is expected to be after the effective date of these standards.

John Lim

Con Edison

Agree: No

Comments: For Tables 1, 2 and 3, many requirements depend on historical retention for one year. The AC dates for those requirements should allow for the beginning of historical retention. Consequently, those AC dates should be pushed out. Budgets would be approved in 2006. Software would be written in 2007. Historical retention begins in 2008. First reporting against historical retention in 2009.

For Table 2, there is concern with compliance for substations. Therefore it is recommended the substantial compliance for substations be phased in over two years. The first year would expect 50% of substations to be substantially compliant. The second year would expect 100% of substations to be substantially compliant.

For Table 3, if someone registers January 1, 2006 then the last column will be January 1, 2009. The last column in Table 2 is December 31, 2009. If the registration is in 2006, then these dates should be pushed out or Table 2 applies.

Please see responses to Ray A'Brial, Central Hudson Gas & Electric Corp.

Deborah Linke

Bureau of Reclamation

Agree: Yes

Comments:

Greg Mason

Dynegy Generation

Agree: Yes

Comments:

Paul McClay

Tampa Electric

Agree: No

Comments: We thank the drafting committee for recognizing the complexity and cost associated with coming into compliance with the requirements of this standard. We strongly support an implementation plan that provides a phased approach to compliance. Any more aggressive plan would make it extremely difficult to meet the objectives of these standards.

In a NERC conference call, it was stated that the entity to which the tables apply is the functional entity. So that if a company is registered under multiple functional entities, our assumption is that not all functional areas of the company must implement the standards at the same time. Ergo Table 1 applies to critical cyber assets used by the Energy Control Center (balancing authority and transmission operator who were required to self-certify under std 1200). The Generating Plants function (Generation Owners), once they register, would use Table 3 and the Transmission Provider (sic) function within same company would use Table 2. If that is correct, can you clarify that in the Implementation Plan wording?

Transmission Provider is not a term used in the currently posted Functional Model. Should this say Transmission Service Provider?

Please clarify what it means to be in Substantial compliance (SC). In an EEI conference call, it was stated that you should have all procedures in place to be in SC. If you have only “begun to implement something” as the definition suggests or are even in-progress of implementing in second quarter of 2006, you cannot have data from the previous full calendar year in 2nd quarter of 2007 to be Auditably Compliant (AC) by then. With the exception of those few requirements where you are SC for two years before being AC, SC would seem to mean that you are compliant with the exception of having a full calendar year of documentation.

Table 1
As the implementation plan currently reads, in order to be Auditably Compliant (AC) in 2nd quarter of 2007, you must have documentation/records for all of 2006. For System Control Centers this implementation plan requires that you have many procedures and documents in place by the end of 2005. There are numerous new requirements in this standard as compared to the Urgent Action Standard. If this standard is not approved until November 2005, it would be difficult to get all new procedures in place by year end in order to be AC by 2nd quarter of 2007. We request that the drafting committee reassess the timeframe from compliance to all new requirements included in CIP-002 through CIP-009 and change AC to 4th qtr 2007.

CIP007-1 Systems Security Management; requirement for the control center goes from BW in 2nd qtr 2006 to AC in 2nd Qtr 2007; suggest changing to SC in 2nd quarter, 2007.

Please see responses to Linda Campbell, FRCC.

Table 2
What does “Dec 31, 2009 & beyond” mean?
Table 2 includes Transmission Providers (assuming this means Transmission Service Provider). According to the NERC website, this entity hasn’t been identified as registered yet. From the NERC site:
Although the NERC standards identify numerous entities, NERC has only identified six categories of entities at this time:
? Balancing authorities
? Planning authorities
? Regional reliability organizations
? Reliability coordinators
? Transmission operators
? Transmission planners

Therefore, it would seem more appropriate to include Transmission Service Providers in Table 3.

Several requirements (CIP-008 R1 & R2, CIP-009 R1 and R3, R4, R5) must be in Auditable Compliance by 2nd qtr 2007. This requires Substantial Compliance by 2nd qtr 2006 in order to meet document retention requirements. But the requirements show Begin Work for that date. Since Transmission Service Providers are not yet registered, this seems quite unreasonable. Suggest auditable compliance be moved to 2nd qtr 2008.

CIP002-1 requirements don’t need to be fully completed until 2nd quarter 2008 in order to be in auditable compliance by Dec 31, 2009 & beyond, but several other requirements (CIP-003 R3, R4, R5. R6; CIP-004 R4; and CIP009 R2) must be in auditable compliance before this. It seems inconsistent to require auditable compliance for procedures and actions on your assets before the lists of critical assets and critical cyber assets are in auditable compliance.

Table 3
It would appear that you must have a compliance plan (BW) at the time you register as any of the functional entities listed for Table Three. Is this reasonable? It does not appear there is a schedule for registration at this time, but if anytime soon, this is not realistic. Is there any incentive or penalty for registering or not? This could be a dis-incentive to register.

CIP-009-1 requires auditable compliance by registration + 12 months. The subject of CIP-009-1 is recovery plans for those Critical Cyber Assets that are defined in standard CIP-002-1. However, CIP-002-1 is not in auditable compliance until registration + 24 months. This seems inconsistent.

David McCoy

Great Plains Energy/Kansas City Power & Light

Agree: Yes

Comments:

Don Miller

First Energy Corp

Agree: Yes

Comments:

Patrick Miller

PacifiCorp

Agree: Yes

Comments:

Jeff Mitchell

ECAR

Agree:	Yes	
Comments:	The above comments are related to CIP-002-1 R-1 only to remove IROL languave from the standard.	CIP-002 has been revised.

Scott Mix

KEMA, Inc

Agree: Yes

Comments:

Darrick Moe

WAPA

Agree: Yes

Comments:

Selby Mohr

Sacramento Municipal Utility District

Agree: Yes

Comments:

Kurt Muehlbauer

Exelon

Agree: No

Comments: We agree with the comments from PJM.
Since the standard will not become official before October 1, 2005, it is unrealistic to expect an acceptable level of auditable compliance in 2007 for the following reasons:
- NERC CIP-002 through CIP-009 establish requirements which are new and/or requirements of broader scope or much greater detail than those of NERC 1200 (See attached table). A significant amount of work will be needed to come into compliance with these new/extended requirements, even for Responsible Entities that are currently compliant with NERC 1200.
- Most, if not all, Responsible Entities will require significant expenditure to perform the work needed to come into compliance.
- The implementation plan should recognize typical corporate fiscal planning processes.
- Most Entities are already well into their business planning/budgeting cycle for establishing budgets for 2006. Many, if not most, entities will have finalized their their budgets for 2006 well before this set of Standards is ratified by the NERC Board of Trustees.
- It is unreasonable to expect that Entities will have budgetted on the basis of standards which are still in flux, the approval of which is not a given. Some Entities may feel that approving funds to satisfy a standard which is not yet approved is unacceptably speculative, bordering on the imprudent.
- Even if budgets are approved for 2006 for provisions to come into compliance with the as yet un-approved standards, the scope of CIP-002 through CIP-009 is so much greater than the scope of NERC 1200 that completing the work needed to come into full compliance could take more than a year to complete.
- We suggest that the earliest date at which Responsible Entities should be required to come into Auditable Compliance should be Q2 2008. This is based on an assumption that the Standards will be approved in October, 2005. Should the approval date slip beyond October 2005, the date for Auditable Compliance should be deferred correspondingly.

The Implementation Plan has been revised and these concerns have been addressed.

Jeffrey Mueller

PSEG Companies

Agree:	No	
Comments:	The PSEG Companies have reviewed and share the concerns expressed in the Comments of PJM and EEI. Accordingly, the PSEG Companies support the comments of PJM and EEI, and request that the concerns expressed in those comments be properly addressed in the next version of the draft standard.	Please see responses to Laurence W. Brown, Edison Electric Institute.

Mitchell Needham

Tennessee Valley Authority

Agree: No

Comments: More time is needed to assess the time requirement.

The Implementation Plan has been revised.

Dave Norton

Entergy Transmission

Agree: Yes

Comments: There is never enough time or money - more leeway is better. However, UA 1200 has been established and accepted as our necessary baseline capability for cyber security, and while its been fully in-force for nearly two years we do not yet approach ubiquitous compliance as an industry. The CIP-002/009 Implementation Plan's Table 1 timeline for earliest "auditable compliance" is year-end 2006 ("2ndQtr""2007) - and by and large this applies only for the data center Critical Cyber Assets of those Responsible Entities for whom the UA 1200 has been incumbent over the past two years. Accordingly, the CIP-002/009 Implementation Plan has significant leeway already built-in... If the risk is real, it calls for reasonably near-term compliance dates to foster diligence. This Implementation Plan appears to be a good mix of needed leeway and necessary diligence.

Doug Orlofske

Wisconsin Public Power Inc

Agree: Yes

Comments:

Kevin Perry

Southwest Power Pool

Agree: No

Comments: With the earliest expected approval and adoption of the CIP-002 through CIP-009 standards not occuring until the end of 2005 or, more likely, sometime in 2006, the entity's budget cycle has been long passed. Accordingly, it is unlikely that any requirement that necessitates the expenditure of capital funds or the hiring of additional staff can begin work until 2007. That impacts nearly all of the standards requirements.

Recognition must also be given to the fact that in some cases, compliant does not mean that a full set of documentation covering the prescribed number of retention years will be initially available.

The Implementation Plan has been revised and these issues addressed.

Tom Pruitt

Duke Power Company

Agree: Yes

Comments:

Duane Radzwion

Consumers Energy

Agree: No

Comments:

Howard Rulf

We Energies

Agree: Yes

Comments:

Randy Schimka

San Diego Gas and Electric Co.

Agree: No

Comments: The implementation plan doesn't make clear if the timetables discussed are the beginning or the end of the quarter (i.e 2nd quarter 2006).

The end of the quarter may give us enough time for some of the more difficult items, but if the definition is the beginning of the quarter then we will probably need more time.

We would suggest the end of the 3rd quarter for some of the more time-consuming items listed.

This has been clarified to the "end of the second quarter."

Lyman Shaffer

PG&E

Agree:	Yes	
Comments:	The implementaton plan seems to be reasonable as written. We assume that the time schedules will be adjusted if the issuance of the standard is delayed beyonf the propopsed fall, 2005 target date.	The Implenemtation Plan has been revised to reflect the change in expected effective date.

Neil Shockey

Southern California Edison

Agree: Yes

Comments:

William Smith

Allegheny Power

Agree: Yes

Comments:

Paul Sorenson

Open Access Technology International

Agree: Yes

Comments:

Robert Strauss

NYSEG

Agree: No

Comments: For Tables 1, 2 and 3, many requirements depend on historical retention for one year. The AC dates for those requirements should allow for the beginning of historical retention. Consequently, those AC dates should be pushed out. Budgets would be approved in 2006. Software would be written in 2007. Historical retention begins in 2008. First reporting against historical retention in 2009. Also these dates are based upon approval of the standard by the fall of 2005. If there are substantive changes or approval is delayed these dates may require further adjustment.

For Table 2, there is concern with compliance for substations. Therefore it is recommended the substantial compliance for substations be phased in over two years. The first year would expect 50% of substations to be substantially compliant. The second year would expect 100% of substations to be substantially compliant.

For Table 3, if someone registers January 1, 2006 then the last column will be January 1, 2009. The last column in Table 2 is December 31, 2009. If the registration is in 2006, then these dates should be pushed out or Table 2 applies.

Please see responses to Ray A'Brial, Central Hudson Gas & Electric Corp.

Karl Tammar

IRC

Agree: No

Comments: Since the standard will not become official before October 1, 2005, it is unrealistic to expect an acceptable level of auditable compliance in 2007 for the following reasons:

? NERC CIP-002 through CIP-009 establish requirements which are new and/or requirements of broader scope or much greater detail than those of NERC 1200 (See attached table). A significant amount of work will be needed to come into compliance with these new/extended requirements, even for Responsible Entities that are currently compliant with NERC 1200.

? Most, if not all, Responsible Entities will require significant expenditure to perform the work needed to come into compliance.

? The implementation plan should recognize typical corporate fiscal planning processes.

? Most Entities are already well into their business planning/budgeting cycle for establishing budgets for 2006. Many, if not most, entities will have finalized their their budgets for 2006 well before this set of Standards is ratified by the NERC Board of Trustees.

? It is unreasonable to expect that Entities will have budgetted on the basis of standards which are still in flux, the approval of which is not a given. Some Entities may feel that approving funds to satisfy a standard which is not yet approved is unacceptably speculative, bordering on the imprudent.

? Even if budgets are approved for 2006 for provisions to come into compliance with the as yet un-approved standards, the scope of CIP-002 through CIP-009 is so much greater than the scope of NERC 1200 that completing the work needed to come into full compliance could take more than a year to complete.

? We suggest that the earliest date at which Responsible Entities should be required to come into Auditable Compliance should be Q2 2008. This is based on an assumption that the Standards will be approved in October, 2005. Should the approval date slip beyond October 2005, the date for Auditable Compliance should be deferred correspondingly.

? The draft Implementation Plan specifies the year in which entities must be “Auditably Compliant”. In the WEBEX conference call of June 1, clarification was sought as to whether this means that entities must have the processes and provisions required to meet the Standards first in place no later than that date, or whether entities must also have at that time the historical records required to withstand a full audit. It was clarified that where the Implementation Plan specifies “Auditable Compliance” in year “X”, the Responsible Entity is expected to be able to produce the historical records required by the Standards at that time. In effect, because some Standards require up to one year’s worth of historical records be kept, this means that the Responsible Entity needs to have the processes and provisions in place needed to meet the Standards’ requirements up to one year earlier than the date specified in the Implementation Plan. This is unreasonable and should be revised.

For instance, an entity which must be “Auditably Compliant” to CIP-006 R7 in the

The Implementation Plan has been revised and these concerns have been addressed.

second quarter of 2007 must have provisions in place to begin fulfilling that requirement in the second quarter of 2006. An entity which must be auditably compliant with CIP-008 R2 in 2007 must, in fact, have begun collecting the required records in 2004.

The wording of the standards or of the implementation plan should contemplate that entities may legitimately not have historical records to submit until some time after they are required to come into Auditable Compliance. It is suggested that the pre-amble to the compliance sections of each standard could include text which makes it clear that Responsible Entities which retain necessary documentation from the date that the Standards first come into force will be deemed to be in compliance with requirements to maintain historical records.

The following requirements are either new or substantially greater in scope than those appearing in NERC 1200:

Standard	Requirement Number
CIP-002	R1
CIP-003	R4
	R5
	R6
CIP-005	R1.1
	R1.2
	R1.3
	R1.4
	R1.5
	R2.3
	R2.4
	R2.5
	R3.1
	R3.3
CIP-006	R1
	R1.4
	R7
CIP-007	R1
	R6.1
	R6.2
	R6.3
	R7
	R8
CIP-008	R1.1
	R1.2
	R1.5
CIP-009	R4

Todd Thompson

PJM Interconnection

Agree: No

Comments: Since the standard will not become official before October 1, 2005, it is unrealistic to expect an acceptable level of auditable compliance in 2007 for the following reasons:

- NERC CIP-002 through CIP-009 establish requirements which are new and/or requirements of broader scope or much greater detail than those of NERC 1200 (See attached table). A significant amount of work will be needed to come into compliance with these new/extended requirements, even for Responsible Entities that are currently compliant with NERC 1200.

- Most, if not all, Responsible Entities will require significant expenditure to perform the work needed to come into compliance.

- The implementation plan should recognize typical corporate fiscal planning processes.

- Most Entities are already well into their business planning/budgeting cycle for establishing budgets for 2006. Many, if not most, entities will have finalized their their budgets for 2006 well before this set of Standards is ratified by the NERC Board of Trustees.

- It is unreasonable to expect that Entities will have budgetted on the basis of standards which are still in flux, the approval of which is not a given. Some Entities may feel that approving funds to satisfy a standard which is not yet approved is unacceptably speculative, bordering on the imprudent.

- Even if budgets are approved for 2006 for provisions to come into compliance with the as yet un-approved standards, the scope of CIP-002 through CIP-009 is so much greater than the scope of NERC 1200 that completing the work needed to come into full compliance could take more than a year to complete.

- We suggest that the earliest date at which Responsible Entities should be required to come into Auditable Compliance should be Q2 2008. This is based on an assumption that the Standards will be approved in October, 2005. Should the approval date slip beyond October 2005, the date for Auditable Compliance should be deferred correspondingly.

- The draft Implementation Plan specifies the year in which entities must be “Auditably Compliant”. In the WEBEX conference call of June 1, clarification was sought as to whether this means that entities must have the processes and provisions required to meet the Standards first in place no later than that date, or whether entities must also have at that time the historical records required to withstand a full audit. It was clarified that where the Implementation Plan specifies “Auditable

The Implementation Plan has been revised and these concerns have been addressed.

Compliance" in year "X", the Responsible Entity is expected to be able to produce the historical records required by the Standards at that time. In effect, because some Standards require up to one year's worth of historical records be kept, this means that the Responsible Entity needs to have the processes and provisions in place needed to meet the Standards' requirements up to one year earlier than the date specified in the Implementation Plan. This is unreasonable and should be revised.

For instance, an entity which must be "Auditably Compliant" to CIP-006 R7 in the second quarter of 2007 must have provisions in place to begin fulfilling that requirement in the second quarter of 2006. An entity which must be auditably compliant with CIP-008 R2 in 2007 must, in fact, have begun collecting the required records in 2004.

The wording of the standards or of the implementation plan should contemplate that entities may legitimately not have historical records to submit until some time after they are required to come into Auditable Compliance. It is suggested that the pre-amble to the compliance sections of each standard could include text which makes it clear that Responsible Entities which retain necessary documentation from the date that the Standards first come into force will be deemed to be in compliance with requirements to maintain historical records.

The following requirements are either new or substantially greater in scope than those appearing in NERC 1200:

Standard	Requirement Number
CIP-002	R1
CIP-003	R4
	R5
	R6
CIP-005	R1.1
	R1.2
	R1.3
	R1.4
	R1.5
	R2.3
	R2.4
	R2.5
	R3.1
	R3.3
CIP-006	R1
	R1.4
	R7
CIP-007	R1
	R6.1
	R6.2
	R6.3

	R7
	R8
CIP-008	R1.1
	R1.2
	R1.5
CIP-009	R4

Steven Townsend

Consumers Energy Co.

Agree: Yes

Comments:

Martin Trence

Xcel Energy - Northen States Power (NSP)

Agree: No

Comments: Shift the timeline from beginning in 2nd Qtr 2006 to 2nd Qtr 2007 based on delayed schedule on acceptance and implementation of the 1300 standards.

The Implenemtation Plan has been revised to reflect the change in expected effective date.

Rick Vermeers

Avistacorp

Agree: Yes

Comments:

Robert C. Webb

Instrumentation, Systems and Automation Society

Agree: Yes

Comments:

Laurent Webber

Western Area Power Administration

Agree: Yes

Comments:

Michal Zeithammel

Brascan Power

Agree: No

Comments: Table 3 does not stipulate exactly what and especially when “Registration” is and therefore it is difficult to say if there is enough time for compliance.

Assuming that “Registration” is 1 November 2005, the implementation schedule for CIP-009-1 is too aggressive.

Upon registration of the Functional Model entity. More information about the Functional Model and registration is available from NERC’s Compliance Enforcement office.

Guy Zito

NPCC

Agree: No

Comments: For Tables 1, 2 and 3, many requirements depend on historical retention for one year. The AC dates for those requirements should allow for the beginning of historical retention. Consequently, those AC dates should be pushed out. Budgets would be approved in 2006. Software would be written in 2007. Historical retention begins in 2008. First reporting against historical retention in 2009.

For Table 2, there is concern with compliance for substations. Therefore it is recommended the substantial compliance for substations be phased in over two years. The first year would expect 50% of substations to be substantially compliant. The second year would expect 100% of substations to be substantially compliant.

For Table 3, if someone registers January 1, 2006 then the last column will be January 1, 2009. The last column in Table 2 is December 31, 2009. If the registration is in 2006, then these dates should be pushed out or Table 2 applies.

Please see responses to Ray A'Brial, Central Hudson Gas & Electric Corp.