

Consideration of Comments on Initial Ballot of CIP-002-2 to CIP-009-2 — Cyber Security Standards (Project 2008-06)

Summary Consideration:

Most (91.90%) of those who joined the ballot pool to participate in the balloting of the initial set of revisions to the CIP-002-2 through CIP-009-2 standards returned a ballot, and the initial ballot achieved a weighted affirmative vote of 84.06%. There were only 24 negative ballots submitted with a comment, and as can be seen on the following pages, several of these negative comments were submitted by multiple balloters from a single entity registered in multiple industry segments. There were also several comments submitted with affirmative ballots, primarily to provide the SDT with guidance on issues to address in the next phases of revisions to these standards. The major issues raised with affirmative and negative comments include the following:

1) Designation of a single Senior Manager, as required by CIP-003 Requirement R2, is considered to be overly prescriptive and cannot be supported by either the FERC Order 706 or previous SDT responses to similar industry review comments. Entities object to the standards prescribing their corporate governance. To a lesser extent, some entities would prefer to see the Senior Management requirement moved to CIP-002.

In response, the SDT believes the directive in the FERC order appropriately justifies the revision to the existing requirement. The requirement in the standard does not dictate the management structure of the Responsible Entity. The requirement is to identify a single point of accountability for the implementation and compliance with the CIP standards. The SDT envisions that the Senior Manager will seek the counsel of other Responsible Entity personnel in carrying out this responsibility and can delegate many of the required approvals.

As CIP-003 is the Governance standard and assignment of a Senior Manager is a governance issue, the SDT chose to leave the assignment in CIP-003 and to make CIP-003, Requirement R2 applicable to all Responsible Entities. To have attempted to make the change following the industry comments was deemed to be a significant modification that would have necessitated an additional round of industry comments prior to ballot. That would have resulted in the inability to complete the mandated time-specific modifications per the FERC Order 706. The SDT plans to revisit the placement of the requirement in a future revision to the standards.

2) Entities objected to the addition of "continuous" to CIP-006, Requirement R1.6 with respect to escorted access. Greatest concern is the perceived inability to enforce and audit compliance.

In response, the SDT believes the term "continuous" does not change the original intent or ability to audit. As used, "continuous" is analogous to "supervised" in that the escort is expected to be aware of the escorted visitor's actions at all times. In response to concerns raised regarding how to demonstrate compliance, the SDT offered that there are a number of references available that describe how an entity's visitor control program can be verified. One such reference is the [NIST SP 800-53A \(Guide for Assessing the Security Controls in Federal Information Systems\)](#), Control PE-7 (Visitor Control).

3) Entities commented that the Technical Feasibility Exception (TFE) process, as the alternative to “Reasonable Business Judgment” language, should not have been moved to the Compliance Monitoring and Evaluation Program (CMEP) in the NERC Rules of Procedure. Concerns include the need to define the TFE process in the standards themselves and the TFE stipulation that the standard must provide for feasibility or the TFE process will not allow the entity to seek relief. Concerns were also raised with the removal of the assertion in Section D 1.4.2 (Additional Compliance Information) that duly authorized exceptions would not result in non-compliance.

In response, the CIP SDT has no authority over the approval process for changes to the NERC Rules of Procedure, noting the industry has an opportunity to provide comments to the proposed TFE process prior to adoption by the NERC Board of Trustees and will likely have another opportunity to provide comments as part of the FERC approval process. The SDT recommends the industry take advantage of every opportunity to influence the ultimate TFE process. The SDT also believes an exception taken against the Responsible Entity’s compliance policy does not relieve the entity from compliance with the requirement of the standard and the SDT cannot assert that a properly approved exception to the Responsible Entity’s security policy will not result in non-compliance. The exception taken against a company policy is a separate issue from an exception against the requirement of the standard. A Responsible Entity may find it has to process both types of exceptions.

4) A number of modifications were made to the documentation update timeframe requirements, shortening the time from 90 to 30 days. Entities objected to the 30-day timeframe, commenting that the required 30-day timeframe is unrealistic to adequately document and communicate the related changes to all appropriate staff across a company.

In response, the SDT reduced the timeframe for certain documentation requirements to 30 days to conform to applicable directives in the FERC Order 706. For consistency throughout the standards, the SDT reduced the documentation update timeframe to 30 days for the remaining standards requirements that were not directly referenced in the FERC order. The SDT also clarified that the 30-day timeframe begins with the completion of the related change. The SDT believes the 30-day timeframe for updating documentation is appropriate and reasonable.

Version 2 of the CIP Cyber Security Standards (CIP-002 to CIP-009) includes the time-specific directives taken from FERC Order 706 which made a phased implementation approach to revising the standards necessary. The SDT has attempted to provide efficient and effective language to be compliant with the FERC directives while minimizing the impact on the first round of changes.

A number of comments against requirements that were not revised in Version 2 of the standards were deferred with a recommendation to resubmit the comment against Version 3 of the standard if still appropriate.

If you feel that your comment has been overlooked, please let us know immediately. Our goal is to give every comment serious consideration in this process! If you feel there has been an error or omission, you can contact the Vice President and Director of Standards, Gerry Adamski, at 609-452-8060 or at gerry.adamski@nerc.net. In addition, there is a NERC Reliability Standards Appeals Process.¹

¹ The appeals process is in the Reliability Standards Development Procedures: <http://www.nerc.com/standards/newstandardsprocess.html>.

Consideration of Comments on Initial Ballot — CIP-002-2 to CIP-009-2 — Cyber Security Standards (Project 2008-06)

Voter	Entity	Segment	Vote	Comment
Samuel Cabassa	Covanta Energy	5	Negative	It is not prudent to have the Senior Manager alone do all annual approvals.
Response	The requirement is to identify a single point of accountability for the implementation and compliance with the CIP standards. The SDT envisions that the Senior Manager will seek the counsel of other Responsible Entity personnel in carrying out this responsibility and can delegate many of the required approvals.			
Wayne Guttormson	SaskPower	1	Negative	<p>1) Saskatchewan will not adopt these standards as written. We have some serious concerns/questions about the process and end product. First, changes are being mandated by FERC not by Saskatchewan or other Canadian jurisdictions.</p> <p>2) Secondly, we question the prescriptive nature of most the CIP standards and the philosophy behind them. For example in CIP 002 responses to comments the SDT states that a senior manager is required to be held responsible in order to ensure that there is a clear line of authority and that cyber security functions are given the prominence they deserve. We do not find this argument to be convincing. If this really is the case why do we not use this approach on all of the other standards? Are not the IRO, TOP or EOP standards just as important as the CIP standards? Shouldn't they be given the prominence they deserve?</p>
Response	<p>1) The SDT understands the concerns regarding a US Government Agency attempting to impose standards upon non-jurisdictional Canadian entities. It may be impractical to have differing requirements for protecting the interconnected Bulk Electric System assets.</p> <p>2) The requirement for appointing a Senior Manager (CIP-003, Requirement R2) is to identify a single point of accountability for the implementation and compliance with the CIP standards. The SDT is aware of issues in the existing standards and is working hard to eliminate unnecessary prescription as the standards continue to be revised.</p>			
James R. Nickel	Michigan Public Power Agency	5	Affirmative	MPPA respectfully requests that in the next phase of this project, CIP-003-2 R2 be relocated and inserted as the first requirement of the CIP-002-2 Standard. This is a simple, seemingly non-controversial change which establishes a logical sequence of events and meets FERC's desire for clarity in the NERC process.
Response	As CIP-003 is the Governance standard and assignment of a Senior Manager is a governance issue, the SDT chose to leave the assignment in CIP-003 and to make CIP-003, Requirement R2 applicable to all Responsible Entities. To make the change following the industry comments was deemed to be a significant modification that would have necessitated an additional round of industry comment prior to ballot. That would have resulted in the inability to complete the mandated time-specific modifications per the FERC Order 706. The SDT recommends submitting this comment against Version 3 of the CIP standards if still appropriate.			

Consideration of Comments on Initial Ballot — CIP-002-2 to CIP-009-2 — Cyber Security Standards (Project 2008-06)

Voter	Entity	Segment	Vote	Comment
Gayle Mayo	Indiana Municipal Power Agency	4	Affirmative	Indiana Municipal Power Agency (IMPA) is voting affirmative on the CIP standards. In phase II of these standards, IMPA believes that CIP-003 R2 should be moved into CIP-002 R4 in order to clarify the reference to the senior manager. The stakeholders seem to support this improvement, and it should be a relatively simple task or goal for the Standard Drafting Team to perform during phase II.
Response	As CIP-003 is the Governance standard and assignment of a Senior Manager is a governance issue, the SDT chose to leave the assignment in CIP-003 and to make CIP-003, Requirement R2 applicable to all Responsible Entities. To have attempted to make the change following the industry comments was deemed to be a significant modification that would have necessitated an additional round of industry comment prior to ballot. That would have resulted in the inability to complete the mandated time-specific modifications per the FERC Order 706. The SDT recommends submitting this comment against Version 3 of the CIP standards if still appropriate.			
William SeDoris	Northern Indiana Public Service Co.	3	Affirmative	<p>Responses to Comments are inconsistent:</p> <p>1) Some of the SDT responses to comments provided more clarity than the language drafted within the standard. We believe the same level of clarity should be added to the standard to remove the need for entity interpretation whenever possible.</p> <p>2) An example of this can be seen in the response to the entities asking for clarification on audit data retention periods. The standard formerly held a three year retention period and in the drafting process the SDT removed this retention limit language. Numerous entities questioned the limit on record retention and the SDT responded that audit records would need to be retained until the completion of the next audit. This additional clarifying language should be added to the standard.</p> <p>3) Some of the SDT responses to comments provided additional language and interpretations of the modifications made that appear to be unclear in the standards. An example of this is the liability of the CIP designated Senior Manager. It appears that the intent of removing some of the language in the standard regarding entity responsibility was done to clean up the standard and remove redundancy; however some entities questioned if the SDT was placing the responsibility for compliance on the CIP Senior Manager. It is our understanding that the entity is ultimately responsible for compliance with the NERC CIP standard (as is the case with all NERC standards) and the intent of the CIP senior manager designation was for the purpose of a clearly defined individual with responsibility and authority within the entity. The language in the standard supports our belief; however the response to commenters from the SDT seems to go beyond the language in the standard in stating that the Senior Manager is responsible for compliance. If this is the intent of the SDT then the additional language needs to be included within the standard in order to allow for open comments to those modifications.</p>
Michael K Wilkerson	Northern Indiana Public Service Co.	5	Affirmative	
Joseph O'Brien	Northern Indiana Public Service Co.	6	Affirmative	

Consideration of Comments on Initial Ballot — CIP-002-2 to CIP-009-2 — Cyber Security Standards (Project 2008-06)

Voter	Entity	Segment	Vote	Comment
				<p>4) The drafting process All changes and modifications made by the SDT were not clearly identified in the red-lined version that was released for comment. This needs to be prevented from occurring in the future and if identified it needs to be corrected, not accepted and ignored. It may also be considered misleading to an entity to open the latest version of the redlined draft document and only see the modifications that were made from one draft version to the next. It is our belief that the latest red-lined document should identify the modifications made from the original version not just the modifications from the previous draft document.</p> <p>5) Additionally, comments were submitted in regards to the SDT following the ANSI process that all NERC standards are designed around. It is our belief that the ANSI process should also apply to the standards drafting process and any modifications to the ANSI approved standards format. As the SDT proceeds through the FERC directed changes and modifications are made to the standards, an entity needs to be able to comment on those modifications and receive feedback on the comments submitted.</p> <p>6) In a number of cases an entity raised a question or a comment on a modification made and the response from the SDT was to defer the question or comment to a later phase. In the NERC standards drafting process when a modification to a standard is proposed, an entity has the ability to comment on the modification when it was proposed. Responses to comments should be provided when the modification was made. If an entity wishes to comment or question language at a later phase the entity would need to file for a clarification. If a change is made through the standards drafting process, and a question or comment is raised by an entity it should not be an acceptable response for the SDT to defer a response to a later phase in the drafting process.</p> <p>7) The ballot process We would encourage the SDT to treat the CIP standards like all other NERC reliability standards and ballot the standards independent of each other, not as a set of standards. The independent ballot approach would provide for quicker adoption of a standard as it passes ballot. The current approach could result in an entity balloting "No" due to an issue with one standard and as a result they would have no option but to vote "No" to the entire set. If the majority of entities approve of the modifications made to a particular standard, the entities should be allowed to ballot in the modifications made to that standard. The SDT is taking the approach of deferring implementation of a potentially approved standard until the balloting entities approve all modifications to the standards within CIP. This all or nothing approach is counter productive to the rapid adoption and implementation requested by the FERC. If the standards are drafted</p>

Consideration of Comments on Initial Ballot — CIP-002-2 to CIP-009-2 — Cyber Security Standards (Project 2008-06)

Voter	Entity	Segment	Vote	Comment
				<p>independently there would be a great benefit to the entities that are supplying membership to the SDT. As it stands the SDT is tasked with the entire set of modifications and sponsoring entities may not be able to continue that level of support as the process continues. Individual focused drafting teams would limit the scope and impact on a members time and the impact to the sponsoring entity. Approaching the future phases as individual standards will also allow for more targeted subject matter experts to become involved in specific standards as they pertain to their area of expertise.</p>
Response	<p>Thank you for your comments. The SDT offers the following in response to your concerns:</p> <ol style="list-style-type: none"> 1) To make changes to the language in the standards following the industry comments was deemed to be a significant modification that would have necessitated an additional round of industry comment prior to ballot. That would have resulted in the inability to complete the mandated time-specific modifications per the FERC Order 706. There were issues that required more substantive debate that the SDT chose to defer to Version 3 of the standards. Per the NERC process, the SDT is unable to modify language in this version of the standards once in the balloting phase. 2) The language in Section D "Compliance" was modified to be consistent with the rest of the NERC standards. 3) The requirement for appointing a Senior Manager (CIP-003, Requirement R2) is to identify a single point of accountability for the implementation and compliance with the CIP standards. 4) As required by the NERC standards development process, there were two red-lined versions available for review. The process requires red-lined revisions since the last posting. "Redline Versions to last approval" are the changes made to the Version 1 standards that were posted for industry comment. "Clean and Redline Versions to last posting" are the incremental changes made to the Version 2 standards in response to the industry comments and are the standards submitted for ballot. 5) The SDT agrees that the ANSI-approved standards drafting process should be followed and believes the process has been followed in this instance. Industry comments were solicited and responses made available prior to the submission to ballot. The Standards Committee approved every step of the process followed. 6) The Version 2 changes to the standards have a very narrow focus, with plans for a more complete revision to follow in future versions. A number of comments were raised against requirements that had not been changed between Version 1 and 2. In this instance, the SDT felt it was appropriate to request the comment be deferred until a future revision of the standards. 7) The CIP standards should be viewed as a complete set, with FERC-mandated, time-specific changes made to all eight Version 2 standards. The SDT believes it is appropriate to ballot the eight version 2 standards as a single set for the Version 2 changes. There is also considerable 			

Consideration of Comments on Initial Ballot — CIP-002-2 to CIP-009-2 — Cyber Security Standards (Project 2008-06)

Voter	Entity	Segment	Vote	Comment
				linkage between the eight Version 2 standards, making it very difficult to revise and ballot significant revisions as eight stand-alone standards.
Ralph Rufrano	New York Power Authority	1	Abstain	1) the phrase " the Senior manager" is deemed to be too prescriptive and 2) the term " continuous escort" may cause compliance issues.
Michael Lupo	New York Power Authority	3	Abstain	
Gerald Mannarino	New York Power Authority	5	Abstain	
Response				<p>1) The requirement is to identify a single point of accountability for the implementation and compliance with the CIP standards. Further delegation also needs to be documented to assure the individual granting access or performing other responsibilities normally performed by the Senior Manager has the necessary authorization to do so. The SDT recommends submitting this comment against Version 3 of the CIP standards if still appropriate.</p> <p>2) The term "continuous" does not change the original intent or ability to audit. As used, "continuous" is analogous to "supervised" in that the escort is expected to be aware of the escorted visitor's actions at all times. There are a number of references available that describe how an entity's visitor control program can be verified. One such reference is the NIST SP 800-53A (Guide for Assessing the Security Controls in Federal Information Systems), Control PE-7 (Visitor Control).</p>
Alden Briggs	New Brunswick System Operator	2	Negative	<p>1. "Continuous escorted access" is not measurable. How does one prove this? It should be defined.</p> <p>2. Leadership Role - How an entity is structured to meet compliance to a standard should not be a standard. This could lead to more standards dictating management structure.</p>
Response				<p>1) The term "continuous" does not change the original intent or ability to audit. As used, "continuous" is analogous to "supervised" in that the escort is expected to be aware of the escorted visitor's actions at all times. There are a number of references available that describe how an entity's visitor control program can be verified. One such reference is the NIST SP 800-53A (Guide for Assessing the Security Controls in Federal Information Systems), Control PE-7 (Visitor Control).</p> <p>2) The requirement in the standard does not dictate the management structure of the Responsible Entity. The requirement is to identify a single point of accountability for the implementation and compliance with the CIP standards.</p>
Larry Akens	Tennessee Valley Authority	1	Negative	CIP-006 R1.6 requires a "continuous" escort. This creates a condition that is impossible to prove to auditors. As an alternative, wording might indicate that visitors are to be escorted in a manner to ensure their actions can be supervised and unauthorized disclosures or malicious activities can be prevented, and/or only authorized employees can be escorts.
Frank D	Tennessee Valley	5	Negative	

Consideration of Comments on Initial Ballot — CIP-002-2 to CIP-009-2 — Cyber Security Standards (Project 2008-06)

Voter	Entity	Segment	Vote	Comment
Cuzzort	Authority			
Response	The term "continuous" does not change the original intent or ability to audit. As used, "continuous" is analogous to "supervised" in that the escort is expected to be aware of the escorted visitor's actions at all times. There are a number of references available that describe how an entity's visitor control program can be verified. One such reference is the NIST SP 800-53A (Guide for Assessing the Security Controls in Federal Information Systems), Control PE-7 (Visitor Control) .			
Greg Mason	Dynegy	5	Negative	CIP-006, R1.6 requires a "continuos" escort. The word "continuous" creates an unrealistic compliance expectation and one that would be impossible to prove to auditors.
Response	The term "continuous" does not change the original intent or ability to audit. As used, "continuous" is analogous to "supervised" in that the escort is expected to be aware of the escorted visitor's actions at all times. There are a number of references available that describe how an entity's visitor control program can be verified. One such reference is the NIST SP 800-53A (Guide for Assessing the Security Controls in Federal Information Systems), Control PE-7 (Visitor Control) .			
Benjamin Church	FPL Energy	5	Negative	CIP 005 R1.6 is not auditable from a compliance stand point. Entities will be unable to sufficiently document compliance with the requirement as written.
Response	The term "continuous" does not change the original intent or ability to audit. As used, "continuous" is analogous to "supervised" in that the escort is expected to be aware of the escorted visitor's actions at all times. There are a number of references available that describe how an entity's visitor control program can be verified. One such reference is the NIST SP 800-53A (Guide for Assessing the Security Controls in Federal Information Systems), Control PE-7 (Visitor Control) .			
Kim Warren	Independent Electricity System Operator	2	Affirmative	<p>The IESO votes AFFIRMATIVE so as to move this set of standards forward for further development. However, there still exists a couple of fundamental principle concerns which we expressed earlier, and which we are reiterating below to urge the SDT to address them at the next revision phase</p> <p>a. Standards should hold a functional entity(ies), not a person or a position, responsible for meeting the requirements. Further, delegation is an internal process which does not need to be explicitly mentioned/allowed in a standard. We propose R4 in CIP-002-2 be revised to: "Annual Approval" The Responsible Entity shall appoint a senior manager with the authority to approve annually the risk-based assessment methodology, the list of Critical Assets and the list of Critical Cyber Assets. Based on Requirements R1, R2, and R3, the Responsible Entity may determine that it has no Critical Assets or Critical Cyber Assets. The Responsible Entity shall keep a signed and dated record of its approval of the risk-based assessment methodology, the list of Critical Assets and the list of Critical Cyber Assets (even if such lists are null.)" If appointing a senior manager is required to ensure standards are complied with and implemented, we recommend that CIP-002 be updated by 1) moving CIP-003 R2 into</p>

Consideration of Comments on Initial Ballot — CIP-002-2 to CIP-009-2 — Cyber Security Standards (Project 2008-06)

Voter	Entity	Segment	Vote	Comment
				<p>CIP-002 or 2) CIP-002 R4 should explicitly reference CIP-003 R2. We prefer moving CIP-003 R2 into CIP-002 so that all the Requirements that all Entities must complete are in one Standard</p> <p>b. CIP-006 R1.6 should not require "continuous" escorted access. "Continuous" is a condition that is not measurable and hence does not meet the basic characteristics of reliability standards. We suggest this word be removed.</p>
Response	<p>a) The requirement is to identify a single point of accountability for the implementation and compliance with the CIP standards. Further delegation also needs to be documented to assure the individual granting access or performing other responsibilities normally performed by the Senior Manager has the necessary authorization to do so. As CIP-003 is the Governance standard and assignment of a Senior Manager is a governance issue, the SDT chose to leave the assignment in CIP-003 and to make CIP-003, Requirement R2 applicable to all Responsible Entities. To make the change following the industry comments was deemed to be a significant modification that would have necessitated an additional round of industry comment prior to ballot. That would have resulted in the inability to complete the mandated time-specific modifications per the FERC Order 706. The SDT recommends submitting this comment against Version 3 of the CIP standards if still appropriate.</p> <p>b) The term "continuous" does not change the original intent or ability to audit. As used, "continuous" is analogous to "supervised" in that the escort is expected to be aware of the escorted visitor's actions at all times. There are a number of references available that describe how an entity's visitor control program can be verified. One such reference is the NIST SP 800-53A (Guide for Assessing the Security Controls in Federal Information Systems), Control PE-7 (Visitor Control).</p>			
Alan Adamson	New York State Reliability Council	10	Affirmative	<p>The New York State Reliability Council (NYSRC) supports the need to improve the NERC Cyber Security Standards. Despite reservations with certain revisions in this draft version, we believe that overall, the modified standards will improve system reliability. The NYSRC, therefore, has voted in the Affirmative. Because of the following concerns, the NYSRC encourages the Drafting Team to seriously address these issues when the Cyber Security Standards are next modified:</p> <ol style="list-style-type: none"> 1. CIP-003-1, Requirement 2 - We believe that this requirement, as proposed, oversteps NERC's bounds by giving NERC the authority the dictate corporate governance structure and policy. 2. CIP-006-2, Requirement 1.6 - This requirement does not define what "continuous escorted access" means. Demonstrating compliance with this requirement, as stated, would be very difficult. Removing the word "continuous" would resolve this issue.
Response	<p>1) The requirement is to identify a single point of accountability for the implementation and compliance with the CIP standards. Further delegation also needs to be documented to assure the individual granting access or performing other responsibilities normally performed by the Senior Manager has the necessary authorization to do so. As CIP-003 is the Governance standard and assignment of a Senior Manager is a governance issue, the SDT chose to leave the assignment in CIP-003 and to make CIP-003, Requirement R2 applicable to all Responsible</p>			

Consideration of Comments on Initial Ballot — CIP-002-2 to CIP-009-2 — Cyber Security Standards (Project 2008-06)

Voter	Entity	Segment	Vote	Comment
				<p>Entities. The SDT recommends submitting this comment against Version 3 of the CIP standards if still appropriate.</p> <p>2) The term “continuous” does not change the original intent or ability to audit. As used, “continuous” is analogous to “supervised” in that the escort is expected to be aware of the escorted visitor’s actions at all times. There are a number of references available that describe how an entity’s visitor control program can be verified. One such reference is the NIST SP 800-53A (Guide for Assessing the Security Controls in Federal Information Systems), Control PE-7 (Visitor Control).</p>
Kathleen Goodman	ISO New England, Inc.	2	Negative	<p>As you are aware, ISO New England (ISO-NE) is committed to maintaining and supporting high-quality, enforceable, mandatory Reliability Standards -- a part of which includes the Cyber Security Standards. We have, however, two fundamental enforceability-related concerns with the currently-posted draft. We believe that these concerns warrant a Negative vote. The Standards at issue are CIP-003, R2 and CIP-006, R1.6.</p> <p>To the extent that NERC could sever these two provisions from its filing of the CIP Standard modifications to the Federal Energy Regulatory Commission (“FERC”), or alternatively, FERC (under 18 C.F.R. §39.5(e)) could disapprove, in part, these two aspects of the CIP Standard modifications, ISO-NE would otherwise vote in the Affirmative for these CIP Standard modifications.</p> <p>A. <u>CIP-003, Requirement 2</u></p> <p>Under the Standards as currently drafted (<i>see specifically</i> CIP-002), ISO-NE has a single senior manager responsible for approving annually the list of Critical and Critical Cyber Assets. That list has been developed pursuant to a risk-based methodology adopted by the ISO-NE. Under ISO-NE’s current management structure, business units (in this case the Information Services Department) are responsible for identifying Critical Cyber Assets. Other Departments with key responsibilities – such as setting the ISO’s budget and capital expenditures (as is the case of the Finance Department) – also play a role in ensuring that the Company can implement needed steps to comply. As explained further below, it is difficult to understand how the newly proposed Requirement 2 of CIP-003 has a reasonable relationship to defining or improving upon a “reliability” or “security” objective.</p> <p>Requirement 2 of CIP-003 states “Leadership — The Responsible Entity shall assign a single senior manager with overall responsibility and authority for leading and managing the entity’s implementation of, and adherence to, Standards CIP-002-2 through CIP-009-2.” There are numerous problems with this new requirement.</p> <p>1. <u>The Requirement Does Not Appear to be a Reliability Standard.</u></p>

Consideration of Comments on Initial Ballot — CIP-002-2 to CIP-009-2 — Cyber Security Standards (Project 2008-06)

Voter	Entity	Segment	Vote	Comment
				<p>First, this requirement appears to overstep the authority granted to NERC as the ERO under Section 215 of the Federal Power Act in that it attempts to dictate “how” a responsible entity meets compliance with a reliability/security objective – in this case how the company establishes a management structure to achieve compliance. This requirement sets no actual “reliability” or “cybersecurity” performance requirement, and therefore appears to have no reasonable relationship to NERC’s authority to set “reliability standards” as that term is defined under Section 215. “Reliability Standards” are “requirement[s] for the operation of existing bulk-power system facilities, including cyber-security protection.” Attempting to dictate, in this instance, how companies organize their management goes well beyond NERC’s authority to establish standards governing the “operation” and “protection” of bulk-power system facilities.</p> <p>FERC has previously recognized the distinction between regulating “what” registered entities need to do, as opposed to regulating “how” they achieve those reliability/security objectives, and the need for the ERO to balance these considerations. <i>See</i> Order No. 672 at P260. By establishing a Standard that seeks to regulate internal management structure without explaining how such a requirement itself establishes greater security, the proposed modification would not appear to address the need to balancing “what” is being regulated versus “how” it is accomplished. More generally, the entire enforcement regime helps to ensure that companies are doing what is necessary to implement standards. No specific requirement is needed stating as much.</p> <p><u>2. The Standard Drafting Team Provided No Suitable Rationale as Concerns a Non-Reliability or Security Matter.</u></p> <p>Second, even if this matter is argued to be within NERC’s authority, the Standard Drafting Team provided no suitable justification explaining its purpose. ISO-NE, and other entities, raised this concern in prior comments, and the Standard Drafting Team (“SDT”) simply deferred to generic language in Order No. 706. <i>See, e.g.,</i> Order No. 706 at P381 (the “Commission’s intent is to ensure that there is a clear line of authority and that cyber security functions are given the prominence they deserve.”). <i>See also</i> <u>U.S. – Canada Power System Blackout Task Force, Final Report on the August 14, 2003 Blackout in the United States and Canada: Causes and Recommendations</u> (April 2004) (Blackout Report), Recommendation 43 (recommending that corporations establish “clear authority” for</p>

Consideration of Comments on Initial Ballot — CIP-002-2 to CIP-009-2 — Cyber Security Standards (Project 2008-06)

Voter	Entity	Segment	Vote	Comment
				<p>physical and cyber security, and that this “authority should have the ability to influence corporate decision-making and the authority to make physical and cyber security-related decisions.”) (emphasis added).²</p> <p>However various parties or regulators might interpret what constitutes suitable “influence”, achieving the Commission’s intent on ensuring that cyber-security matters are given “prominence” within a Responsible Entity could be accomplished in a variety of ways other than drafting new Standard requirements. Such other measures could include the manner in which NERC requires periodic reporting by responsible entities, the frequency with which NERC could conduct audits of responsible entities, etc.... In fact, the whole scheme of establishing a phased-in approach for the CIP Standards acts as a means of ensuring that NERC and Regional Entities <i>track</i> Responsible Entities’ progress in meeting the Standards – itself a metric for measuring the “prominence” with which the implementation of Standards is given within a Responsible Entity.</p> <p>The concept of “authority and implementation” – as drafted by the SDT for inclusion as a mandatory <i>Standard</i> – simply does not add much to what the FERC and the Blackout Report has previously observed. However, when drafted as a Standard, the language raises issues of: (a) how the SDT intends this requirement to be interpreted, (b) the ERO’s specific intent under Section 215 of the Federal Power Act behind approving a requirement that regulates management structure, and (c) how Regional Entities, NERC or FERC would enforce such language.</p> <p>More generally, it is well understood that SDT may explore a variety of means to address the FERC’s concerns. In this instance, given the authority issues raised by NERC Stakeholders, the SDT should have provided more rationale of its proposal. It is especially important for the SDT to provide a robust rationale for its decisions if it attempts to regulate non-technical matters, because FERC is only obligated to give “due weight” to the “technical expertise” of the ERO when determining when to approve a Standard or Standard modification. <i>See</i> 18 C.F.R. § 39.5(c)(1). As importantly, given the fact that ERO determinations of a non-technical nature might have <i>broader</i> impacts to how other Standards are developed or modified, understanding the thinking of this particular SDT is necessary to ensuring future standards are drafted appropriately.</p>

² See <http://www.ferc.gov/industries/electric/indus-act/blackout/ch7-10.pdf>

Consideration of Comments on Initial Ballot — CIP-002-2 to CIP-009-2 — Cyber Security Standards (Project 2008-06)

Voter	Entity	Segment	Vote	Comment
				<p>3. <u>Ambiguity in the Standard Suggests that NERC Intends Responsible Entities to Assign Too Much Authority with One Individual.</u></p> <p>As noted above, while the provision itself attempts to address generally expressed concerns in Order No. 706, it also appears to envision a management structure that could be at odds with generally accepted principles of corporate management.</p> <p>While the phrase “overall responsibility and authority for leading and managing the entity’s implementation of, and adherence to” compliance with standards might be susceptible to multiple interpretations, it could unduly “blur the lines” between key Business Officers (for example, between Information Services and Finance as concerns the language relating to “implementation of” compliance). “Implementation” of these standards may involve decisions regarding authorizing capital expenditures, and these decisions may not be within the authority of any specific business unit/manager. These decisions may involve the functions of a Chief Finance Officer or even a Company’s Board of Directors, in which case the “overall responsibility and authority” cannot sit with a single individual.</p> <p>Of course, the SDT may have a different concept in mind when it referred to a single individual having “responsibility” and “authority”, but the SDT never gave a fulsome explanation of what it had in mind, and <i>how it was implementing the issues raised in Order No. 706</i>. This vagueness should establish real concerns about how this “standard” will be enforced.</p> <p>4. <u>Drafting Creates Potential Confusion with Other Standards.</u></p> <p>Finally, even if the provision is a justifiable exercise of NERC’s authority, ISO-NE believes this requirement is poorly drafted as it should be contained within, and harmonized with, CIP-002. Under CIP-002, some Registered Entities will find that the CIP-002 through -009 requirements do not apply. Moreover, because CIP-002 refers to “a senior manager” having responsibility for approving the Critical and Critical Cyber Asset list, placing this new provision in CIP-003 simply creates unnecessary confusion in how to apply multiple provisions that relate to the same thing in different standards.</p> <p>B. <u>CIP-006, Requirement 1.6</u></p> <p>Requirement 1.6 of CIP-006 states “Continuous escorted access within the Physical Security</p>

Consideration of Comments on Initial Ballot — CIP-002-2 to CIP-009-2 — Cyber Security Standards (Project 2008-06)

Voter	Entity	Segment	Vote	Comment
				<p>Perimeter of personnel not authorized for unescorted access.” Of course, under the current version of the Standard, ISO-NE provides “escorted access” through a variety of means, such as through providing physical escorts and through installing electronic surveillance at access points. Because of the ambiguity regarding “continuous,” ISO-NE believes additional information is needed that would support the enforceability/measurement of compliance with the Standard and what is actually needed to implement further measures to ensure compliance. This is particularly important to ISO-NE, because it needs to present its budgeted capital expenditures to its stakeholders for review and advice.</p> <p>First, with regard to the enforceability, ISO-NE is concerned that “<i>continuous</i>” escorted access will prove to be a difficult, if not impossible, Requirement with which registered entities can effectively demonstrate compliance, because of the difficulty determining what records/data can show that such escorting was “uninterrupted.”</p> <p>Second, further information is needed about what “continuous” means, because of the need to develop an appropriate implementation plan to carry out such a requirement. For example, if a company has multiple visitors on site, then the measures employed to ensure “continuous” escorting for each visitor can rapidly increase. For example, if there are multiple personnel working within the Physical Security Perimeter, each one would appear to need a separate escort.</p> <p>While ISO-NE believes that the concerns raised above warrant continued work on this requirement before it should be approved, ISO-NE requests, in the alternative, additional guidance/clarification on how to interpret what constitutes a “continuous” escort.</p> <p>C. Conclusion</p> <p>As stated above, ISO-NE takes its CIP Standard compliance very seriously and supports the development of improved CIP Standards. ISO-NE believes that the Standards proposed for approval here, if omitting the Requirements identified above, would themselves establish a more robust CIP Standard regime.</p> <p>The concerns identified with only these two requirements above were made during the comment period of the drafts now being balloted. In ISO-NE’s view, these concerns have not been sufficiently dealt with by the SDT to produce an enforceable, auditable product. A more robust explanation from the SDT might have served to address ISO-NE’s concerns, but lacking that, ISO-NE is compelled to raise its objections again at this time. We look forward to working closely with the SDTs in the future to ensure high-quality Standards for protecting</p>

Consideration of Comments on Initial Ballot — CIP-002-2 to CIP-009-2 — Cyber Security Standards (Project 2008-06)

Voter	Entity	Segment	Vote	Comment
				the bulk-power system's reliability and cyber-security and enabling robust enforcement.
Response	<p>A) ISO New England expressed concern that CIP-003, Requirement R2 does not appear to be a reliability standard and the SDT provided no suitable rationale as concerns a non-reliability or security matter. ISO-NE also expressed concern that ambiguity in the standard suggests that NERC intends Responsible Entities to assign too much authority with one individual and that this requirement is poorly crafted and creates potential confusion with other standards.</p> <p>The FERC, at Paragraph 381 of Order 706, "requires the designation of a single manager who has direct and comprehensive responsibility and accountability for implementation and ongoing compliance with the CIP Reliability Standards. The Commission's intent is to ensure that there is a clear line of authority and that cyber security functions are given the prominence they deserve. The Commission agrees with commenters that the senior manager, by virtue of his or her position, is not a user, owner or operator of the Bulk-Power System that is personally subject to civil penalties pursuant to section 215 of FPA." The SDT believes the directive in the FERC order appropriately justifies the revision to the existing requirement. The requirement in the standard does not dictate the management structure of the Responsible Entity. The requirement is to identify a single point of accountability for the implementation and compliance with the CIP standards. The SDT envisions that the Senior Manager will seek the counsel of other Responsible Entity personnel in carrying out this responsibility and can delegate many of the required approvals.</p> <p>B) ISO-NE expressed concern that the requirement for "continuous" escort will be difficult to prove to auditors and that additional information is required defining the meaning of "continuous."</p> <p>The term "continuous" does not change the original intent or ability to audit. As used, "continuous" is analogous to "supervised" in that the escort is expected to be aware of the escorted visitor's actions at all times. There are a number of references available that describe how an entity's visitor control program can be verified. One such reference is the NIST SP 800-53A (Guide for Assessing the Security Controls in Federal Information Systems), Control PE-7 (Visitor Control).</p>			
Brian Evans-Mongeon	Utility Services LLC	8	Negative	Utility Services LLC supports the comments as filed by ISO New England regarding this matter. In particular, the "continuous" monitoring aspect is extremely burdensome for smaller entities.
Response	<p>A) ISO New England expressed concern that CIP-003, Requirement R2 does not appear to be a reliability standard and the SDT provided no suitable rationale as concerns a non-reliability or security matter. ISO-NE also expressed concern that ambiguity in the standard suggests that NERC intends Responsible Entities to assign too much authority with one individual and that this requirement is poorly crafted and creates potential confusion with other standards.</p> <p>The FERC, at Paragraph 381 of Order 706, "requires the designation of a single manager who has direct and comprehensive responsibility and accountability for implementation and ongoing compliance with the CIP Reliability Standards. The Commission's intent is to ensure that there is a clear line of authority and that cyber security functions are given the prominence they deserve. The Commission agrees with commenters that the senior manager, by virtue of his or her position, is not a user, owner or operator of the Bulk-Power System that is personally subject to civil penalties pursuant to section 215 of FPA." The SDT believes the directive in the FERC order appropriately justifies the revision to the existing</p>			

Consideration of Comments on Initial Ballot — CIP-002-2 to CIP-009-2 — Cyber Security Standards (Project 2008-06)

Voter	Entity	Segment	Vote	Comment
				<p>requirement. The requirement in the standard does not dictate the management structure of the Responsible Entity. The requirement is to identify a single point of accountability for the implementation and compliance with the CIP standards. The SDT envisions that the Senior Manager will seek the counsel of other Responsible Entity personnel in carrying out this responsibility and can delegate many of the required approvals.</p> <p>B) ISO-NE expressed concern that the requirement for “continuous” escort will be difficult to prove to auditors and that additional information is required defining the meaning of “continuous.”</p> <p>The term “continuous” does not change the original intent or ability to audit. As used, “continuous” is analogous to “supervised” in that the escort is expected to be aware of the escorted visitor’s actions at all times. There are a number of references available that describe how an entity’s visitor control program can be verified. One such reference is the NIST SP 800-53A (Guide for Assessing the Security Controls in Federal Information Systems), Control PE-7 (Visitor Control).</p>
Gregory Campoli	New York Independent System Operator	2	Affirmative	The NYISO supports continued development of CIP standards to more effectively address growing security concerns in the industry. The NYISO would also like to identify some issues observed that need to be addressed. CIP-006 Req 1.6 requires continuous escort. It is not clear at this time how this requirement would be monitored or how an entity would show compliance. A requirement should be structured so that compliance is measurable and enforceable.
Response				The term “continuous” does not change the original intent or ability to audit. As used, “continuous” is analogous to “supervised” in that the escort is expected to be aware of the escorted visitor’s actions at all times. There are a number of references available that describe how an entity’s visitor control program can be verified. One such reference is the NIST SP 800-53A (Guide for Assessing the Security Controls in Federal Information Systems) , Control PE-7 (Visitor Control).
Kent Saathoff	Electric Reliability Council of Texas, Inc.	10	Affirmative	<p>1) Voting affirmative or negative to NERC standards CIP002-2 through CIP009-2 in totality creates a situation where the wording contained in one standard can result in the rejection of solid requirements within other standards. The collective voting of the CIP standards is in direct conflict with the balloting processes used for other NERC Reliability standards. Each standard should be drafted to stand on its own merits and must not hold modifications to any other standard hostage to the weaknesses of a subset. Below are ERCOT’s comments regarding the changes proposed to the CIP standards.</p> <p>2) CIP-002-2 R4 The concept of “the senior manager” is not addressed until CIP-003. It would be advised to clarify who is being referred to here or move the Leadership requirement within CIP-003-2 into CIP-002-2.</p> <p>3) CIP-003-2 R3 It is unclear as to whether NERC’s intent is that the practice under exception cannot commence until an exception is approved. There will be situations where systems, processes, or practices are already well established and in full operation prior to the effective</p>

Consideration of Comments on Initial Ballot — CIP-002-2 to CIP-009-2 — Cyber Security Standards (Project 2008-06)

Voter	Entity	Segment	Vote	Comment
				<p>date of the standards. Clarification of this is requested.</p> <p>4) CIP-006-2 R1.6 requires a "continuous" escort. Absolutes such as "continuous", "always", etc. create a condition that is impossible to prove to auditors and, in most cases, impossible to achieve.</p>
Response				<p>1) The CIP standards should be viewed as a complete set, with FERC-mandated changes made to all eight version 2 standards. The SDT believes it is appropriate to ballot the eight version 2 standards as a single set for the Version 2 changes.</p> <p>2) As CIP-003 is the Governance standard and assignment of a Senior Manager is a governance issue, the SDT chose to leave the assignment in CIP-003 and to make CIP-003, Requirement R2 applicable to all Responsible Entities. The SDT agrees after receiving the industry review comments that the assignment of the Senior Manager would be less confusing if it were moved to CIP-002. However, to make the change following the industry comments was deemed to be a significant modification that would have necessitated an additional round of industry comment prior to ballot. That would have resulted in the inability to complete the mandated time-specific modifications per the FERC Order 706. The SDT recommends submitting this comment against Version 3 of the CIP standards if still appropriate.</p> <p>3) CIP-003, Requirement R3 provides for the Responsible Entity taking an exception to its Cyber Security Policy required by CIP-003, Requirement R1. This is separate from the proposed modifications to the NERC Rules of Procedure providing for Technical Feasibility Exceptions. Both require compensating measures and those measures can be implemented prior to receiving approval of the applicable exception.</p> <p>4) The term "continuous" does not change the original intent or ability to audit. As used, "continuous" is analogous to "supervised" in that the escort is expected to be aware of the escorted visitor's actions at all times. There are a number of references available that describe how an entity's visitor control program can be verified. One such reference is the NIST SP 800-53A (Guide for Assessing the Security Controls in Federal Information Systems), Control PE-7 (Visitor Control).</p>
Horace Stephen Williamson	Southern Company Services, Inc.	1	Affirmative	1. We are concerned that NERC staff has taken the Technical Feasibility Exception (TFE) process out of the hands of the Standards Drafting Team (SDT) and placed it in the decision making process of NERC staff alone. This will not allow an industry vote on these new Rules of Procedure.
Robin Hurst	Alabama Power Company	3	Affirmative	2. This new TFE document, that is out for comments through April 30th, only allow exceptions to be requested for 8 requirements in 2 (of the 8) CIP standards. Entities should be allowed to seek exceptions on all of the CIP requirements if legacy systems prevent them from complying with these current standards. Therefore, we request the SDT initiate that change in Version 3.
Leslie Sibert	Georgia Power Company	3	Affirmative	
Gwen S Frazier	Gulf Power Company	3	Affirmative	3. CIP-006 R1.6 requires a "continuous" escort. This creates a condition that is difficult, if not impossible, to prove to auditors. We suggest that the drafting team work on alternate language to allow for 'supervised' access.
Don Horsley	Mississippi Power	3	Affirmative	

Consideration of Comments on Initial Ballot — CIP-002-2 to CIP-009-2 — Cyber Security Standards (Project 2008-06)

Voter	Entity	Segment	Vote	Comment
Response				<p>1) Respectfully, the CIP SDT has no control over the approval process for changes to the NERC Rules of Procedure. The industry has an opportunity to provide comments to the proposed TFE process prior to adoption by the NERC Board of Trustees. The industry will likely have another opportunity to provide comments as part of the FERC approval process. The SDT recommends the industry take advantage of every opportunity to influence the ultimate TFE process.</p> <p>2) The suggestion to modify Version 3 of the standards to allow a TFE to be requested for any CIP standard requirement will be considered by the SDT. In the mean time, the SDT recommends the industry comment to NERC and, if necessary, FERC proposing how the issue might be remedied in the TFE process.</p> <p>3) The term “continuous” does not change the original intent or ability to audit. As used, “continuous” is analogous to “supervised” in that the escort is expected to be aware of the escorted visitor’s actions at all times. There are a number of references available that describe how an entity’s visitor control program can be verified. One such reference is the NIST SP 800-53A (Guide for Assessing the Security Controls in Federal Information Systems), Control PE-7 (Visitor Control).</p>
Richard J. Kafka	Potomac Electric Power Co.	1	Affirmative	<p>1) Pepco ,indeed all Pepco Holdings affiliates, is concerned about the process used to remove the technical feasibility language and proposed changes to the Rules of Procedure. The industry has been following an implementation schedule for the version 1 set of CIP -002 through CIP-009 for nearly 3 years and are already in or nearing the compliance date and the period to begin documenting compliance. While we understand the need to make the change, there is no discussion of a phase-in of this change. One can anticipate NERC being overwhelmed with TFE Requests and a large number still pending (or even sent back with required changes) after the compliance period for CIP-002 - CIP-009 has begun. The Implementation Plan realistically provides an example showing the effective date as early as January 1, 2010, possibly delayed until April 1 depending on the timing of the approvals. This may force registered entities into non-compliance even though they have been rigorously pursuing compliance.</p> <p>2) Entities may also be forced into non-compliance if there is no timely response from NERC to the TFE Requests.</p>
Response				<p>1) The drafting team anticipates that the Phase 1 revisions to the standards will not be approved by the NERC Board of Trustees until the end of May 2009. Accordingly, the earliest possible effective date would be January 1, 2010. Regulatory agency approval processes could push this date out even further for Responsible Entities within those jurisdictions. The drafting team believes the six to nine month implementation plan is reasonable.</p> <p>2) Respectfully, the CIP SDT has no control over the approval process for changes to the NERC Rules of Procedure. The industry has an opportunity to provide comments to the proposed TFE process prior to adoption by the NERC Board of Trustees. The industry will likely have another opportunity to provide comments as part of the FERC approval process. The SDT recommends the industry take advantage of every opportunity to influence the ultimate TFE process.</p>

Consideration of Comments on Initial Ballot — CIP-002-2 to CIP-009-2 — Cyber Security Standards (Project 2008-06)

Voter	Entity	Segment	Vote	Comment
Michael Gammon	Kansas City Power & Light Co.	1	Affirmative	The scope of the Technical Feasibility Exception process should not be limited to the specific CIP requirements listed. It is unrealistic to expect that standard writers will be able to identify in advance all areas that may require a TFE.
Charles Locke	Kansas City Power & Light Co.	3	Affirmative	
Thomas Saitta	Kansas City Power & Light Co.	5	Affirmative	
Response	Respectfully, while the CIP SDT will consider the TFE issue in future revisions to the standards, the SDT cannot predict and account for all possible nuances that might require a TFE. The handling of TFE requests in those instances where they not currently permitted by the proposed Appendix 4D to the NERC Rules of Procedure is best addressed by a modification to the Rules of Procedure. The industry has an opportunity to provide comments to the proposed TFE process prior to adoption by the NERC Board of Trustees. The industry will likely have another opportunity to provide comments as part of the FERC approval process. The SDT recommends the industry take advantage of every opportunity to influence the ultimate TFE process. The SDT recommends the industry comment to NERC and, if necessary, FERC proposing how the issue might be remedied in the TFE process.			
Scott M. Helyer	Tenaska, Inc.	5	Negative	Various CIP standards are not acceptable as written without Technical Feasible Exemptions (TFE) being included in the standards themselves or without some reference to TFE approved in another process. As the potential approval of TFE through a separate process is not occurring prior to this vote, then the following CIP standards need to include TFE as follows: CIP-005 R2.4. Where external interactive access into the Electronic Security Perimeter has been enabled, the Responsible Entity shall implement strong procedural or technical controls at the access points to ensure authenticity of the accessing party, where technically feasible. R2.6. Appropriate Use Banner – Where technically feasible, electronic access control devices shall display an appropriate use banner on the user screen upon all interactive access attempts. The Responsible Entity shall maintain a document identifying the content of the banner. R3.1. For dial-up accessible Critical Cyber Assets that use non-routable protocols, the Responsible Entity shall implement and document monitoring process(es) at each access point to the dial-up device, where technically feasible. R3.2. Where technically feasible, the security monitoring process(es) shall detect and alert for attempts at or actual unauthorized accesses. These alerts shall provide for appropriate notification to designated response personnel. Where alerting is not technically feasible, the Responsible Entity shall review or otherwise assess access logs for attempts at or actual unauthorized accesses at least every ninety calendar days. CIP-007 R5.3. At a minimum, the Responsible Entity shall require and use passwords, subject to the following, as technically feasible: R5.3.1. Each password shall be a minimum of six characters. R5.3.2. Each password shall consist of a combination of alpha, numeric, and "special" characters. R5.3.3. Each password shall be changed at least

Consideration of Comments on Initial Ballot — CIP-002-2 to CIP-009-2 — Cyber Security Standards (Project 2008-06)

Voter	Entity	Segment	Vote	Comment
				<p>annually, or more frequently based on risk. R6. Security Status Monitoring” The Responsible Entity shall ensure that all Cyber Assets within the Electronic Security Perimeter, as technically feasible, implement automated tools or organizational process controls to monitor system events that are related to cyber security. R6.3. The Responsible Entity shall maintain logs of system events related to cyber security, where technically feasible, to support incident response as required in Standard CIP- 008-2.</p>
Response	<p>The proposed TFE process currently allows for TFE Requests against requirements R2.4, R2.6, R3.1 and R3.2 of CIP-005-1, and R2.3, R4, R5.3, R6 and R6.3 of CIP-007-1, and any subsequent versions of these Requirements that continue to expressly provide either (i) that compliance with their terms is required where or as technically feasible or (ii) that technical limitations may preclude compliance with the terms of the Requirement. Per the language in the proposed TFE process, the TFE Request is allowed for the same requirements in version 2 of the CIP standards. Respectfully, while the CIP SDT will consider the TFE issue in future revisions to the standards, the SDT cannot predict and account for all possible nuances that might require a TFE. The handling of TFE requests in those instances where they not currently permitted by the proposed Appendix 4D to the NERC Rules of Procedure is best addressed by a modification to the Rules of Procedure. The industry has an opportunity to provide comments to the proposed TFE process prior to adoption by the NERC Board of Trustees. The industry will likely have another opportunity to provide comments as part of the FERC approval process. The SDT recommends the industry take advantage of every opportunity to influence the ultimate TFE process. The SDT recommends the industry comment to NERC and, if necessary, FERC proposing how the issue might be remedied in the TFE process.</p>			
Edward W Pourciau	Georgia System Operations Corporation	3	Negative	<p>1) After thorough review of the Proposed Procedure for Requesting and Receiving Technical Feasibility Exception it has become obvious that the CIP Standards CIP-002 through CIP-009 do not account for other possible exceptions to the standards. In addition, there are some inconsistencies in where “technically feasible” and “technical limitation” verbiage is placed within CIP standard or sub-standard. In CIP-007 R5.2.1 the verbiage states “where possibility” and not “technically feasible”</p>
Guy Andrews	Georgia System Operations Corporation	4	Negative	<p>2) In CIP-003 through CIP-009 section D. 1.5 needs to reinstate the statement “Duly authorized exceptions will not result in non-compliance”.</p> <p>3) The “Effective Date” verbiage in all CIP standards is awkward and could be confusing.</p> <p>4) Recommend verbiage changes for the following sections in all CIP standards: D. Compliance 1.1.2 ERO for Regional Entity and Responsible Entity in certain cases 1.1.3 Third-Party monitor for NERC without vested interest in the outcome. 1.4.1 as part of a Compliance Violation investigation. 1.4.2 term “audit records” is unclear</p> <p>5) In CIP-003 R5.1 word “logical” should be changed to “Cyber”</p> <p>6) In CIP-006 R1.8 should read “Review the physical security plan at least once every 12</p>

Consideration of Comments on Initial Ballot — CIP-002-2 to CIP-009-2 — Cyber Security Standards (Project 2008-06)

Voter	Entity	Segment	Vote	Comment
				<p>months"</p> <p>7) In CIP-007 B. Requirements the verbiage that was deleted in the first line should be reinstated.</p> <p>8) In CIP-007 R9 and CIP-009 R3 "thirty" should be changed to "sixty"</p>
Response				<p>1) Respectfully, while the CIP SDT will consider the TFE issue in future revisions to the standards, the SDT cannot predict and account for all possible nuances that might require a TFE. Per the NERC process, the SDT is unable to modify language in this version of the standards once in the balloting phase. The handling of TFE requests in those instances where they not currently permitted by the proposed Appendix 4D to the NERC Rules of Procedure is best addressed by a modification to the Rules of Procedure. The industry has an opportunity to provide comments to the proposed TFE process prior to adoption by the NERC Board of Trustees. The industry will likely have another opportunity to provide comments as part of the FERC approval process. The SDT recommends the industry take advantage of every opportunity to influence the ultimate TFE process.</p> <p>2) The language in Section D "Compliance" was modified to be consistent with the rest of the NERC standards.</p> <p>3) A clarifying example of the effective date was included in the "Implementation Plan for Version 2 of Cyber Security Standards CIP-002-2 through CIP-009-2" document.</p> <p>4) The language in Section D "Compliance" was modified to be consistent with the rest of the NERC standards and is defined in the NERC Compliance Monitoring and Evaluation Program (CMEP). The SDT is not able to modify the language as suggested.</p> <p>5) Per the NERC process, the SDT is unable to modify language in this version of the standards once in the balloting phase. The SDT recommends submitting this comment against Version 3 of the CIP standards if still appropriate.</p> <p>6) Per the NERC process, the SDT is unable to modify language in this version of the standards once in the balloting phase. The SDT recommends submitting this comment against Version 3 of the CIP standards if still appropriate.</p> <p>7) The stricken language was duplicative of language in Section A.3., "Purpose." The SDT recommends submitting this comment against Version 3 of the CIP standards if still appropriate.</p> <p>8) The Commission stated in Paragraph 651 of FERC Order 706 that 30 days were sufficient to update the documentation required by CIP-007, Requirement R9. Likewise, the Commission stated in Paragraph 731 of Order 706 that 30 days were sufficient to update the Recovery Plans.</p>
Dana Cabbell	Southern California Edison Co.	1	Negative	SCE supports the changes in the revised Critical Infrastructure Protection Standards ("CIP Standards"), and greatly appreciates the expedited effort put forth by the 706 Standards Drafting Team ("SDT") to revise the standards. However, SCE is concerned about inconsistencies between the Version 2 CIP Standards, and the NERC's proposed revision to
	Southern California	3	Negative	

Consideration of Comments on Initial Ballot — CIP-002-2 to CIP-009-2 — Cyber Security Standards (Project 2008-06)

Voter	Entity	Segment	Vote	Comment
<p>David Schiada</p> <p>Marcus V Lotto</p>	<p>Edison Co.</p> <p>Southern California Edison Co.</p>	<p>6</p>	<p>Negative</p>	<p>the Procedure For Requesting And Receiving Technical Feasibility Exceptions To NERC Critical Infrastructure Protection Standards (“Rules of Procedure”). While SCE understands that the proposed change to the Rules of Procedure is not directly associated with the CIP Version 2 ballot, SCE is of the opinion that the two documents are inextricably linked and cannot be considered independently. SCE’s concerns are as follows:</p> <p>1.) The proposed change to the Rules of Procedure implies that a claim of technical limitation or feasibility represents non-compliance with a requirement. As written, in both Version 1 and 2, there is no language in the requirements that indicate a claim of technical feasibility or limitation, does not meet the requirement.</p> <p>2.) The revised standards state the following assignment for the SDT CS0706: “...assigned the responsibility to review each of the following reliability standards to ensure that they conform to the latest version of the ERO Rules of Procedure, including the Reliability Standards Development Procedure...” SCE is concerned that the proposed revision to the Rules of Procedure was released subsequent to the posting of Version 2 standards revision. Since the revised Rules of Procedure were written after the drafting of the Version 2 standards, the drafting team could not draft to ensure conformance with the Rules of Procedure., rather the team considered the previous version of the Rules of Procedure. SCE does not believe the Version 2 CIP Standards adequately address technical feasibility, and that modifications of the technical feasibility requirements should be handled through modification of the standards themselves, not through a procedural change of the Rules of Procedure. Changing the requirements for the technical feasibility exception through the standards development process will provide clarity to the standards and ensure consistency across the industry. To remedy these concerns, SCE recommends that NERC revise the proposed Rules of Procedure to reflect that the modifications regarding technical limitations or feasibility be applicable to the CIP Version 3 standards under development to ensure clear alignment of the rules of procedure and the CIP standards. This would allow the Version 3 standards to have clear language about the requirements for technical limitations or feasibility. Alternatively, SCE supports an expedited revision to the Version 2 CIP standards intended to clarify the scope and context of technical feasibility limitations within the requirements themselves.</p>
<p>Response</p>	<p>1) An exception taken against the Responsible Entity’s compliance policy does not relieve the entity from compliance with the requirement of the standard. The ERO (NERC) has determined that inability to strictly comply with the requirements of a CIP standard is, in fact, a violation of the standard requirement and has proposed a TFE process whereby the Responsible Entity can remedy the issue without being subject to a finding of violation or imposition of penalties.</p>			

Consideration of Comments on Initial Ballot — CIP-002-2 to CIP-009-2 — Cyber Security Standards (Project 2008-06)

Voter	Entity	Segment	Vote	Comment
				<p>2) Respectfully, while the CIP SDT will consider the TFE issue in future revisions to the standards, the SDT cannot predict and account for all possible nuances that might require a TFE. The handling of TFE requests in those instances where they not currently permitted by the proposed Appendix 4D to the NERC Rules of Procedure is best addressed by a modification to the Rules of Procedure. The industry has an opportunity to provide comments to the proposed TFE process prior to adoption by the NERC Board of Trustees. The industry will likely have another opportunity to provide comments as part of the FERC approval process. The SDT recommends the industry take advantage of every opportunity to influence the ultimate TFE process.</p>
Martin Bauer	U.S. Bureau of Reclamation	5	Negative	<p>1) The level of specificity in the original version of the standard far exceeds any other reliability standard. This departure in practice was accepted by the utilities because along with the incredible detail, there was an allowance for companies to exercise a certain degree of discretion in implementing the standard. The Commission has "...acknowledged the importance of flexibility and discretion in the CIP NOPR." While the Commission has expressed concern that standards need to be explicit in order to be enforceable it has also expressed that "...the CIP Reliability Standards do not simply allow flexibility, they require it." The Commission appears to understand the concern expressed by utilities in the NOPR process; and, while it required elimination of the term "reasonable business judgment", it has also allowed that "...ERO and the participants in the Reliability Standards development process may choose to develop alternative language to replace reasonable business judgment and propose it for Commission approval." While the standards drafting team was working on addressing the "alternative language", NERC has submitted a Technically Feasible Exemption (TFE) procedure for comment. The draft TFE is more restrictive by eliminating "reasonable business judgment" and "acceptance of risk" as a basis for exemptions. The standards drafting team submitted a revised set of standards that did not include any alternative language. It appears that references in the standards to "reasonable business judgment" and "acceptance of risk" were removed in deference to NERC's draft Technically Feasible Exemption (TFE) procedure which provided a mechanism to request and obtain such exemptions. The presence of the two (NERC Draft TFE and revised CIP002-CIP009 standards) are contradictory to the overall construction of the CIP002-CIP009 standards which relied upon the flexibility afforded by reasonable business judgment. Without the flexibility afforded by alternative language, the level of specificity in the CIP002-CIP009 is unacceptable. Either the alternative language is developed to support the high level of specificity or the standards need to be redrafted to confirm to overall approach used in the other reliability standards. A number of the requirements CIP005 R2.4, 2.6, 3.1, 3.2, CIP007 R4, 5.3, 6, and 6.3 asked that something be done where "technically feasible". These requirements appear to indicate the application of judgment of feasibility, however, no guidance is given on what has to be done when it is not "technically feasible" to remain compliant</p> <p>2) In addition, the Measures for these standards require the entities to make products of each</p>

Consideration of Comments on Initial Ballot — CIP-002-2 to CIP-009-2 — Cyber Security Standards (Project 2008-06)

Voter	Entity	Segment	Vote	Comment
				requirement conceivably available to any requestor. We believe this poses a security issue.
Response				<p>1) The SDT is diligently working to improve the CIP standards through a phased update approach. Version 2 of the standards removed the “reasonable business judgment” and “acceptance of risk” language as directed by the FERC in Order 706. While FERC Order 706 allowed for the development of alternative language, the SDT was not able to draft any suitable alternative that did not suffer the same issues as the language that was removed. The proposed process for requesting and approving Technical Feasibility Exceptions is a viable alternative. The proposed TFE modifications to the NERC Rules of Procedure define the basis for requesting a TFE and the actions that must be performed by the Responsible Entity to defer findings of non-compliance and imposition of penalties while working to achieve strict compliance with the Applicable Standard. The industry has an opportunity to provide comments to the proposed TFE process prior to adoption by the NERC Board of Trustees. The industry will likely have another opportunity to provide comments as part of the FERC approval process. The SDT recommends the industry take advantage of every opportunity to influence the ultimate TFE process. The SDT also recommends submitting this comment against Version 3 of the CIP standards if still appropriate.</p> <p>2) The NERC Monitoring and Enforcement Process, approved by Federal regulation, requires compliance data to be made available for inspection by the Compliance Enforcement Authority (CEA), subject to the US and Canadian laws and regulations regarding certain classes of protected information. The CEA Eligible Reviewer is obligated to protect such information from unauthorized disclosure. The proposed TFE process and Section 1500 of the NERC Rules of Procedure prescribe how such sensitive information will be protected. NERC continues to work through the process for dealing with this issue.</p>
Colin Anderson	Ontario Power Generation Inc.	5	Negative	<p>1) OPG has serious reservations with respect to two areas in the suite of CIP standard revisions: 1.) Multiple areas in the revisions in which the requirements for documenting change have been reduced from 90 to 30 days. These revised timeframes are unrealistic. Rushing such changes will likely create more of a reliability issue than the change itself seeks to remedy. OPG cannot support these revisions.  CIP-006 R1.7 - The requirement to update the physical security plan within 30 days.  CIP-007 R9 - The requirement for documenting changes to systems or controls within 30 days  CIP-008 R1.4 - The requirement to update the Cyber Security Incident Response Plan within 30 calendar days of any changes</p> <p>2.) CIP-006 R3 - This new requirement, not contemplated in FERC’s Order 706, is problematic in situations where a third party is used to monitor and administer portions of the program or where personnel are required to provide remote support to components of the ESP under emergency conditions. OPG submits that this revision has been hastily proposed and not fully considered.</p> <p>3) OPG is also surprised to see only one ballot (where revisions to all standards must be accepted or rejected as a group). Individual ballots would have better facilitated approvals.</p>
Response				1) Respectfully, the SDT believes the 30-day time frame from the completion of the change for updating documentation is appropriate and

Consideration of Comments on Initial Ballot — CIP-002-2 to CIP-009-2 — Cyber Security Standards (Project 2008-06)

Voter	Entity	Segment	Vote	Comment
				<p>reasonable. Having up-to-date documentation is essential to the management of the Cyber Assets and response to cyber incidents.</p> <p>2) CIP-006, Requirement R3 clarifies what was always expected by the CIP Standards. The SDT believes the Cyber Assets used to control and/or monitor ESP access will necessarily be internal to the Responsible Entity's protected network. Remote access for the purposes of contract support or emergency access can be managed like any other approved access into the ESP.</p> <p>3) The CIP standards should be viewed as a complete set, with FERC-mandated changes made to all eight version 2 standards. The SDT believes it is appropriate to ballot the eight version 2 standards as a single set for the Version 2 changes.</p>
Tony Kroskey	Brazos Electric Power Cooperative, Inc.	1	Negative	<p>1) Do not fully agree with the SDT responses to comments on CIP-006-R1.7, CIP-008-R1.4, CIP-004-R3, and</p> <p>2) the response for Question #10 relating to "compliant upon commissioning".</p>
Response				<p>1) The SDT interprets this comment as voicing a concern about reducing the timeframe to update documentation to 30 days. Respectfully, while the SDT acknowledges that the FERC Order 706 did not direct the timeframe to be reduced, the SDT believes 30 days from the completion of the change to update the Security Plan (CIP-006, Requirement R1.7) is no less reasonable than any other documentation update requirement. The SDT reduced this requirement to 30 days to be consistent with the rest of the update requirements throughout the CIP standards. With respect to CIP-008, Requirement R1.4, the SDT believes it is essential that up-to-date response plans be available in the event of an incident. The SDT determined 90 days to update response plans after an incident was too long and selected 30 days to be consistent with the rest of the update requirements throughout the CIP standards. The Commission in FERC Order 706, Paragraph 443, directed that "newly-hired personnel and vendors should not have access to critical cyber assets prior to the satisfactory completion of a personnel risk assessment, except in specified circumstances such as an emergency." The Responsible Entity is given the latitude to define emergency circumstances in its Cyber Security Policy required by CIP-003, Requirement R1.</p> <p>2) The SDT believes a Cyber Asset being installed as part of a planned change, either a new asset or replacing an existing one, should be evaluated for Critical Cyber Asset status as part of the asset implementation and that compliance with the CIP standards should be built in as part of the project. In doing so, the Cyber Asset is expected to be "compliant upon commissioning."</p>
Richard Salgo	Sierra Pacific Power Co.	1	Affirmative	<p>1) While I am voting "affirmative" on this ballot, I disagree with the change that was made in four of the Standards (CIP-006 R1.7, CIP-007 R9, CIP-008 R1.4, and CIP-009 R3) to reduce the time period for documentation of various changes from the present 90 days to 30 days. This may be achievable in some instances, however, this is felt to be imposing an undue burden on the entities for no tangible benefit to reliability.</p> <p>2) As well, we believe that CIP-006 is unclear with respect to requirements around relocation of security access control equipment. Does this require the relocation of such equipment within the Secure Perimeter?</p>

Consideration of Comments on Initial Ballot — CIP-002-2 to CIP-009-2 — Cyber Security Standards (Project 2008-06)

Voter	Entity	Segment	Vote	Comment
Response				<p>1) Respectfully, while the SDT acknowledges that the FERC Order 706 did not direct the timeframe to be reduced, the SDT believes 30 days from completion of the change to update the Security Plan (CIP-006, Requirement R1.7) is no less reasonable than any other documentation update requirement. The SDT reduced this requirement to 30 days to be consistent with the rest of the update requirements throughout the CIP standards. In Paragraph 651 of FERC Order 706, the FERC stated that 30 days was reasonable to update documentation (CIP-007, Requirement R9). The SDT agrees with the FERC assertion. With respect to CIP-008, Requirement R1.4, the SDT believes it is essential that up-to-date response plans be available in the event of an incident. The SDT determined 90 days to update response plans after an incident was too long and selected 30 days to be consistent with the rest of the update requirements throughout the CIP standards. In response to the FERC assertion at Paragraph 731 of FERC Order 706 that recovery plans should be updated within 30 days the SDT modified the CIP-009 requirement to require 30 days for updating the Recovery Plan. Per the NERC process, the SDT is unable to modify language in this version of the standards once in the balloting phase. The SDT recommends submitting this comment against Version 3 of the CIP standards if still appropriate.</p> <p>2) Requirement R2 refers to all components of the physical access control system, including the control panels that interface with the entrance sensors/locking mechanisms and the Cyber Assets used to manage/configure the control panels and interact (HMI interface) with the physical access control system. In Requirement R2.1, the SDT chose to use the terminology “protected from unauthorized physical access” in recognition that not all components of the physical access control system can be reasonably placed within the Physical Security Perimeter. The intent of this requirement is that the Cyber Assets that cannot be reasonably placed within the PSP, such as the HMI interface systems that might reside within the Security Department offices or guard station, be properly secured when not in use to prevent unauthorized reconfiguration of access rights. There is no requirement to relocate all security access control equipment within a Physical Security Perimeter so long as the equipment is protected from unauthorized access.</p>
John J. Blazekovich	Exelon Energy	1	Affirmative	Exelon does not support the 30 day timeframe for updates to the Phase 1 changes in the areas of physical security plan, recovery plan, systems and controls, and updates to the plan for the response to cyber security incidents documentation because it does not provide sufficient time to complete update, review and approval of documentation with leadership. The proposed 30 day timeframe should be increased to 60 days because in Order 706 there are references to other time periods. For example, P 731 covers R3 of CIP-009 and states, “However, the Reliability Standards development process may propose a time period other than 30 days, with justification that it is equally efficient and effective.” The 30 day timeframe should also not apply to situations where the entity has made 'administration only' changes to the documentation or other changes driven by internal business requests and/or decisions
Response				Per the NERC process, the SDT is unable to modify language in this version of the standards once in the balloting phase. The SDT recommends submitting this comment against Version 3 of the CIP standards if still appropriate.
Thomas C. Mielnik	MidAmerican Energy Co.	3	Affirmative	1) MidAmerican is concerned that the following statement has been removed throughout the standards: Duly authorized exceptions will not result in noncompliance. This sentence should be included in CIP-003-2, R3. This retains the clarity in version 1 that authorized exceptions are not violations.

Consideration of Comments on Initial Ballot — CIP-002-2 to CIP-009-2 — Cyber Security Standards (Project 2008-06)

Voter	Entity	Segment	Vote	Comment
				2) Exclude the client side of client-server applications used for access control and/or monitoring from CIP-006-2 protection requirements in R2 and R3.
Response	<p>1) An exception taken against the Responsible Entity's compliance policy does not relieve the entity from compliance with the requirement of the standard. The proposed modification to the NERC Rules of Procedure regarding Technical Feasibility Exceptions provides the appropriate relief from findings of non-compliance, subject to the terms of the TFE being met. The SDT cannot assert that a properly approved exception to the Responsible Entity's security policy will not result in non-compliance.</p> <p>2) The client side systems, such as the HMI interface, need to be protected from unauthorized access.</p>			
Charles W. Jenkins	Oncor Electric Delivery	1	Affirmative	Although NERC interpretation 2007-27, requested by SCE&G, is not included in Version 2, we rely on NERC's interpretation specifically stating that dial-up Critical Cyber Assets do not require physical protection required by CIP-006.
Response	Respectfully, neither the NERC BOT nor the FERC has adopted the referenced interpretation.			
Harvie D. Beavers	Colmac Clarion/Piney Creek LP	5	Negative	Changes have taken a fairly confusing set of standards and converted them into a nearly 'all encompassing' lawyers dream. Almost every generation facility has a control system that is a 'routable protocol', yet many have no external control or access, thus are not 'vulnerable' to external attack. Appears that all will have to be available to interpretation of current wording by not only plant management but any audit action. The 'criticality' of a generating asset is proportional to how many are operating in each load section and the load they are supplying. Current Glossary added to these procedures can be inferred to make everything a critical asset
Response	The determination on whether a facility is a Critical Asset is made independent of whether the cyber assets within it are critical cyber assets. This determination for cyber assets only occurs after a facility is declared a Critical Asset: there has been no change made to the glossary from version 1 to version 2. The current standards clearly state that for a cyber asset to be declared critical, it must satisfy the requirements of CIP-002 R3.1, R3.2 or R3.3: in the case of cyber assets which do not satisfy any of these criteria, they are not required to be declared Critical Cyber Assets.			
Thomas J. Szelistowski	Tampa Electric Co.	1	Negative	<p>1) CIP Standards Version 2 comments Implementation Plan Table 1 examples. How would an entity handle the reclassification of an asset from Cyber Asset to Critical Cyber Asset due to a new or re-interpretation of the wording and intent of the standard where the entity's methodology did not necessarily change.</p> <p>2) P5 Table 2. Depending upon the size and scope of the Critical Asset coming under the standard and entity subject to category 2 compliance will need more than 12 months to come into compliance with the requirements of CIP005 through CIP007. A significant effort is involved in planning for the execution of many of these requirements. Additionally, fiscal planning cycles may not align with the timing of the asset being deemed critical, leaving</p>

Consideration of Comments on Initial Ballot — CIP-002-2 to CIP-009-2 — Cyber Security Standards (Project 2008-06)

Voter	Entity	Segment	Vote	Comment
				<p>considerably less than 12 months for actual application of the standards. A 12 month cycle serves as a dis-incentive to the entity in declaring the asset critical as soon as it is aware of the need for reclassification. We suggest that at a minimum 24 months be allowed.</p> <p>3) P6 CIP002 through CIP009 General Comments Page numbering inaccurate, making review difficult</p> <p>4) Throughout, applicability provides exemption to facilities regulated under the US Nuclear Regulatory Commission. Needs to be updated to reflect recent FERC ruling.</p> <p>5) While the drafting team is performing edits to this document, it might be an appropriate time to remove some of the cross referrals within CIP005 and CIP006 to other standards. These can lead to confusion and mis-interpretation during implementation. Our organization and others within our region have had to create internal matrices to track all of these cross referrals. This draft introduces more cross referrals. If these must remain, then perhaps the drafting team can maintain either as a part of the standards or as a separate document a matrix that the industry can rely upon for consistency.</p> <p>6) For all revised standards, the Data Retention information 1.3 states Compliance Enforcement Authority in conjunction with the Registered Entity shall keep the last audit records and all requested and submitted subsequent audit records. The retention use to be three years and the registered entity had no responsibility to maintain audit records. It is not clear for registered entities what "last audit records" includes? Please detail what is considered an "audit record." In addition, based on current wording, "and all requested and submitted subsequent audit records", subsequent records (which would mean after the audit) appear to need to be retained forever.</p> <p>7) We continue to have serious concerns related to the "exception process" as we indicated in our last comments (Regarding the removal of the language in Section 1.5: Additional Compliance Information: It is not clear if removal of this language is implying that authorized exceptions result in non-compliance. There are situations where requirements of this standard cannot be met, particularly for legacy equipment and associated vendor supplied systems" and your response (Situations where the standards requirements cannot be met will be handled through the Technical Feasibility Exception process under the NERC Rules of Procedure.</p> <p>8) The technical feasibility exception process will address the requirements for documenting,</p>

Consideration of Comments on Initial Ballot — CIP-002-2 to CIP-009-2 — Cyber Security Standards (Project 2008-06)

Voter	Entity	Segment	Vote	Comment
				<p>approving, and remediating the exception. Any sanction decisions will arise from the TFE process. It is not appropriate to assert that “duly authorized exceptions will not result in non-compliance” within Section D-1.5 of the standard.) As the TFE process is now drafted, it addresses only those areas where technical infeasibility is mentioned in the standard.</p> <p>9) There are other requirements where it may be operationally unsafe or technically infeasible to meet. Under version 1 standards, this was recognized and provisions made to allow for exceptions without non-compliance. Under this version, it would appear that an exception to our cyber security policy may result in non-compliance. If this is the intent, the drafting team should review every requirement and identify every requirement where operational or technical infeasibility may be applicable so that the TFE process may be followed.</p> <p>10) CIP002- no comments</p> <p>11) CIP003 - It is not clear if this standard is going to be modified to incorporate or reflect the Technical Feasibility Exception process that is under development by NERC. We expect that the drafting team is working with NERC to reconcile this standard with the newly proposed process.</p> <p>12) CIP004 - no comments</p> <p>13) CIP005 - R1.5 needs clarification. Is the intent to protect devices which do security monitoring or should it include any type of monitoring which is done? Devices which perform performance monitoring of the perimeter, such as bandwidth analysis, etc should not be subject to these requirements as an access control or monitoring device. They may be a cyber asset within the perimeter, but they may be performing their performance monitoring from outside the perimeter. We suggest the following wording change: “Cyber Assets used in the access control and/or security monitoring of the Electronic Security Perimeter....” R1.5 Afforded the protective measures ofStandard CIP-006-2 Requirement R3 It is not clear how one monitors the physical security perimeter CIP006 -R3 when it is not required to have one around the devices listed in CIP005 R1.5</p> <p>14) CIP006 - No comment</p> <p>15) CIP007 - no comments</p> <p>16) CIP008 - no comments</p>

Consideration of Comments on Initial Ballot — CIP-002-2 to CIP-009-2 — Cyber Security Standards (Project 2008-06)

Voter	Entity	Segment	Vote	Comment
				17) CIP009 - no comments
Response				<p>1) This would be treated the same as an unplanned change due to a change in system conditions. The Responsible Entity would need to document why the new Critical Asset or Critical Cyber Asset is only now being identified.</p> <p>2) The 12-month timeframe is reasonable for most instances. Both the Self-Report with mitigation plan and the proposed TFE process changes to the NERC Rules of Procedure provide for requesting additional time to comply.</p> <p>3) Thank you for your comment. The SDT apologizes for the inconvenience and has made NERC staff aware of the issue.</p> <p>4) The exemption language is consistent with the definition of “facility” in FERC Order 706B at Paragraph 11. FERC clarified its terminology at Paragraphs 14 and 15. Per the NERC process, the SDT is unable to modify language in this version of the standards once in the balloting phase. This is an administrative change that can be accommodated separately.</p> <p>5) Per the NERC process, the SDT is unable to modify language in this version of the standards once in the balloting phase. The SDT recommends submitting this comment against Version 3 of the CIP standards if still appropriate.</p> <p>6) The language in Section D “Compliance” was modified to be consistent with the rest of the NERC standards.</p> <p>7) An exception taken against the Responsible Entity's compliance policy does not relieve the entity from compliance with the requirement of the standard. The exception taken against a company policy is a separate issue from an exception against the requirement of the standard. A Responsible Entity may find it has to process both types of exceptions. Respectfully, the CIP SDT has no control over the approval process for changes to the NERC Rules of Procedure. The industry has an opportunity to provide comments to the proposed TFE process prior to adoption by the NERC Board of Trustees. The industry will likely have another opportunity to provide comments as part of the FERC approval process. The SDT recommends the industry take advantage of every opportunity to influence the ultimate TFE process.</p> <p>8) Respectfully, the CIP SDT has no control over the approval process for changes to the NERC Rules of Procedure. The industry has an opportunity to provide comments to the proposed TFE process prior to adoption by the NERC Board of Trustees. The industry will likely have another opportunity to provide comments as part of the FERC approval process. The SDT recommends the industry take advantage of every opportunity to influence the ultimate TFE process.</p> <p>9) The observation is correct. An exception taken against the Responsible Entity's compliance policy does not relieve the entity from compliance with the requirement of the standard. Respectfully, while the CIP SDT will consider the TFE issue in future revisions to the standards, the SDT cannot predict and account for all possible nuances that might require a TFE. Per the NERC process, the SDT is unable to modify language in this version of the standards once in the balloting phase. The handling of TFE requests in those instances where they not currently permitted by the proposed Appendix 4D to the NERC Rules of Procedure is best addressed by a modification to the Rules of Procedure. The industry has an opportunity to provide comments to the proposed TFE process prior to adoption by the NERC Board of Trustees. The industry will likely have</p>

Consideration of Comments on Initial Ballot — CIP-002-2 to CIP-009-2 — Cyber Security Standards (Project 2008-06)

Voter	Entity	Segment	Vote	Comment
				<p>another opportunity to provide comments as part of the FERC approval process. The SDT recommends the industry take advantage of every opportunity to influence the ultimate TFE process. The SDT recommends the industry comment to NERC and, if necessary, FERC proposing how the issue might be remedied in the TFE process.</p> <p>10) Thank you.</p> <p>11) While the CIP SDT will consider the TFE issue in future revisions to the standards, the proposed TFE process is a separate document under the NERC Rules of Procedure. The industry has an opportunity to provide comments to the proposed TFE process prior to adoption by the NERC Board of Trustees. The industry will likely have another opportunity to provide comments as part of the FERC approval process. The SDT recommends the industry take advantage of every opportunity to influence the ultimate TFE process.</p> <p>12) Thank you.</p> <p>13) The SDT understands this comment to suggest adding the word "security" before "monitoring." Per the NERC process, the SDT is unable to modify language in this version of the standards once in the balloting phase. The SDT recommends submitting this comment against Version 3 of the CIP standards if still appropriate.</p> <p>14) Thank you.</p> <p>15) Thank you.</p> <p>16) Thank you.</p> <p>17) Thank you.</p>
James R. Keller	Wisconsin Electric Power Marketing	3	Negative	<p>1) Comments on CIP 006-2, R2.1 We Energies understands that this requirement refers to the programmable logic controller in a card reader system that is often referred to as the "panel". The panel is the intelligent device that serves a card reader-controlled door. The proposed text requires protection of the panels from unauthorized physical access. We believe that the use of the word "unauthorized" establishes a more stringent requirement than that which the drafting team intended. We believe this because authorization implies establishment of a list of individuals who have been authorized to physically access the asset and implies the installation of some mechanism to distinguish between authorized and unauthorized attempts to physically access the panel door. In effect, it appears to create a duty to add a card reader to the panel door, itself. We Energies agrees that the panels need to be protected against physical tampering and we believe that installation of a key lock and intrusion detection capability for the panel door is appropriate and adequate. Accordingly, we believe that R2.1 should have read, "Be protected from undetected physical access." If this was the drafting</p>
Anthony Jankowski	Wisconsin Energy Corporation	4	Negative	
Linda Horn	Wisconsin Electric Power Company	5	Negative	

Consideration of Comments on Initial Ballot — CIP-002-2 to CIP-009-2 — Cyber Security Standards (Project 2008-06)

Voter	Entity	Segment	Vote	Comment
				<p>team's intention, We Energies requests this clarification.</p> <p>2) Comments on CIP 006-2, R2.2 We Energies understands that this requirement refers to the programmable logic controller in a card reader system that is often referred to as the "panel". The panel is the intelligent device that serves a card reader-controlled door. The proposed text appears to require that the panels be protected from physical tampering by placing them inside an already-protected physical security perimeter (PSP), or appears to require construction of a new PSP solely to protect the panel. The former sometimes can be easily accomplished by moving a panel from a location just outside the PSP to a location just inside the PSP. The latter is more challenging when the panel is distant from the PSP, sometimes separated by hundreds of feet and substantial barriers. We Energies agrees that the panels need to be protected against physical tampering and placing them inside a PSP offers better protection than leaving them outside a PSP. Locking the panel door and installing intrusion detection on the door is even better. However, these do not offer protection against cyber tampering. For instance, a panel is not protected against cyber tampering at the point where the panel's data communications cable connects to the LAN/WAN network in a remote data closet. Simply unplugging this cable in the data closet and connecting it to a laptop PC on which has been installed the access control system application affords an individual the ability to tamper with the data and settings in the panel. We Energies can eliminate the risk to the data and settings in the panel without physically moving it by replacing the conventional copper data cable with a fiber-optic cable and encrypting the communications. This is more effective than physically moving the panel to a location inside a PSP. We Energies suggests establishment of an option under R2 which would permit such a technical alternative to physically relocating the panels.</p>
Response	<p>1) Requirement R2 refers to all components of the physical access control system, including the control panels that interface with the entrance sensors/locking mechanisms and the Cyber Assets used to manage/configure the control panels and interact (HMI interface) with the physical access control system. In Requirement R2.1, the SDT chose to use the terminology "protected from unauthorized physical access" in recognition that not all components of the physical access control system can be reasonably placed within the Physical Security Perimeter. The intent of this requirement is that the Cyber Assets that cannot be reasonably placed within the PSP, such as the HMI interface systems that might reside within the Security Department offices or guard station, be properly secured when not in use to prevent unauthorized reconfiguration of access rights.</p> <p>2) Requirement R2 refers to all components of the physical access control system, including the control panels that interface with the entrance sensors/locking mechanisms and the Cyber Assets used to manage/configure the control panels and interact (HMI interface) with the physical access control system. In Requirement R2.2, placing the panel referred to in the comment within the PSP it controls, or any other suitable PSP, is consistent with SDT's understanding the requirement. Protecting the connecting data cable from unauthorized access via the data closet is also expected if required to prevent unauthorized logical access as described in the comment.</p>			

Consideration of Comments on Initial Ballot — CIP-002-2 to CIP-009-2 — Cyber Security Standards (Project 2008-06)

Voter	Entity	Segment	Vote	Comment
Raymond Phillips	Alabama Municipal Electric Authority	4	Affirmative	I understand why the SDT decided to approach changes to the CIP standards in phases but it makes for a lot of additional work on everyone involved.
Response	Included in the FERC Order 706 were time-specific directives that made a phased implementation approach necessary. The SDT has attempted to minimize the impact of the first round of changes as much as possible.			
Catherine Koch	Puget Sound Energy, Inc.	1	Affirmative	PSE votes affirmative with version 2 changes, but anticipates the opportunity to provide more detailed comment regarding each standard in general when version 3 draft is available for comment. The standards are in need of further clarity to ensure compliance in the most effective manner.
Response	Thank you for your comment. The SDT looks forward to your comments when Version 3 of the standards is submitted for industry review.			
Anita Lee	Alberta Electric System Operator	2	Abstain	The AESO is not certain of the impact of these standards on the market and grid operation in Alberta.
Response	Thank you for your comment. Respectfully, the SDT is not able to respond to your concern.			
John D. Martinsen	Public Utility District No. 1 of Snohomish County	4	Negative	The District understands the removal of "reasonable business judgment" was done in accordance with FERC Order 706 and the proposed Technical Feasibility Exception Process should address the concerns regarding the removal of reasonable business judgment. The District agrees that "reasonable business judgment" is not the ideal statement however we are also concerned with the response that the proposed "Technical Feasibility Exception Process should address the concerns". A more prescriptive process may address this concern but it could just as likely produce unacceptable consequences. The District believes that assessment of risk and engineering/economic judgment are all necessary skills when assessing critical assets. It is important to understand the impacts that a cyber or other failure may have on the Bulk Electric System and assess the risk internally as well as neighboring systems. This assessment must focus on risk/exposure and the level of impact. There are many risks to the electric industry, and it is important that the standards focus limited resources on addressing exposures by include risk levels and impacts into the decision making process.
Response	The Version 2 revisions to the CIP standards are intended to address the time-specific changes mandated by the FERC. The SDT recommends submitting this comment against Version 3 of the CIP standards if still appropriate.			
John Apperson David Godfrey	PacifiCorp	3 5	Affirmative Affirmative	The following statement has been removed throughout the standards: "Duly authorized exceptions will not result in noncompliance." While PacifiCorp understands that the proposed NERC procedure for Requesting and Receiving Technical Feasibility Exceptions to NERC Critical Infrastructure Protection Standards is intended to provide guidance and clarity on how these necessary exceptions will be viewed by NERC, the standards as presented lack the clarity that authorized exceptions are not violations.
Response	An exception taken against the Responsible Entity's compliance policy does not relieve the entity from compliance with the requirement of the			

Consideration of Comments on Initial Ballot — CIP-002-2 to CIP-009-2 — Cyber Security Standards (Project 2008-06)

Voter	Entity	Segment	Vote	Comment
				standard. The proposed modification to the NERC Rules of Procedure regarding Technical Feasibility Exceptions provides the appropriate relief from findings of non-compliance, subject to the terms of the TFE being met. The SDT cannot assert that a properly approved exception to the Responsible Entity's security policy will not result in non-compliance.
William Mitchell Chamberlain	California Energy Commission	9	Affirmative	This affirmative vote is based on the continuing nature of Project 2008-06 which needs to address ambiguous language being identified by parties, and the belief that NERC audit activities will take into account known issue areas yet to be addressed within the Project.
Diane J. Barney	National Association of Regulatory Utility Commissioners	9	Affirmative	
Response				Thank you for your comment. The SDT is already working on additional revisions to the CIP standards. Please be sure to comment on future revisions to the standards when posted for industry review.