Consideration of Comments on Initial Ballot — Cyber Security Ninety-day Response (Project 2009-21)

Summary Consideration: The initial ballot achieved a quorum and a weighted segment approval of 88.07%. There were 16 comments submitted with a negative ballot, and six comments submitted with an affirmative ballot. All of the comments received and the drafting team's consideration of those comments are shown below.

The comments mostly addressed changes made to the Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities and the visitor control program in CIP-006. The drafting team considered the comments and responded with clarifications on the intent and scope of the changes made to the draft for the initial ballot. No changes were made to the standards and the implementation plans following the initial ballot.

Segment:	1
Organization:	American Transmission Company, LLC
Member:	Jason Shaver
Comment:	It is ATC's opinion that the 12 months provided in Table 2 for becoming compliant with CIP-006-2 and CIP-007-2 may not be arealistic time line, depending on the facility identified, and that the SDT should re-evaluate its proposal. ATC would prefer to see CIP-006 and CIP-007 align with CIP-004's implementation milestone. (CIP-004 allows for an 18 month implementation window) a. CIP-004 establishes the requirements for how entities will identify the training and access to Critical Cyber Assets located within a Physical Security Parameter. b. CIP-006 establishes the requirements for how entities will (Physically) protect it's Critical Cyber Assets. Specifically R2.1 states that entities have to protect from unauthorized physical access. In other words from individuals that have not been identified in CIP-004 as having access and training. c. CIP-007 establishes the requirements for how entities will (Cyber) protect it's Critical Cyber Assets. Specifically R3.2 states that entities have to detect and alert for attempts at or actual unauthorized access. i. Because these three standards do not align in terms of implementation milestone it seems that a situation could occur in which entities have both Physical and Cyber protection for their Critical Cyber Assets but necessary personnel may not have the access per CIP-004.

	We believe that the 18 months implementation milestone for CIP-004 is necessary but that both CIP-006 and CIP-007 need to align with CIP-004 in-order to avoid the situation we have identified. ATC suggest that the SDT update Table 2 to acknowledge that it applies to both Version 2 and Version 3 standards. (NOTE: Table 3 already contains an "or" statement) The version 2 standards will become mandatory and enforceable on April 1, 2010. The Version 3 standards state that they will become effective on the first day of the third calendar quarter after applicable regulatory approval. (Example: If these standards are approved by FERC anytime between January 1, 2010 and March 31 2010 then they will become effective on November 1, 2010.) Does the SDT agree with our understanding? The Version 3 implementation plan states that "When these standards (Version 3) become effective, all prior versions of these standards are retired". ATC is curious with the recent NERC filing (FERC Docket RM10-5) for an interpretation for CIP-007-2a. It is our understanding that the interpretation contained in CIP-007-2a was not incorporated in CIP-007-3. Will the interpretation contained in CIP-007-2a be appended to CIP-007-3 following FERC approval?
Response: Thank you for your comments. It is the drafting team's opinion that 12 months is a reasonable time frame for the implementation of CIP-006 and CIP-007 for entities that already have a CIP compliance program in place. The additional 6 months allowed for CIP-004 provides the time necessary for entities to complete the training and risk assessment for any additional personnel once these have been implemented. Entities can start performing the training and risk assessment concurrent with the implementation of CIP-005, CIP-006 and CIP-007. The compliance milestones did not change from Version 2 to Version 3, but the drafting team will address this issue as part of the Version 4 development. The posted Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities includes the following statement on Page 1, immediately following the title: "***This Implementation Plan applies to Cyber Security Standards CIP-002-2 through CIP-009-2 and CIP-002-3 through CIP-009-3.***" FERC approved interpretations are attached to the affected standard (in a similar way the interpretation for CIP-006 R1.1 was attached as Appendix 1 to CIP-006-3a).	
Segment:	1, 3
Organization:	Duke Energy Carolina
Member:	Douglas E. Hils, Henry Ernst-Jr
Comment:	Duke Energy appreciates the drafting team's efforts on the CIP standards and Implementation Plan. However, the Implementation Plan for newly identified Critical Cyber Assets is unnecessarily complex and should be simplified in

	a future revision. It forces entities to track compliance at the Critical Cyber Asset level; this means at the device level. For each new cyber asset to which the standards apply, we must determine the time of compliance by each requirement because the length of time allowed to meet compliance may vary by each requirement. This approach is un-necessarily complex and will result in a lot of record keeping for the entities with little actual enhancement to security. Anything that can be done to simplify the approached used would be of benefit.
Response: Thank you for your comment. There are many circumstances under which a particular Responsible Entity can have newly identified Critical Cyber Assets. The Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities covers these many circumstances to provide for an implementation schedule that is fair for all circumstances while reducing the complexity as much as possible. The compliance milestones did not change from Version 2 to Version 3, but the drafting team will address this issue as part of the Version 4 development.	
Segment:	1; 3; 3; 3; 3
Organization:	Southern Company Services, Inc.; Georgia Power Company; Gulf Power Company; Mississippi Power; Alabama Power Company
Member:	Horace Stephen Williamson; Leslie Sibert; Gwen S Frazier; Don Horsley; Bobby Kerley
Comment:	The documentary evidence necessary to prove auditable compliance on every new CCA device at every point in time will likely prove to be unreasonably burdensome. Also the implementation plan is unreasonably complex and needs to be revamped. We need a straightforward way to maintain the CCA list along with a reasonable way to demonstrate that changes were appropriate, timely, and in compliance with standards. The current implementation plan does not lend itself to straightforward way of maintaining the CCA list.
Response: Thank you for your comment. There are many circumstances under which a particular Responsible Entity can have newly identified Critical Cyber Assets. The Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities covers these many circumstances to provide for an implementation schedule that is fair for all circumstances while reducing the complexity as much as possible. The compliance milestones did not change from Version 2 to Version 3, but the drafting team will address this issue as part of the Version 4 development.	
Segment:	3

Organization:	Central Lincoln PUD
Member:	Steve Alexanderson
Comment:	NERC may find it difficult to achieve approval when so much is included in a single project. Central Lincoln finds the use of the word "milestone" used in the context of Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities to be odd. The word is usually associated with multiple stones along a path to an ultimate destination, yet only one milestone is associated with each requirement in a category per Table 2. Could this be reworded better?
Response: Thank you for your comment. The definition of "milestone" in common dictionaries includes: "a significant point in development " (Merriam-Webster) and "an event or achievement that marks an important stage in a process" (MacMillan). In the opinion of the drafting team, this word conveys the intent in the document.	
Segment:	1; 5; 6
Organization:	Manitoba Hydro
Member:	Michelle Rheault; Mark Aikens; Daniel Prowse
Comment:	The Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities was significantly changed after approval by industry and the NERC BOT. The changes, pertaining to periodic requirements, were not directed by FERC in Order 706 or Order RD09-7-000, or through industry comments. The changes require that for a number of requirements, which were not specified by NERC, with "… a prescribed periodicity… the first occurrence of the recurring requirement must be completed by the Compliant milestone date…", which could advance the need to meet the requirements up to a year. This is not the general understanding of the industry, and was not the guidance provided in the NERC (Revised) Implementation Plan for Cyber Security Standards CIP-002-1 through CIP-009-1. From the (Revised) Implementation Plan for Cyber Security Standards CIP-002-1 through CIP-009-1 document provided with the Version 1 standards, "Compliant means that the entity meets the full intent of the requirements, and is beginning to maintain required "data", "documents", "logs", and "records". Auditably Compliant means that the entity meets the full intent of the requirements and can demonstrate compliance to an auditor, including 12-calendar-months of auditable "data", "documents", "logs", and "records"." Meeting the intent of the requirements means that the processes, procedures and infrastructure are in place to begin collecting data during the Auditably Compliant period. A quarterly review should not need to be conducted before the Compliant date; it is completed, at latest, at the end of the first quarter of the compliance period.

	The direction provided in the new Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities is unclear and inconsistent, as some unspecified requirements with a prescribed periodicity must have their first periodic occurrence completed by the compliance date, while other unspecified periodic requirements can begin collection of their respective data by the compliance date. It is too late to introduce new compliance direction for standards whose initial compliance dates will have passed by the time the Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities is approved. We recommend the removal of the paragraph on Page 2 which begins "A number of the NERC Reliability Standard requirements include a prescribed periodicity …". With the removal of that paragraph, the following paragraphs in that section are unnecessary and should also be removed.
Response: Thank you for your comment. References to this interpretation of periodicity were removed from the document before we began the initial ballot.	

Segment:	1
Organization:	Baltimore Gas & Electric Company
Member:	John J. Moraski
Comment:	Clarification is needed on how to apply a visitor control program for PSPs that have been established at a cabinet level (e.g., CCAs, or equipment treated as a CCA per CIP requirements, are housed within a secured cabinet that is located within a data center, and they are the only CCAs within the data center. Access to the cabinet that houses the CCAs is controlled, and therefore the cabinet serves as the PSP for these cyber assets)?
Response: Thank you for your comment. The visitor control program applies to all Physical Security Perimeters. Implementation of the specific controls to satisfy the requirements of the visitor control program is left up to each Responsible Entity.	

Segment:	1; 3; 4; 5
Organization:	Sacramento Municipal Utility District
Member:	Tim Kelley; James Leigh-Kendall; Mike Ramirez; Bethany Wright
Comment:	Sacramento Municipal Utility District disagrees with the defined "continuous" escort of R1.6.2. In its strictest sense it requires not letting the visitor out of sight. As with other standards reasonableness must be applied to standard

	interpretations. This standard should not require visitor escort into a room that contains no CCAs and only a single access point to the room, i.e. bathroom or meeting room. Discretion should be permitted by the responsible person(s) providing the escort to such facilities.
Response: Thank you for your comment. The requirement for continuous escort applies to any defined Physical Security Perimeter. If the Physical Security Perimeter includes meeting rooms or rooms with no Critical Cyber Asset, then the Responsible Entity is required to meet the requirements for continuous escort for persons who do not have authorized unescorted access to the defined Physical Security Perimeter. Responsible Entities have flexibility in defining Physical Security Perimeters as long as all Critical Cyber Assets are within a Physical Security Perimeter. This requirement was not changed from the Version 2 standards.	
Segment:	4
Organization:	Public Utility District No. 1 of Snohomish County
Member:	John D. Martinsen
Comment:	The definition of “continuous” in its strictest sense may be interpreted as not letting the visitor out of sight. More work is needed to clarify this, since restrooms, or other facilities may be within the security parameter. This may be addressed by addressed by adding language regarding areas in the secure areas that have a single point of entry or exit.
Response: Thank you for your comment. The requirement for continuous escort applies to any defined Physical Security Perimeter. The Responsible Entity is required to meet the requirements for continuous escort for persons who do not have authorized unescorted access to the defined Physical Security Perimeter. Responsible Entities have flexibility in defining Physical Security Perimeters as long as all Critical Cyber Assets are within a Physical Security Perimeter. This requirement was not changed from the Version 2 standards.	
Segment:	3
Organization:	San Diego Gas & Electric
Member:	Scott Peterson

Comment:	SDG&E does not agree with the change under CIP-006 to require logging each time a visitor exits the PSP, especially since the visitors are escorted. SDG&E believes that logging each time a visitor enters and logging the visitor out at the end of the visit is sufficient.
Response: Thank you for your comment. The FERC directive in the order specifically included logging of exit.	
Segment:	5
Organization:	U.S. Bureau of Reclamation
Member:	Martin Bauer
Comment:	Unfortunately, the SDT revised the language in CIP 006 regarding the visitor control program from the earlier version. While we agree with the change in R 1.6.2, the change to R 1.6.1 reduced the clarity and watered down what was required to be included in the visitor program. This change eliminates the requirement to log the visitors identity as well as who performed the escort. The changes were only apparent by comparing the two documents (see below). The changes were made on the pretext that is was more consistent with the FERC order and in response to comments received. Since FERC cannot write standard and the comments reduced the clarity of the requirement, we would disagree that it was an appropriate change. A visitor management program that does not include identification of visitors (unique identifiers as characterized in V1/2) is not a visitor management program. If you cannot identify who was there, there is no point in logging anything.
Response: Thank you for your comment. Requirement R6 of CIP-006-3 specifically requires sufficient information to uniquely identify individuals and the time of access. R1.6.1 provides the additional minimum requirements for the logging of visitors. Responsible Entities can include any additional requirements in their specific Visitor Control Program.	
Segment:	2
Organization:	Midwest ISO, Inc.
Member:	Jason L Marshall
Comment:	We voted affirmative because we do not have any major issues with the content of the changes. However, we disagree with the need to violate the FERC approved NERC Reliability Standards Development Procedure by shortcircuiting the time line of the procedure. None of these changes are significant or even plug a reliability gap.

	Rather the changes are really clarifications of what is required by continous escorting in CIP-006-2 R1.6. In fact, visitor pass management is already required by CIP-006-2 R1.4. We object to rushing these changes through because it does not allow proper vetting of the changes and because it distracts scarce resources working on the next generation of CIP standards from that important job of improving cyber security. The Commission's 90-day timeline does not allow one to file an intervention, request for time extension or clarification with any reasonable expectation of a response before NERC must have their changes ready. Further, the 90-day timeline also does not allow the NERC standards drafting team to make changes based on industry comments or voting. Furhtermore, the scarce resources drafting the next generation of CIP standards are same resources that had to make these changes to the CIP standards and respond to industry comments. This only serves to delay the development of the true enhancements to the CIP standards by the amount of time it takes to develop these Commission ordered clarifying modifications.

Response: The drafting team appreciates your comment. As the ERO, NERC has an obligation to comply with the Commission's directives.

Segment:	5
Organization:	Northern States Power Co.
Member:	Liam Noailles
Comment:	We felt that the drafting team's response to our comment in the last ballot was very helpful and addressed our concern. However, no corresponding clarification was made to the interpretation. Interpretations should not introduce new ambiguity. We feel that it is the drafting team's responsibility to ensure that the issues relating to "potential sources" is clear in the interpretation and modifications should be made. One suggested way to clarify the interpretation is to add some of the language in the drafting team's response to our comment in the last ballot.

Response: Thank you for your comment. However, this comment is not relevant to the modifications made for the Cyber Security 90-day response.